ГЕОРГИ
ГЕНОВ
СТОИЛ
МИХОВСКИ
ТОДОР
МОЛЛОВ

Алгебра с теория на числата

ИЗДАТЕЛСТВО НАУКА И ИЗКУСТВО, СОФИЯ, 1991

В предлаганата книга е включен основният материал от най-важните раздели на алгебрата. Разглежданите в нея въпроси лежат в теоретичния фундамент на съвременната математика и на нейните приложения.

Книгата е учебник за студентите по математика от Пловдивския университет „Паисий Хилендарски", но може да се използува и от студентите в другите висши учебни заведения.

c/o Jusautor, Sofia
Индекс 51

СЪДЪРЖАНИЕ

Глава V
Пръстени и полета

Глава VI
Области на главни идеали

Глава VII
Елементи от теория на числата

Глава VIII
Елементи от теория на полетата

Глава IX
Модули

Глава X
Нормална форма на линейните преобразувания

Глава XI
Тела. Линейни асоциативни алгебри над полета

Глава XII
Елементи от теорията на Галоа

Допълнение

ПРЕДГОВОР КЪМ ВТОРОТО ИЗДАНИЕ

Във второто издание са нанесени поправки на забелязаните неточности и печатни грешки в първото издание на учебника. Отчетени са също така някои препоръки от страна на колегите ни. Допълнително включихме два нови раздела. Първият е глава XII, в която излагаме основите на теорията на Галоа. С това се запълва един съществен недостатък на първото издание. Във втория нов раздел — Допълнение, са включени основни понятия от теория на множествата и някои елементарни факти за целите числа. Опитът показва, че включването на тези елементарни сведения е необходимо за по-доброто усвояване на основния материал.

Добавянето на нов материал ни застави да извършим някои съкращения. По нов начин излагаме материала от края на глава III. С ново, по-кратко доказателство е дадена структурната теорема за крайно породените модули над област на главни идеали, а § 7, 8 и 9 на глава IX от първото издание са изцяло пропуснати. Доказателствата на редица твърдения са опростени.

Приятна ни е възможността да изкажем най-сърдечна благодарност на К. Чакърян и С. Додунеков, които със своите критични бележки допринесоха много за подобряване на качеството на учебника. Следва да отбележим особено прецизното и компетентно рецензиране на глава XII от К. Чакърян, което повлия силно върху окончателния облик на тази глава.

От авторите

ПРЕДГОВОР
КЪМ ПЪРВОТО ИЗДАНИЕ

Алгебрата един от основните раздели на математиката Със своите методи, резултати и удобен език тя навлезе широко в другите теоретични и приложни области на математиката. Това прави немислимо изучаването на която и да било съвременна математическа дисциплина без познаването на основите на алгебрата. Целта на предлагания учебник е да се изложат тези основи в обема и стила на съвременните учебни програми за студентите по математика в Пловдивския университет „Паисий Хилендарски". Във връзка с това в учебника е включена глава VII по теория на числата. Теорията на числата е един от първоизточниците на алгебрата. Като нарушаваме обаче историческата последователност на развитие, първо изучаваме групи и пръстени, а след това прилагаме редица от получените резултати при разглеждането на въпроси от теорията на числата. С това се постига по-голяма яснота, краткост и, което е по-важно според нас, по-голяма алгебричност на доказателствата.

Във всяка една глава на учебника за всяко ново понятие сме развили теорията до постигането на сравнително нетривиални и дълбоки резултати. Така например за групи доказваме теоремите на Силов; за пръстени — китайската теорема за остатъците, основната теорема на аритметиката на области на главни идеали; за полета — теоремите за съществуване и единственост на полето на разлагане на полином, теоремата за пълното описание на крайните полета; за модули — структурната теорема за крайно породените модули над област на главни идеали; за асоциативни алгебри над поле — теоремата на Фробениус и теоремата на Ведербърн за комутативността на крайните тела; като приложение на теорията на полетата доказваме критерия за разрешимост на задачите за построените с линия и пергел. В глава X сме развили теорията на Жордан за нормалната форма на линейните преобразувания. Доказателството на теоремата на Жордан е проведено с прилагане на структурната теорема за крайно породените модули над област на главни идеали, което е най-естественото за този учебник.

Тъй като учебникът е предназначен за студентите по математика от първи и втори курс на редовното и задочното обучение, то изложението на материала е сравнително елементарно, с примери и на много места със задачи. За разбирането му се изисква минимално количество знания в обема на традиционния курс по линейна адгебра. На някои места сме давали кратки исторически сведения за появата на едно или друго понятие, проблем или ре-

зултат, но изложението на тези сведения не е систематично и няма претенции за пълнота.

За да добие сегашния си вид и за да бъде в съответствие с новите учебни програми, съдържанието на учебника бе преработвано неоднократно и лекции по него са четени вече няколко години пред студентите по математика от Пловдивския университет „Паисий Хилендарски“. Надяваме се, че сме постигнали вече еднаквост на стила във всичките му части.

В заключение искаме да изкажем горещата благодарност на М. Гаврилов и Л. Давидов, които най-задълбочено прегледаха ръкописа и с направените препоръки значително ни помогнаха за неговото подобряване. Благодарим за проявеното старание и на машинописката Сн. Ямалиева. Като съзнаваме, че и тримата автори носим еднакво отговорността за качествата на учебника, готови сме да приемем с благодарност всяка обоснована критика, препоръка или отделна забележка.

От авторите

ГЛАВА I

КОМПЛЕКСНИ ЧИСЛА

§ 1. Построяване на множеството на комплексните числа

В училищния курс по математика се разглеждат множествата **N**, **Z** и **Q** съответно на естествените, целите и рационалните числа и се изгражда известна представа за реалните и комплексните числа. По-нататък, при изучаване на диференциалното и интегрално смятане, се въвежда строго понятието реално число и множеството **R** на реалните числа. Понятието реално число обаче все още не е достатъчно общо. Най-проста, но не и единствена причина за необходимостта от разширяване на множеството на реалните числа до множеството на комплексните числа е фактът, че не всяко квадратно уравнение с реални коефициенти има корен в R. Например няма реално число, което да е корен на уравнението $x^2+1=0$. Следователно представлява интерес да се разшири множеството на реалните числа така, че в новото числово множество да съществуват операции събиране и умножение със същите свойства както при реалните числа и уравнението $x^2+1=0$ вече да има корен. По-късно ще се види, че след осъществяването на тази цел е постигнато много повече и че в известен смисъл множеството на комплексните числа е единствено, т. е. въвеждането на комплексните числа е последен и окончателен етап в развитието на понятието число.

Нека

$$\mathbf{C}=\{(a, b)|a, b\in \mathbf{R}\}$$

е множеството на всички наредени двойки (a, b) от реални числа a и b. По определение ще считаме, че $(a, b)=(c, d)$ тогава и само тогава, когато $a=c$ и $b=d$. В множеството C дефинираме операции събиране и умножение съгласно равенствата

$$(1)\qquad (a, b)+(c, d)=(a+c, b+d),$$

$$(2)\qquad (a, b).(c, d)=(ac-bd, ad+bc).$$

Нека α, β и γ са три произволни елементи от C. Не е трудно да се провери, че събирането и умножението на елементи от C притежават следните свойства:

1) $\alpha+\beta=\beta+\alpha$ — *комутативен закон при събиране;*

2) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ — *асоциативен закон при събиране;*

3) *съществува и при това еднозначно определен нулев елемент на* C, *т. е. такъв елемент* ω *от* C, *за който е в сила равенството* $\alpha+\omega=\alpha$; очевидно $\omega=(0; 0)$;

4) *за всеки елемент* a *от* C *съществува и при това ед*

нозначно определен противоположен елемент, т. е. такъв елемент $-\alpha \in \mathbf{C}$, че $\alpha+(-\alpha)=\omega$; ако $\alpha=(a, b)$, очевидно $-\alpha=(-a, -b)$;

5) $\alpha\beta=\beta\alpha$ — *комутативен закон при умножение;*

6) $(\alpha\beta)\gamma=\alpha(\beta\gamma)$ — *асоциативен закон при умножение;*

7) $(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$ — *дистрибутивен закон;*

8) $\alpha\omega=\omega$, *където* ω *е нулевият елемент на* C;

Ще покажем, че в C може да се въведат операциите изваждане и деление, които са обратни съответно на събирането и умножението.

Твърдение 1. *За произволни елементи* α *и* β *от* C *уравнението* $\alpha+x=\beta$ *има единствено решение* x *в* C.

Доказателство. Нека $\alpha=(a, b)$ и $\beta=(c, d)$. Лесно се проверява, че елементът $x=(c-a, d-b)$ от C е решение на разглежданото уравнение. От друга страна, ако $\xi=(u, v)\in \mathbf{C}$ е произволно решение на $\alpha+x=\beta$, т. е. $(a+u, b+v)=(c, d)$, то $a+u=c$, $b+v=d$, откъдето следва, че $u=c-a$, $v=d-b$. Така се получава, че $\xi=x$, т. е. x е единствено решение на разглежданото уравнение. Твърдението е доказано.

Единственото решение x на уравнението $\alpha+x=\beta$ се бележи с $\beta-\alpha$ и се нарича *разлика* на β и α. По такъв начин имаме

$$(c, d)-(a, b)=(c-a, d-b). \tag{3}$$

Твърдение 2. *Ако* α *и* β *са два произволни елемента от* C *и* $\alpha\neq\omega$, *то уравнението* $\alpha x=\beta$ *има единствено решение в* C.

Доказателство. Нека $\alpha=(a, b)$ и $\beta=(c, d)$. Да допуснем, че уравнението $\alpha x=\beta$ притежава решение $x=(u, v)\in \mathbf{C}$. Тогава $(au-bv, av+bu)=(c, d)$ и следователно

$$\begin{cases} au-bv=c, \\ bu+av=d. \end{cases}$$

Тъй като $\alpha\neq\omega$, то $a^2+b^2\neq 0$ и горната система притежава единственото решение

$$u=\frac{ac+bd}{a^2+b^2},\quad v=\frac{ad-bc}{a^2+b^2}, \tag{4}$$

т. е. ако решението $x=(u, v)$ съществува, то се определя еднозначно от формулите (4). Обратно, с непосредствена проверка се убеждаваме, че двойката (u, v), определена от (4), е решение на уравнението $\alpha x=\beta$.

Ако $\alpha=(a, b)\neq\omega$ и $\beta=(c, d)$, единственото решение $\delta\in \mathbf{C}$ на уравнението $\alpha x=\beta$ ще бележим с $\delta=\frac{\beta}{\alpha}$ и ще го наричаме *частно* на β и α. Следователно

$$\frac{(c, d)}{(a, b)}=\left(\frac{ac+bd}{a^2+b^2}, \frac{ad-bc}{a^2+b^2}\right), \tag{5}$$

където $(a, b)\neq(0, 0)$.

Наредената двойка $\epsilon=(1, 0)$ е единствен елемент от C, за

който $\alpha\varepsilon=\alpha$ при всяко $\alpha\in C$ и поради това $\varepsilon=(1, 0)$ се нарича *единичен* елемент на C.

Ако $\alpha\neq\omega$, единственото решение на уравнението $\alpha x=\varepsilon$ се нарича *обратен* елемент на α и се бележи с α^{-1}.

Определение 1. Множеството C от наредените двойки реални числа с дефинираните операции събиране (1) и умножение (2) се нарича *множество на комплексните числа*, а всеки елемент на C се нарича *комплексно число.*

На реалното число a да съпоставим комплексното число $(a, 0)$. Тогава ако $a, b\in R$, то на реалните числа $a+b$, $a-b$ и ab ще съответствуват комплексните числа $(a+b, 0)=(a, 0)+(b, 0)$, $(a-b, 0)=(a, 0)-(b, 0)$ и $(ab, 0)=(a, 0).(b, 0)$. В случая, когато $b\neq 0$, на реалното число $\frac{a}{b}$ ще съответствува комплексното число $\left(\frac{a}{b}, 0\right)=\frac{(a, 0)}{(b, 0)}$. Поради това ние отъждествяваме реалното число a с комплексното число $(a, 0)$, т. е. ще считаме, че $a=(a, 0)$. Сега вече множеството R на реалните числа е подмножество на множеството C на комплексните числа и операциите в C над елементи от R съвпадат с операциите над реалните числа. Елементът (0, 1) от C ще означаваме с i и ще го наричаме *имагинерна единица*, а поради това, че числото 0 се отъждествява с $\omega=(0, 0)$, комплексното число (0, 0) ще означаваме вече с 0. Тъй като $i^2=(-1, 0)$, т. е. $i^2=-1$, комплексното число i е решение на уравнението $x^2+1=0$, с което постигнахме основната цел, която си бяхме поставили.

Поради отъждествяването, което направихме, на реалното число a с комплексното число от вида $(a, 0)$, то

$$(a, b)=(a, 0)+(0, b)=(a, 0)+(b, 0).(0, 1)=a+bi.$$

Както лесно се вижда, записването на комплексното число (a, b) във вида $a+bi$ е единствено. Това записване се нарича представяне на комплексното число в *алгебричен вид.*

Сега равенствата (1) и (2) придобиват съответно вида

$$(1') \qquad (a+bi)+(c+di)=(a+c)+(b+d)i,$$

$$(2') \qquad (a+bi).(c+di)=(ac-bd)+(ad+bc)i.$$

Числата a и b $(a, b\in R)$ се наричат съответно *реална* и *имагинерна* част на комплексното число $\alpha=a+bi$ и се означават с $a=\mathrm{Re}\alpha$ и $b=\mathrm{Im}\alpha$.

Ако $\alpha=a+bi$ е произволно комплексно число, то комплексното число $\bar{\alpha}=a-bi=(a, -b)$ се нарича *конюговано* или *комплексно-спрегнато* на α. Следователно $\mathrm{Re}\alpha=\mathrm{Re}\,\bar{\alpha}$ и $\mathrm{Im}\,\alpha=-\mathrm{Im}\,\bar{\alpha}$. Непосредствено се проверяват следните равенства:

$$\alpha+\bar{\alpha}=2\mathrm{Re}\,\alpha,$$

$$\alpha-\bar{\alpha}=2(\mathrm{Im}\,\alpha)i,$$

$$\alpha\bar{\alpha}=a^2+b^2=(\mathrm{Re}\,\alpha)^2+(\mathrm{Im}\,\alpha)^2.$$

Очевидно е, че числото α е реално тогава и само тогава, когато $\alpha=\bar{\alpha}$.

Ако $\alpha=a+bi$ и $\beta=c+di$ са две произволни комплексни числа и $\alpha\neq 0$, формулата (5) можем да получим със следното умножение:

$$\frac{\beta}{\alpha}=\frac{\beta\bar{\alpha}}{\alpha\bar{\alpha}}=\frac{(c+di)(a-bi)}{(a+bi)(a-bi)}=\frac{ac+bd}{a^2+b^2}+\frac{ad-bc}{a^2+b^2}i.$$

С непосредствена проверка се доказват и равенствата

$$\overline{(\alpha\pm\beta)}=\bar{\alpha}\pm\bar{\beta},$$

$$\overline{\alpha\beta}=\bar{\alpha}.\bar{\beta}, \tag{6}$$

$$\overline{\left(\frac{\alpha}{\beta}\right)}=\frac{\bar{\alpha}}{\bar{\beta}},$$

където α и β са произволни комплексни числа.

Ако числото $z=f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ се получава от комплексните числа $\alpha_1, \alpha_2, \ldots, \alpha_n$ само с операциите събиране, изваждане, умножение и деление и в израза $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ заменим α_k с неговото комплексно спрегнато $\bar{\alpha}_k$ $(k=1, 2, \ldots, n)$, от формулите (6) следва, че полученото число ще бъде комплексно спрегнатото $\bar{z}$ на z, т. е. $\bar{z}=f(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n)$.

Множествата **Z**, **Q**, **R** и **C** съответно на целите, рационалните, реалните и комплексните числа относно събирането и умножението имат много общи свойства, а именно свойствата 1) —8), посочени по-горе. Всяко числово множество, което притежава тези осем свойства, се нарича *числов пръстен*. Може да се покаже, че непразното множество S от числа е числов пръстен тогава и само тогава, когато за всеки две числа a и b (съвпадащи или не) от S разликата $a-b$ и произведението им ab се съдържат също в S. Но пръстенът **Z** на целите числа се различава от пръстените **Q**, **R** и **C** по това, че в него невинаги е възможно деление на различно от нула число. Всеки числов пръстен S, който съдържа поне едно ненулево число и в който за всеки две числа a и b $(b\neq 0)$ от S частното $\frac{a}{b}$ е също от S, се нарича *числово поле*. Числови полета са **Q**, **R** и **C**, но числовият пръстен **Z** не е числово поле. Освен това не е трудно да се съобрази, че множеството **N** на естествените числа не е числов пръстен.

За всяко комплексно число α по определение полагаме $\alpha^0=1$. Също така за всяко естествено число n полагаме

$$\alpha^n=\alpha.\alpha\ldots\alpha\ (n \text{ множителя}),$$
$$\beta^{-n}=(\beta^n)^{-1}=(\beta^{-1})^n\ (0\neq\beta\in\mathbf{C}).$$

За степените на комплексни числа лесно се доказват следните равенства:

a) $$(\alpha . \beta)^n = \alpha^n . \beta^n;$$

b) $$\left(\frac{\alpha}{b}\right)^n = \frac{\alpha^n}{\beta^n};$$

c) $$\alpha^n . \alpha^m = \alpha^{n+m};$$

d) $$(\alpha^n)^m = \alpha^{nm},$$

където n и m са произволни цели числа.

§ 2. Тригонометрична форма на комплексните числа

Ако в равнината въведем правоъгълна координатна система Oxy, то на всяка точка α от равнината еднозначно съответствува наредената двойка (a, b) от реални числа, където a е абсцисата на α, а b е ординатата на α. Обратно, на всяка наредена двойка (a, b), $a, b \in \mathbf{R}$, отговаря точно една точка α от равнината с координати a и b. По такъв начин получаваме взаимно еднозначно съответствие между множеството от комплексните числа и точките на равнината: ако α има координати a и b, то тя съответствува на комплексното число $(a, b) = a + bi$. Благодарение на това съответствие можем да отъждествим всяко комплексно число със съответствуващата му точка от равнината и да я означим със същата буква. Равнината Oxy (с посоченото отъждествяване на точките с комплексните числа) се нарича комплексна равнина.

Нека $\alpha = (a, b)$ е произволна точка от комплексната равнина и ρ — дължината на отсечката $O\alpha$. Да означим с φ ъгъла между положителния лъч на абсцисната ос и лъча $\overrightarrow{O\alpha}$, измерен в посока обратна на часовниковата стрелка. Тогава

$$\begin{aligned} &a = \rho \cos\varphi, \quad b = \rho \sin\varphi, \\ &\alpha = \rho(\cos\varphi + i\sin\varphi), \quad \rho = \sqrt{a^2 + b^2}. \end{aligned} \tag{1}$$

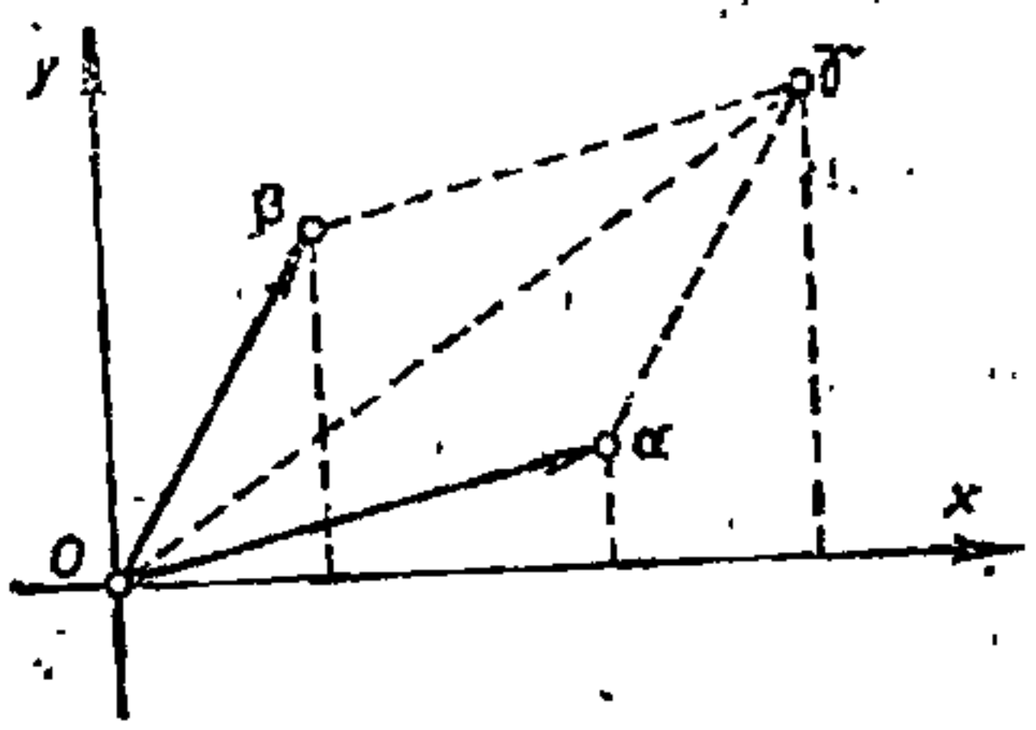
Записването на едно комплексно число α във вида (1) се нарича негов *тригонометричен вид*, неотрицателното реално число ρ — *модул* на α, а φ — *аргумент* на α. Модулът на α се означава с $|\alpha|$, а аргументът — с $\arg\alpha$. Трябва да отбележим, че докато модулът $\rho = |\alpha| = \sqrt{a^2 + b^2}$ на α е еднозначно определен, то аргументът на α може да се вземе с точност до целократно на 2π, тъй като за всяко цяло число k комплексните числа $\rho(\cos\varphi + i\sin\varphi)$ и $\rho[\cos(\varphi + 2k\pi) + i\sin(\varphi + 2k\pi)]$ съвпадат. Затова е вярно следното

Твърдение 3. *Комплексните числа* $\alpha = \rho(\cos\varphi + i\sin\varphi)$ *и* $\beta = \sigma(\cos\psi + i\sin\psi)$ *съвпадат тогава и само тогава, когато* $\rho = \sigma$ *и* $\varphi - \psi = 2k\pi$ *за някое цяло число* k.

Геометричната интерпретация на комплексните числа ни позволява да онагледим геометрично операциите събиране и изваждане. Именно сумата $\gamma = \alpha + \beta$ се получава като четвърти връх на успоредника, две от страните на който са отсечките $O\alpha$ и $O\beta$ (черт. 1).

Наистина абсцисата и ординатата на този връх са равни съответно на сумите от абсцисите и ординатите на α и β.

За да получим разликата $\delta=\alpha-\beta$, достатъчно е да вземем под внимание, че $\alpha=\delta+\beta$, т. е. δ е четвъртият връх на успоредника, две от страните на който са отсечките $O\beta$ и $\alpha\beta$.



Черт. 1

Геометричното онагледяване на умножението и делението на комплексните числа също се получава лесно с помощта на тригонометричната им форма.

Нека $\alpha=\rho(\cos\varphi+i\sin\varphi)$ и $\beta=\sigma(\cos\psi+i\sin\psi)$.

Тогава

$$\alpha\beta=\rho\sigma[(\cos\varphi\cos\psi-\sin\varphi\sin\psi)+i(\cos\varphi\sin\psi+\cos\psi\sin\varphi)]=$$

$$=\rho\sigma[\cos(\varphi+\psi)+i\sin(\varphi+\psi)].$$

Следователно при умножение на две комплексни числа модулите им се умножават, а аргументите им се събират.

Нека $\beta\neq 0$ и $\delta=\frac{\alpha}{\beta}$ има тригонометричен вид

$$\delta=\tau(\cos\xi+i\sin\xi).$$

Тогава $\alpha=\beta\delta$ и затова

$$\rho(\cos\varphi+i\sin\varphi)=\sigma\tau[\cos(\psi+\xi)+i\sin(\psi+\xi)].$$

Оттук съгласно твърдение 3 имаме

$$\tau=\frac{\rho}{\sigma},\ \xi=\varphi-\psi+2k\pi.$$

Това показва, че при делене на две комплексни числа модулите се делят, а аргументите им се изваждат.

С помощта на тригонометричната форма на комплексните числа ще докажем следната теорема за модулите.

Теорема 1. *Ако α и β са две произволни комплексни числа, то*

(2) $$||\alpha|-|\beta|| \leqq |\alpha+\beta| \leqq |\alpha|+|\beta|.$$

Равенство вляво можем да имаме тогава и само тогава, когато $\arg\alpha=\arg\beta+\pi$, *а вдясно равенство се достига тогава и само тогава, когато* $\arg\alpha=\arg\beta$.

Доказателство. Нека $\alpha=\rho(\cos\varphi+i\sin\varphi)$, а $\beta=\sigma(\cos\psi+i\sin\psi)$. Тогава

$$|\alpha+\beta|^2=(\rho\cos\varphi+\sigma\cos\psi)^2+(\rho\sin\varphi+\sigma\sin\psi)^2=$$
$$=\rho^2+\sigma^2+2\rho\sigma\cos(\varphi-\psi).$$

Тъй като $\cos(\varphi-\psi)$ се изменя между -1 и 1, то при постоянни ρ и σ най-голяма стойност на $|\alpha+\beta|^2$ ще имаме при $\cos(\varphi-\psi)=+1$, т. е. когато $\varphi=\psi+2k\pi$, а най-малка — при $\cos(\varphi-\psi)=-1$, т. е. при $\varphi=\psi+\pi+2k\pi$. Следователно

$$|\alpha+\beta|^2 \leqq \rho^2+\sigma^2+2\rho\sigma=(\rho+\sigma)^2,$$
$$|\alpha+\beta|^2 \geqq \rho^2+\sigma^2-2\rho\sigma=(\rho-\sigma)^2.$$

При това първото неравенство се превръща в равенство само ако $\arg\alpha=\arg\beta$, а второто — при $\arg\alpha=\arg\beta+\pi$. От получените неравенства непосредствено следва, че са изпълнени неравенствата (4).

§ 3. Степенуване и коренуване на комплексни числа

В предишния параграф беше показано, че при умножаване на две комплексни числа модулите се умножават, а аргументите се събират. Не е трудно по индукция да се докаже, че същото правило е в сила и за произволен брой множители, т. е. за произволно естествено число n е вярно равенството

(1) $$\prod_{k=1}^{n}\rho_k(\cos\varphi_k+i\sin\varphi_k)=\sigma(\cos\psi+i\sin\psi),$$

където $\sigma=\rho_1\rho_2\ldots\rho_n$, а $\psi=\varphi_1+\varphi_2+\ldots+\varphi_n$. Ако всички множители в (1) са равни на $\alpha=\rho(\cos\varphi+i\sin\varphi)$, се получава формулата

(2) $$[\rho(\cos\varphi+i\sin\varphi)]^n=\rho^n(\cos n\varphi+i\sin n\varphi),$$

известна под името *формула на Моавър* за степенуване на комплексни числа.

Очевидно е, че при $\alpha\neq 0$ формула (2) остава вярна и когато $n=0$. Ще докажем, че тази формула е валидна и при произволни отрицателни стойности на n и $\alpha\neq 0$. Наистина нека $n=-m$, $m\in N$. Тогава

$$[\rho(\cos\varphi+i\sin\varphi)]^n=\frac{1}{[\rho(\cos\varphi+i\sin\varphi)]^m}=\frac{\cos 0+i\sin 0}{\rho^m(\cos m\varphi+i\sin m\varphi)}=$$
$$=\rho^{-m}[\cos(-m\varphi)+i\sin(-m\varphi)]=\rho^n(\cos n\varphi+i\sin n\varphi).$$

Да разгледаме сега въпроса за коренуване на комплекени

числа. Всяко комилексно число, което е решение на биномното уравнение $x^n=\alpha$ ($\alpha\in\mathbf{C}$, $n\in\mathbf{N}$), се нарича *n-ти корен на комплексното число* α и се означава с $\sqrt[n]{\alpha}$.

Ако е необходимо да извлечем квадратен корен от числото $a+bi$ и да търсим стойностите му във вида $x+yi$, чрез повдигане в квадрат на равенството $\sqrt{a+bi}=x+yi$ стигаме до извода, че x и y трябва да се определят от системата

$$\begin{cases} x^2-y^2=a \\ 2xy=b, \end{cases}$$

откъдето намираме

$$x=\pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}},\quad y=\pm\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}.$$

Като вземем под внимание, че знакът на произведението xy съвпада със знака на b, то в изразите за x и y избираме еднакви знаци, ако $b>0$, и противоположни, когато $b<0$. По такъв начин за $\sqrt{a+bi}$ получаваме две стойности.

При намиране на $\sqrt[n]{\alpha}$ ($\alpha\in\mathbf{C}$), където $n>2$, е по-удобно да се използува тригонометричната форма на α.

Теорема 2. *Ако α е различно от нула комплексно число, а n е произволно естествено число, то съществуват точно n на брой различни комплексни числа, които са n-ти корени на α. Ако $\alpha=\rho(\cos\varphi+i\sin\varphi)$, то всички стойности на $\sqrt[n]{\alpha}$ са числата*

$$\beta_k=\sqrt[n]{\rho}\left(\cos\frac{\varphi+2k\pi}{n}+i\sin\frac{\varphi+2k\pi}{n}\right),$$

където $k=0, 1, 2, \ldots, n-1$, а $\sqrt[n]{\rho}$ е аритметичен n-ти корен от положително число ρ.

Доказателство. Непосредствено от формулата на Моавър (2) следва, че $\beta_k^n=\alpha$, т. е. посочените числа β_k са n-ти корени от α. Освен това $\beta_0, \beta_1, \ldots, \beta_{n-1}$ са различни, понеже всяко от тях има аргумент, който е с $\frac{2\pi}{n}$ по-голям от аргумента на предхождащото го число и броят им е n.

Нека числото $\beta=\sigma(\cos\psi+i\sin\psi)$ е произволен n-ти корен на α, т. е. $\beta^n=\alpha$. Тогава

$$\sigma^n(\cos n\psi+i\sin n\psi)=\rho(\cos\varphi+i\sin\varphi),$$

което показва, че са изпълнени равенствата $\sigma^n=\rho$ и $n\psi-\varphi=2\pi s$ ($s\in\mathbf{Z}$). Следователно

$$\sigma=\sqrt[n]{\rho},\quad \psi=\frac{\varphi+2\pi s}{n}.$$

Да означим с q и r съответно непълното частно и остатъка от делението на s с n, т. е. $s=qn+r$, където $0\leqq r<n$. Тогава

$$\beta=\sqrt[n]{\rho}\left[\cos\left(\frac{\varphi+2\pi r}{n}+2\pi q\right)+i\sin\left(\frac{\varphi+2\pi r}{n}+2\pi q\right)\right]=\beta_r,$$

с което теоремата е доказана.

Нека $\frac{m}{n}$ $(n>0)$ е произволно рационално число. Тогава можем да обединим формулата на Моавър с твърдението на теорема 2 в следната формула

$$[\rho(\cos\varphi+i\sin\varphi)]^{\frac{m}{n}}=\rho^{\frac{m}{n}}\left(\cos\frac{m\varphi+2k\pi}{n}+i\sin\frac{m\varphi+2k\pi}{n}\right),$$

където $k=0, 1,\ldots, n-1$.

Очевидно числото 0 е единствен корен n-ти от 0, тъй като уравнението $x^n=0$ има единствено решение $x=0$.

§ 4. Корени на единицата

Особен интерес представляват n-тите корени $(n\geqq 1)$ от числото 1, които се наричат още *корени на единицата* от n-та степен. Както показахме в предишния параграф, тези корени са n на брой и поради равенството $1=\cos 0+i\sin 0$ те се определят по формулата

$$\varepsilon_k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}\quad(k=0, 1, 2,\ldots, n-1). \tag{1}$$

Множеството от всички n-ти корени на 1 ще бележим с $C(n)$ т. е. $C(n)=\{\varepsilon_0, \varepsilon_1,\ldots, \varepsilon_{n-1}\}$.

Твърдение 4. *Нека ξ и η са два произволни n-ти корена на единицата. Тогава ξ^{-1} и $\xi\eta$ са също n-ти корени на единицата.*

Наистина $(\xi^{-1})^n=(\xi^n)^{-1}=1^{-1}=1$ и $(\xi\eta)^n=\xi^n\eta^n=1$, т. е. ξ^{-1}, $\xi\eta\in C(n)$.

Важността на n-тите корени от единицата може да се обясни в частност с това, че с тяхна помощ е удобно да се определят n-тите корени от произволно комплексно число α. Действително нека β е един произволен n-ти корен от α, а ε е произволен n-ти корен на единицата. Тогава $(\beta\varepsilon)^n=\beta^n\varepsilon^n=\alpha\cdot 1=\alpha$, т. е. $\beta\varepsilon$ е n-ти корен от α. Затова числата $\beta\varepsilon_0, \beta\varepsilon_1,\ldots, \beta\varepsilon_{n-1}$ са n-ти корени от α. Но тези числа са различни и са n на брой. Следователно те са всичките n-ти корени от α.

Определение 2. n-тият корен ε на единицата се нарича *примитивен*, ако той не е корен на единицата от по-ниска степен от n, т. е. ако $\varepsilon^n=1$ и $\varepsilon^m\neq 1$ за всяко m, за което $0<m<n$.

За всяко естествено число n съществува поне един примитивен n-ти корен на единицата. Например $\varepsilon_1=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ е

такъв корен, понеже от (1) и формулата на Моавър следва $\varepsilon_1^n = 1$, но $\varepsilon_1^k = \varepsilon_k \neq 1$ за $k = 1, 2, \ldots, n-1$.

Следващото твърдение би могло да се вземе за определение на примитивен корен на единицата.

Твърдение 5. *n-тият корен* ε *на единицата е примитивен тогава и само тогава, когато неговите степени* $\varepsilon^0, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}$ *са различни, т. е. с тях се изчерпват всички n-ти корени на единицата.*

Доказателство. Ако ε е примитивен n-ти корен на единицата и $\varepsilon^k = \varepsilon^l$ при $0 \leqq k < l \leqq n-1$, то $\varepsilon^{l-k} = 1$ и $0 < l-k < n$, което е противоречие. Обратно, ако посочените степени на n-тия корен ε на единицата са различни, то очевидно ε е примитивен n-ти корен на единицата.

Нека ε е n-ти корен на единицата и n дели цялото число m, т. е. $m = nq$. Тогава $\varepsilon^m = (\varepsilon^n)^q = 1$ и затова ε е и m-ти корен от единицата. Следователно можем да говорим изобщо за корени на единицата. Ако η е произволен корен на единицата, то най-малкото естествено число s, за което $\eta^s = 1$, се нарича *показател* на η. Очевидно η има показател s тогава и само тогава, когато η е примитивен s-ти корен на единицата.

Лема 1. *Ако* ε *е примитивен n-ти корен на единицата, равенството* $\varepsilon^m = 1$ $(m \in Z)$ *е изпълнено тогава и само тогава, когато* n/m*.*

Доказателство. Нека е изпълнено равенството $\varepsilon^m = 1$ и $m = nq + r$ $(0 \leqq r < n)$. Тогава по определение 8 равенствата

$$1 = \varepsilon^m = \varepsilon^{nq+r} = (\varepsilon^n)^q \cdot \varepsilon^r = \varepsilon^r$$

са изпълнени точно тогава, когато $r = 0$, т. е. тогава и само тогава, когато n/m.

Следствие 1. *Нека* ε *е корен на единицата. Ако* $\varepsilon^m = 1$ *и* $m \in Z$*, то показателят на* ε *дели числото* m*.*

Въпросът за броя и намирането на всички примитивни n-ти корени на единицата се решава от следното твърдение.

Теорема 3. *Ако* ε *е примитивен n-ти корен на единицата, то* ε^k *е примитивен n-ти корен на единицата тогава и само тогава, когато целите числа* k *и* n *са взаимно прости.*

Доказателство. Нека ε^k е примитивен n-ти корен на единицата. Да допуснем, че най-големият общ делител $d = (n, k)$ на n и k е по-голям от 1. Тогава $n = n_1 d$, $k = k_1 d$ и

$$(\varepsilon^k)^{n_1} = \varepsilon^{k_1 d n_1} = (\varepsilon^n)^{k_1} = 1,$$

т. е. степен на числото ε^k със степенен показател $n_1 < n$ е равна на 1, което противоречи на предположението.

Обратно, нека $(k, n) = 1$. Ако допуснем, че ε^k е примитивен m-ти корен на единицата за $m < n$, то по лема 11 следва, че n/km. Понеже $(k, n) = 1$, то n/m, а това е противоречие.

Следствие 2. *Броят на примитивните n-ти корени на*

---

* Със символа n/m означаваме, че n *дели* m.

единицата е равен на броя на естествените числа, които са по-малки от n и са взаимно прости с n.

Този брой се означава с $\varphi(n)$. Така се получава числова функция $\varphi(n)$, която е известна като *функция на Ойлер* или *индикатор* на n. Тази функция играе важна роля в теорията на числата.

Да разгледаме множеството $C(4)=\{1, -1, i, -i\}$ от корените на единицата от степен 4. Сред тях i и $-i$ са примитивни от 4-а степен, -1 е примитивен от 2-ра степен, а 1 е примитивен от първа степен.

Ако p е просто число, то примитивните p-ти корени на единицата са $\varphi(p)=p-1$ на брой, т. е. всеки различен от 1 p-ти корен на единицата е примитивен p-ти корен.

ГЛАВА II

ПОЛИНОМИ С ЧИСЛОВИ КОЕФИЦИЕНТИ И ТЕХНИТЕ КОРЕНИ

§ 1. Операции над полиноми

Нека x е променлива. Ще считаме, че нулевата степен x^0 на променливата x е равна на числото едно.

Формален израз $f(x)$ от вида

$$(1) \qquad f(x)=a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1}+a_nx^n,$$

където n е произволно цяло неотрицателно число, а $a_0, a_1, \ldots, a_n$ са фиксирани комплексни числа, се нарича *полином* с коефициенти $a_0, a_1, \ldots, a_n$.

Коефициентът a_0 на полинома $f(x)$ се нарича *свободен член* на $f(x)$ и се разглежда като коефициент пред нулевата степен $x^0=1$ на x.

От определението на полином следва, че комплексните числа могат да се разглеждат като полиноми от вида cx^0 $(c \in C)$.

По определение ще считаме, че полиномът $f(x)$ е равен на полинома

$$(2) \qquad g(x)=b_0+b_1x+b_2x^2+\ldots+b_{m-1}x^{m-1}+b_mx^m,$$

(което ще записваме $f(x)=g(x)$) тогава и само тогава, когато са изпълнени следните условия:

а) ако $a_k \neq 0$, то $k \leqq m$ и $a_k=b_k$;

б) ако $b_l \neq 0$, то $l \leqq n$ и $b_l=a_l$.

С други думи, два полинома са равни точно тогава, когато са равни различните им от нула коефициенти пред еднаквите степени на x.

По този начин всеки два полинома с нулеви коефициенти са равни и съвпадат с числото нула, разглеждано като полином. Този полином ще наричаме *нулев полином* и ще го бележим с 0.

Ако поне един от коефициентите на полинома $f(x)$ е различен от нула, то $f(x)$ не съвпада с нулевия полином и ние ще казваме, че $f(x)$ е *ненулев полином*. Най-високата степен на променливата x, която участвува с ненулев коефициент в записването (1) на полинома $f(x)$, се нарича *степен* на полинома $f(x)$ и се бележи с $\deg f(x)$. Само на нулевия полином засега не приписваме никаква степен.

Очевидно е, че един полином $g(x)$ има нулева степен тогава и само тогава, когато свободният му член е различен от нула, а останалите му коефициенти са равни на нула. Затова различните от нула числа и само те са полиноми от нулева степен.

Ако степента на полинома $f(x)$ е равна на n, то коефициентът a_n пред x^n в записването на $f(x)$ е последният различен от нула коефициент и се нарича *старши коефициент* на $f(x)$, а $a_n x^n$ се нарича *старши член* на полинома $f(x)$.

Множеството от всички полиноми с комплексни числови коефициенти ще бележим с $\mathbf{C}[x]$.

Тук трябва да отбележим, че полиномите с числови коефициенти можем да разглеждаме и от друга гледна точка. Полиномът $f(x)$ може да се тълкува и като функция, която е определена върху множеството $\mathbf{C}$ от комплексните числа, приема функционалните си стойности в $\mathbf{C}$ и която може да се представи във вида (1). В математическия анализ две такива функции $f(x)$ и $g(x)$ се считат за *равни*, ако за всяко комплексно число c те приемат едни и същи функционални стойности, т. е. $f(c)=g(c)$. Веднага възниква въпросът, дали два различни (в приетия от нас формално алгебричен смисъл) полинома могат да са равни като функции. На този въпрос ще отговорим по-нататък. Засега само ще отбележим, че тези два подхода на разглеждане на числовите полиноми съвпадат.

В множеството $\mathbf{C}[x]$ на всички полиноми с комплексни коефициенти ще въведем операции *умножение* и *събиране*. Нека $f(x)$ и $g(x)$ са полиномите от (1) и (2). *Произведение* на полиномите $f(x)$ и $g(x)$ се нарича полиномът

$$f(x)\,g(x)=d_0+d_1x+d_2x^2+\ldots+d_{n+m}\,x^{n+m},$$

където коефициентите d_i се определят по формулите

$$d_i=a_0b_i+a_1b_{i-1}+\ldots+a_{i-1}b_1+a_ib_0 \quad (i=0,\ 1,\ldots,\ m+n),$$

в които при $j>n$ считаме $a_j=0$ и при $j>m$ считаме $b_j=0$. В частност изпълнено е равенството $d_{n+m}=a_nb_m$. Ако $n=\deg f(x)$, а $m=\deg g(x)$, то $d_{n+m}=a_n\,b_m\neq 0$. Затова произведението на два ненулеви полинома е ненулев полином и неговата степен е равна на сумата от степените на множителите. Ако поне един от множителите $f(x)$ и $g(x)$ е равен на нулевия полином, произведението $f(x)\,g(x)$ е също равно на нулевия полином.

За да избегнем увеличаването на обема на записване и говорене, произтичащо от факта, че на нулевия полином не сме приписали степен, ние ще припишем на този полином степен, равна на символа $-\infty$ (четем „минус безкрайност“). Ще считаме, че $-\infty$ може да сравняваме с всяко число n и че $-\infty<n$. Освен това полагаме $(-\infty)+(-\infty)=-\infty$ и $-\infty+n=n+(-\infty)=-\infty$ за всяко цяло число n. *Не трябва да се влага в символа* $-\infty$ *повече смисъл от този, който сега му се приписва.* В удобството от въвеждането на такава степен на нулевия полином ще имаме възможност да се убедим по-нататък.

Тъй като прибавянето на членове с нулеви коефициенти в записването на един полином не изменя самия полином, то полиномите $f(x)$ и $g(x)$ могат да се представят като суми на еднакъв брой членове, т. е.

$$f(x)=\sum_{i=0}^{r} a_i x^i,\ g(x)=\sum_{i=0}^{r} b_i x^i,$$

където $r=\max\{m, n\}$.

Сума на полиномите $f(x)$ и $g(x)$ се нарича полиномът, коефициентите на който са суми от съответните коефициенти на $f(x)$ и $g(x)$, т. е.

$$f(x)+g(x)=\sum_{i=0}^{r} (a_i+b_i)\, x^i.$$

Очевидно е, че когато степените на два полинома $f(x)$ и $g(x)$ са равни и техните старши коефициенти са противоположни, то степента на сумата е строго по-малка от степента на $f(x)$ и $g(x)$. Когато степените на събираемите са различни или когато тези степени са равни, но старшите коефициенти на $f(x)$ и $g(x)$ не са противоположни, степента на сумата $f(x)+g(x)$ е равна на: $\max\{\deg f(x), \deg g(x)\}$.

Следователно в сила е следното

Твърдение 1. *Произведението на всеки два полинома $f(x)$ и $g(x)$ е полином от степен, равна на сумата от степените на $f(x)$ и $g(x)$, а сумата $f(x)+g(x)$ е полином, степента на който не е по-голяма от* $\max\{\deg f(x), \deg g(x)\}$.

Непосредствено от определенията на събирането и умножението на полиноми се получават следните свойства на тези операции:

1) $f(x)+g(x)=g(x)+f(x)$ — *комутативност на събирането*;

2) $[f(x)+g(x)]+h(x)=f(x)+[g(x)+h(x)]$ — *асоциативност на събирането*;

3) $f(x)+0=f(x)$, където 0 е нулевият полином;

4) $f(x)g(x)=g(x)f(x)$ — *комутативност на умножението*;

5) $[f(x)\,g(x)]\,h(x)=f(x)\,[g(x)\,h(x)]$ — *асоциативност на умножението*;

6) $[f(x)+g(x)]\,h(x)=f(x)\,h(x)+g(x)\,h(x)$ — *дистрибутивен закон*;

7) $f(x)\cdot 1=f(x)$, където 1 е числото едно, разглеждано като полином.

Горните равенства са изпълнени при произволни полиноми

$$f(x)=\sum_{r=0}^{k} a_r x^r,\ g(x)=\sum_{s=0}^{l} b_s x^s,\ h(x)=\sum_{t=0}^{m} c_t x^t.$$

За илюстрация ще докажем само асоциативността на умножението.

Нека

$$f(x)\,g(x)=\sum_{i=0}^{k+l} d_i x^i,\ g(x)h(x)=\sum_{j=0}^{l+m} e_j x^j.$$

където

$$d_i=\sum_{r+s=i} a_r b_s,\quad e_j=\sum_{s+t=j} b_s c_t.$$

Тогава коефициентът пред x^p $(p=0, 1, 2, \ldots, k+l+m)$ в полинома $f(x)[g(x)\,h(x)]$ ще бъде равен на числото

$$\sum_{r+i=p} a_r e_i=\sum_{r+j=p} a_r\left(\sum_{s+t=i} b_s c_t\right)=\sum_{r+s+t=p} a_r b_s c_t,$$

а в полинома $[f(x)\,g(x)]\,h(x)$ този коефициент ще бъде равен на числото

$$\sum_{i+t=p} d_i c_t=\sum_{i+t=p}\left(\sum_{r+s=i} a_r b_s\right)c_t=\sum_{r+s+t=p} a_r b_s c_t.$$

Следователно $f(x)[g(x)\,h(x)]$ и $[f(x)\,g(x)]\,h(x)$ имат еднакви коефициенти пред съответните степени на x и затова тези полиноми са равни.

Следващото твърдение показва, че е възможна винаги и операцията изваждане на полиноми.

Твърдение 2. *Ако $f(x)$ и $g(x)$ са два произволни полинома, то съществува един-единствен полином $h(x)$, за който е вярно равенството $f(x)+h(x)=g(x)$. Полиномът $h(x)$ се нарича разлика на полиномите $g(x)$ и $f(x)$ и се бележи с $h(x)=g(x)-f(x)$.*

Доказателство. Като вземем предвид посочената по-горе възможност да допълваме записа на един полином с нулеви членове, можем да считаме, че $f(x)$, $g(x)$ и $h(x)$ са от вида

$$f(x)=\sum_{i=0}^{n} a_i x^i,\quad g(x)=\sum_{i=0}^{n} b_i x^i,\quad h(x)=\sum_{i=0}^{n} c_i x^i.$$

Предстои ни да намерим коефициентите c_i на полинома $h(x)$ и да се убедим, че те са еднозначно определени. Тъй като

$$f(x)+h(x)=\sum_{i=0}^{n}(a_i+c_i)x^i=g(x),$$

то $a_i+c_i=b_i$ за всяко $i=0, 1, 2, \ldots, n$. Следователно $c_i=b_i-a_i$ за полинома $h(x)$ получаваме

$$h(x)=\sum_{i=0}^{n}(b_i-a_i)x^i,$$

т. е. само този полином би могъл да удовлетворява условието на твърдението. От друга страна, веднага се вижда, че полученият полином притежава желаното свойство, с което доказателството е завършено.

Следствие 1. *За всеки полином* $f(x)=a_0+a_1x+\ldots+a_nx^n$ *съществува точно един полином* $h(x)$, *за който е изпълнено равенството* $f(x)+h(x)=0$. Този полином се нарича *противоположен* на $f(x)$, бележи се с $-f(x)$ и

$$-f(x)=\sum_{i=0}^{n}(-a_i)\,x^i.$$

Както при целите числа, и при полиномите операцията деление невинаги е възможна. Наистина в сила е следното

Твърдение 3. *За полинома* $f(x)$ *съществува полином* $g(x)$ *със свойството* $f(x)\,g(x)=1$ *тогава и само тогава, когато* $f(x)$ *е число, различно от нула.*

Доказателство. Ако $g(x)$ съществува, то от равенството $f(x)g(x)=1$ следва, че е изпълнено равенството

$$\deg f(x)+\deg g(x)=\deg 1=0.$$

Следователно $\deg f(x)=\deg g(x)=0$, което показва, че $f(x)$ и $g(x)$ са различни от нула комплексни числа.

Обратно, ако $f(x)$ е различно от нула комплексно число, т. е. $f(x)=c\neq 0$, то $g(x)=c^{-1}$ е полином от нулева степен и $f(x)g(x)=1$.

Подобно на делимостта на целите числа в следващите два параграфа ще развием теория за делимост на полиномите.

§ 2. Деление на полиноми

Множеството $P\subset\mathbf{C}$ се нарича *числово поле*, ако то съдържа поне две различни числа и ако са изпълнени следните две условия: а) ако a и b са числа от P, то $a+b$, $a-b$ и ab са също числа от P; б) ако $a\neq 0$ и a се съдържа в P, то a^{-1} е число от P.

Множествата $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$ съответно на рационалните, реалните и комплексните числа са полета.

Множеството от всички полиноми с коефициенти от дадено числово поле P се бележи с $P[x]$. Лесно се вижда, че сумата, разликата и произведението на полиноми от $P[x]$ са полиноми с коефициенти от P, т. е. те са също полиноми от $P[x]$.

Ако $f(x)$ е полином от степен n с числови коефициенти, то често ще го записваме и с обратна номерация на коефициентите, а именно

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n. \tag{1}$$

Теорема 1. *Нека* $f(x)$ *и* $g(x)$ *са два полинома с коефициенти от числовото поле* P *и* $g(x)$ *е ненулев полином. Тогава съществуват еднозначно определени полиноми* $q(x)$ *и* $r(x)$ *с коефициенти от* P, *които удовлетворяват следните две условия:*

1) $f(x)=q(x)g(x)+r(x)$,

2) $\deg r(x)<\deg g(x)$.

Доказателство. Ако $\deg g(x)=m$, от условието $g(x)\neq 0$ следва, че $m\geqq 0$. Най-напред ще докажем съществуването на полиномите $q(x)$ и $r(x)$. Нека $f(x)$ има вида (1), а

$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_{m-1}x+b_m,\ b_0\neq 0.$$

Ако $\deg f(x)<\deg g(x)$, полагаме $q(x)=0$, $r(x)=f(x)$ и тези полиноми удовлетворяват условията на теоремата.

Да допуснем, че $n=\deg f(x)\geqq\deg g(x)$. Полагаме

$$f_1(x)=f(x)-\frac{a_0}{b_0}x^{n-m}g(x).$$

Тогава степента $\deg f_1(x)=n_1$ е строго по-малка от степента на $f(x)$, защото старшият член на $f(x)$ е равен на старшия член на полинома $\frac{a_0}{b_0}x^{n-m}g(x)$. Да предположим, че все още $n_1\geqq m$ и да означим с a_{01} старшия коефициент на $f_1(x)$. Полагаме

$$f_2(x)=f_1(x)-\frac{a_{01}}{b_0}x^{n_1-m}g(x).$$

Степента n_2 на $f_2(x)$ е строго по-малка от n_1. Ако $n_2\geqq m$, означаваме с a_{02} старшия коефициент на $f_2(x)$ и полагаме

$$f_3(x)=f_2(x)-\frac{a_{02}}{b_0}x^{n_2-m}g(x)$$

и т. н. Тъй като степените на полиномите $f_1(x)$, $f_2(x)$, . . . строго намаляват, след краен брой стъпки ще получим полином

$$f_k(x)=f_{k-1}(x)-\frac{a_{0,\,k-1}}{b_0}x^{n_{k-1}-m}g(x)$$

от степен $n_k<m$. Като съберем всички равенства за $f_1(x)$, $f_2(x)$ . . ., $f_k(x)$, ще получим

$$f_k(x)=\left(-\frac{a_0}{b_0}x^{n-m}-\frac{a_{01}}{b_0}x^{n_1-m}-\ldots-\frac{a_{0,\,k-1}}{b_0}x^{n_k-1-m}\right)g(x)+f(x).$$

Полагаме

$$q(x)=\frac{a_0}{b_0}x^{n-m}+\frac{a_{01}}{b_0}x^{n_1-m}+\ldots+\frac{a_{0,\,k-1}}{b_0}x^{n_{k-1}-m}$$

и $r(x)=f_k(x)$. Тогава $f(x)=q(x)g(x)+r(x)$ и $\deg r(x)=n_k<m$. Остава само да отбележим, че полиномите $f_1(x)$, $f_2(x)$, . . . , $f_k(x)$ са с коефициенти от полето P, защото са такива полиномите $f(x)$ и $g(x)$. Затова $r(x)$ и $q(x)$ са също с коефициенти от P.

Да допуснем, че съществува и друга двойка полиноми $q_1(x)$ и $r_1(x)$, които удовлетворяват условията на теоремата. Тогава ще имаме

$$f(x)=q(x)g(x)+r(x)=q_1(x)g(x)+r_1(x),$$

където $\deg r(x)<m$, $\deg r_1(x)<m$. Оттук следва равенството

$$[q(x)-q_1(x)]g(x)=r_1(x)-r(x).$$

Ако предположим, че $q(x)-q_1(x)\neq 0$, то

$$\deg[r_1(x)-r(x)]=\deg[q(x)-q_1(x)]+\deg g(x),$$

при което $\deg[q(x)-q_1(x)]\geqq 0$. Следователно ще бъде изпълнено неравенството

$$\deg[r_1(x)-r(x)]\geqq\deg g(x).$$

Но от твърдение 1 ще следва, че $\deg[r_1(x)-r(x)]<\deg g(x)$. Полученото противоречие показва, че $q(x)-q_1(x)=0$ и затова $r_1(x)-r(x)=0$, т. е. $q_1(x)=q(x)$ и $r_1(x)=r(x)$. Теоремата е доказана.

Да отбележим, че $q(x)$ се нарича непълно частно, а $r(x)$ — остатък от делението на полинома $f(x)$ с полинома $g(x)$.

Определение 1. Ще казваме, че полиномът $g(x)$ *дели* полинома $f(x)$ и ще записваме кратко този факт с $g(x)/f(x)$, ако съществува такъв полином $\varphi(x)$, че $f(x)=g(x)\varphi(x)$. Ако $g(x)/f(x)$, то $g(x)$ се нарича *делител* на полинома $f(x)$.

Твърдение 4. *Ненулевият полином $g(x)$ е делител на полинома $f(x)$ тогава и само тогава, когато остатъкът от делението на $f(x)$ с $g(x)$ е равен на нула.*

Действително нека $f(x)=q(x)g(x)+r(x)$, където $\deg r(x)<\deg g(x)$. Ако $r(x)=0$, то $f(x)=q(x)g(x)$ и затова $g(x)/f(x)$. Обратно, ако $g(x)/f(x)$ и $f(x)=\varphi(x)g(x)$, от единствеността на частното и остатъка следва, че $q(x)=\varphi(x)$ и $r(x)=0$.

Ще посочим някои основни свойства на делимостта на полиноми, които в бъдеще многократно ще използуваме:

1. *Ако $f(x)/g(x)$ и $g(x)/h(x)$, то $f(x)/h(x)$.*

Наистина от $g(x)=f(x)\varphi(x)$ и $h(x)=g(x)\psi(x)$ следва равенството $h(x)=f(x)[\varphi(x)\psi(x)]$, т. е. $f(x)/h(x)$.

2. *Ако $f(x)/g(x)$ и $f(x)/h(x)$, то $f(x)/[g(x)\pm h(x)]$.*

3. *Ако $f(x)/g(x)$ и $h(x)$ е произволен полином, то $f(x)$ дели произведението $g(x)h(x)$.*

4. *Ако c е произволно ненулево число, а $f(x)$ е полином, то $c/f(x)$.*

Наистина $f(x)=cg(x)$, където $g(x)=c^{-1}f(x)$.

5. *Ако $f(x)/g(x)$ и c е произволно различно от нула число, то $cf(x)/g(x)$.*

Наистина от $g(x)=f(x)\varphi(x)$ следва $g(x)=cf(x)[c^{-1}\varphi(x)]$ и затова $cf(x)/g(x)$.

6. *Ако $f(x)/g(x)$ и $\deg f(x)=\deg g(x)$, то $g(x)=cf(x)$, където c е число, различно от нула.*

Наистина нека $g(x)=\varphi(x)f(x)$. Тогава

$$\deg g(x)=\deg\varphi(x)+\deg f(x).$$

Но по условие $\deg g(x)=\deg f(x)$ и затова $\deg\varphi(x)=0$, т. е. $\varphi(x)$ е число, различно от нула.

7. *Ако $f(x)/g(x)$ и $g(x)/f(x)$, то $g(x)=cf(x)$, където c е ненулево число.*

Наистина от условията се получава съответно $\deg f(x)\leqq$

$\leqq \deg g(x)$ и $\deg g(x) \leqq \deg f(x)$, т. е. $\deg f(x) = \deg g(x)$. Тогава твърдението следва от свойство 6.

8. *Полиномът $f(x)$ се дели на нулевия полином тогава и само тогава, когато $f(x)=0$.*

§ 3. Най-голям общ делител на полиноми

Аналогия между делимостта на целите числа и делимостта на полиномите съществува и по отношение на понятието най-голям общ делител (кратко означение — НОД).

Нека $f_1(x), f_2(x), \ldots, f_n(x)$ $(n \geqq 1)$ са краен брой полиноми. Полиномът $f(x)$ се нарича *общ делител* на тези полиноми, ако $f(x)$ дели всеки от полиномите $f_1(x), \ldots, f_n(x)$. Ясно е, че сред общите делители на всяка система от полиноми се намират и ненулевите комплексни числа. Ако полиномите $f_1(x), \ldots, f_n(x)$ не притежават други общи делители освен ненулевите числа, казваме, че те са *взаимно прости*.

Определение 2. Ще казваме, че полиномът $d(x)$ е *най-голям общ делител (НОД)* на полиномите $f_1(x), f_2(x), \ldots, f_n(x)$, ако $d(x)$ е техен общ делител и $d(x)$ се дели на всеки друг общ делител на тези полиноми.

Лесно се проверява, че НОД на полиномите $f_1(x)=f_2(x)=\ldots=f_n(x)=0$ е полиномът $d(x)=0$. Действително всеки полином е делител на тези полиноми, но само нулевият полином се дели на всички техни общи делители. Оказва се, че НОД на няколко полинома е еднозначно определен само в този случай.

Лема 1. *Ако $d(x)$ е НОД на полиномите $f_1(x), \ldots, f_n(x)$, то полиномът $d_1(x)$ е техен НОД тогава и само тогава, когато $d_1(x)=c\,d(x)$, където c е комплексно число, различно от нула.*

Доказателство. Ако $d_1(x)$ е НОД на $f_1(x), \ldots, f_n(x)$, то $d_1(x)/d(x)$, защото $d_1(x)$ е общ делител, а $d(x)$ е НОД на дадените полиноми. По аналогични причини $d(x)/d_1(x)$ и следователно $d_1(x)=c\,d(x)$, където c е число, различно от нула.

Обратно, нека $d_1(x)=c\,d(x)$, където c е различно от нула число. Тъй като $d(x)$ дели всеки от дадените полиноми, то и $d_1(x)$ ще бъде техен общ делител. От друга страна, всеки делител на $d(x)$ е делител и на $d_1(x)$. Следователно $d_1(x)$ се дели на всеки общ делител на полиномите $f_1(x), \ldots, f_n(x)$ и значи $d_1(x)$ е НОД на тези полиноми. Лемата е доказана.

Един ненулев полином се нарича *нормиран*, ако неговият старши коефициент е равен на единица. Удобно е да приемем, че нулевият полином е също нормиран.

Теорема 2. *Всяка крайна система от полиноми $f_1(x), \ldots, f_n(x)$ с числови коефициенти притежава точно един нормиран НОД $d(x)$, който може да се запише във вида*

$$d(x)=u_1(x)f_1(x)+u_2(x)f_2(x)+\ldots+u_n(x)f_n(x),$$

където $u_i(x)$ *са полиноми. Ако полиномите* $f_1(x), \ldots, f_n(x)$ *са с коефициенти от числовото поле* P, *то* $d(x)$ *е полином с коефициенти от* P, *а полиномите* $u_1(x), \ldots, u_n(x)$ *могат да бъдат подбрани така, че да бъдат също с коефициенти от* P.

Доказателство. Единствеността на нормирания НОД на полиномите $f_1(x), \ldots, f_n(x)$ следва непосредствено от лема 1.

Ще докажем съществуването на нормирания НОД. Ще предполагаме, че полиномите са с коефициенти от числовото поле P (в частност P може да съвпада с $\mathbf{C}$).

Ако $f_1(x)=f_2(x)=\ldots=f_n(x)=0$, то $d(x)=0$ и полиномите $u_1(x), u_2(x), \ldots, u_n(x)$ могат да бъдат избрани по произволен начин. Затова ще предположим, че поне един от полиномите $f_1(x), f_2(x), \ldots, f_n(x)$ е ненулев. Да означим с M множеството на всички полиноми от вида

$$v_1(x) f_1(x)+v_2(x) f_2(x)+\ldots+v_n(x) f_n(x),$$

където $v_i(x)$ са произволни полиноми от $P[x]$. Тъй като

$$f_i(x)=0 \cdot f_1(x)+\ldots+1 \cdot f_i(x)+\ldots+0 \cdot f_n(x),$$

то $f_i(x) \in M$ и затова в M се съдържат ненулеви полиноми. Ясно е, че ако $f(x)$ и $g(x)$ са от M, то и $f(x) \pm g(x)$ е полином от M. Ако $\varphi(x) \in P[x]$, а $f(x) \in M$, то $\varphi(x) f(x)$ е също полином от M. Нека $d(x)$ е един ненулев нормиран полином от M от възможно най-ниска степен. Такъв полином съществува, защото множеството от всички степени на ненулевите полиноми от M е непразно подмножество на множеството от неотрицателните цели числа, а всяко такова множество съдържа най-малко число. Ще докажем, че $d(x)$ е търсеният НОД на полиномите $f_1(x), \ldots, f_n(x)$. Тъй като $d(x) \in M$, то

$$d(x)=u_1(x) f_1(x)+\ldots+u_n(x) f_n(x).$$

за някои полиноми $u_1(x), \ldots, u_n(x)$ от $P[x]$. Затова ако $\varphi(x)$ е общ делител на $f_1(x), \ldots, f_n(x)$, то $\varphi(x) / d(x)$. Остава да докажем само, че $d(x)$ е общ делител на полиномите $f_1(x), \ldots, f_n(x)$. За целта ще докажем, че $d(x)$ дели всеки полином от M, а тъй като $f_i(x)$ се съдържат в M, то с това доказателството ще бъде завършено.

Нека $f(x)$ е произволен полином от M и

$$f(x)=q(x) d(x)+r(x),$$

където $\deg r(x)<\deg d(x)$. Полиномът $r(x)$ се съдържа в M, защото $r(x)=f(x)-q(x) d(x)$, $f(x) \in M$ и $d(x) \in M$. Ако допуснем, че $r(x) \neq 0$, като нормираме полинома $r(x)$, ще получим нормиран ненулев полином от M от степен, по-малка от степента на $d(x)$, което е противоречие. Следователно $r(x)=0$ и $d(x) / f(x)$. Теоремата е доказана.

Единственият нормиран НОД на полиномите $f_1(x), f_2(x), \ldots, f_n(x)$ е прието да се бележи с $(f_1(x), f_2(x), \ldots, f_n(x))$.

Следствие 2. *Полиномите* $f_1(x), \ldots, f_n(x)$ *са взаимно прос-*

ти тогава и само тогава, когато съществуват такива полиноми $u_1(x), u_2(x), \ldots, u_n(x)$, *за които е изпълнено равенството*

$$u_1(x) f_1(x) + u_2(x) f_2(x) + \ldots + u_n(x) f_n(x) = 1.$$

Наистина последното равенство е равносилно на равенството $(f_1(x), f_2(x), \ldots, f_n(x)) = 1$.

С помощта на доказаните вече твърдения ще получим някои допълнителни важни свойства на полиномите, свързани с понятието делимост.

а) *Ако* $h(x) / f(x) g(x)$ *и* $(h(x), f(x)) = 1$, *то* $h(x)$ *дели полинома* $g(x)$.

Наистина съгласно теорема 2 съществуват такива полиноми $u(x)$ и $v(x)$, че $u(x) h(x) + v(x) f(x) = 1$. Умножаваме това равенство с $g(x)$ и получаваме

$$[u(x) g(x)] h(x) + v(x) [f(x) g(x)] = g(x).$$

Тъй като $h(x)$ дели всяко събираемо в лявата страна на последното равенство, то $h(x) / g(x)$.

б) *Ако* $(h(x), f(x)) = 1$ *и* $(h(x), g(x)) = 1$, *то* $(h(x), f(x) g(x)) = 1$.

Действително, тъй като

$$u(x) h(x) + v(x) f(x) = 1, \quad \varphi(x) h(x) + \psi(x) g(x) = 1$$

за някои полиноми $u(x)$, $v(x)$, $\varphi(x)$ и $\psi(x)$, то като умножим почленно тези равенства, получаваме

$$q(x) h(x) + p(x) [f(x) g(x)] = 1,$$

където

$$p(x) = v(x) \psi(x), \quad q(x) = u(x) \varphi(x) h(x) + u(x) \psi(x) g(x) + v(x) f(x) \varphi(x).$$

Тогава от теорема 2 следва $(h(x), f(x) g(x)) = 1$.

в) *Ако* $f(x) / h(x)$, $g(x) / h(x)$ *и* $(f(x), g(x)) = 1$, *то* $f(x) g(x) / h(x)$.

Наистина $h(x) = f(x) \varphi(x)$. Освен това $g(x) / f(x) \varphi(x)$ и $(g(x), f(x)) = 1$. По свойство а) имаме $g(x) / \varphi(x)$, т. е. $\varphi(x) = g(x) \psi(x)$. Но тогава $h(x) = f(x) g(x) \psi(x)$, т. е. $f(x) g(x) / h(x)$.

Лесно може да се докаже с метода на пълната математическа индукция, че посочените свойства остават в сила и за повече полиноми.

Ще покажем, че намирането на НОД на няколко полинома се свежда до намирането на НОД на два полинома.

Твърдение 5. *Нормираният НОД на полиномите* $f_1(x), \ldots, f_n(x)$ *е равен на нормирания НОД на полиномите* $h(x)$ *и* $f_n(x)$, *където* $h(x)$ *е нормираният НОД на полиномите* $f_1(x), f_2(x), \ldots, f_{n-1}(x)$.

Доказателство. Да положим $d(x) = (h(x), f_n(x))$. Очевидно $d(x) / f_i(x)$ за $i = 1, 2, \ldots, n$.

Нека $d_1(x)$ е произволен общ делител на $f_1(x), f_2(x), \ldots, f_n(x)$. Тогава $d_1(x) / h(x)$, защото $h(x) = (f_1(x), \ldots, f_{n-1}(x))$ и $d_1(x) / f_n(x)$. Но $d(x) = (h(x), f_n(x))$ и затова $d_1(x) / d(x)$. Тъй като

$d(x)$ е нормиран полином, то $d(x)=(f_1(x), f_2(x), \ldots, f_n(x))$.

Практическото намиране на НОД на два полинома $f(x)$ и $g(x)$ се извършва чрез алгоритъма на Евклид. За целта без ограничение на общността можем да считаме, че $g(x)\neq 0$ и че $\deg f(x)\geqq\deg g(x)$. Делим $f(x)$ на $g(x)$ и получаваме остатък $r_1(x)$. Ако $r_1(x)$ е различен от нула, делим $g(x)$ на $r_1(x)$ и получаваме остатък $r_2(x)$. Ако $r_2(x)\neq 0$, делим $r_1(x)$ на $r_2(x)$ и получаваме остатък $r_3(x)$ и т. н. Тъй като степените на получаваните остатъци строго намаляват, след краен брой стъпки ще получим остатък $r_{k+1}(x)=0$, т. е.

$$\begin{aligned}
f(x) &= g(x)\,q_1(x)+r_1(x),\\
g(x) &= r_1(x)q_2(x)+r_2(x),\\
r_1(x) &= r_2(x)\,q_3(x)+r_3(x),\\
&\cdots\cdots\cdots\cdots\cdots\\
r_{k-2}(x) &= r_{k-1}(x)q_k(x)+r_k(x),\\
r_{k-1}(x) &= r_k(x)q_{k+1}(x).
\end{aligned}$$

Тогава последният ненулев остатък $r_k(x)$ е НОД на $f(x)$ и $g(x)$. Наистина, тъй като $r_k(x)/r_{k-1}(x)$, от предпоследното равенство следва, че $r_k(x)/r_{k-2}(x)$, а от по-горното равенство заключаваме, че $r_k(x)/r_{k-3}(x)$. Като продължаваме така, стигаме до извода, че $r_k(x)/r_2(x)$ и $r_k(x)/r_1(x)$. Тогава от второто и първото равенство получаваме, че $r_k(x)$ дели съответно $f(x)$ и $g(x)$. Следователно $r_k(x)$ е общ делител на $f(x)$ и $g(x)$. Нека сега $d_1(x)$ е произволен общ делител на $f(x)$ и $g(x)$, т. е. $d_1(x)/f(x)$ и $d_1(x)/g(x)$. От първото равенство следва, че $d_1(x)/r_1(x)$, а от второто — $d_1(x)/r_2(x)$ и т. н. По такъв начин, като се движим от първото към последното равенство, стигаме до извода, че $d_1(x)/r_k(x)$. С това е доказано, че $r_k(x)$ е НОД на полиномите $f(x)$ и $g(x)$.

Определение 3. Полиномът $f(x)$ от положителна степен с коефициенти от числовото поле P се нарича *неразложим над* P, ако той не може да се представи като произведение на два полинома от положителни степени и с коефициенти от P. В противен случай $f(x)$ се нарича *разложим над* P.

Тук следва изрично да отбележим, че за полиномите от нулева степен и за нулевия полином понятията разложим и неразложим полином не се дефинират и не се разглеждат.

От примерите, които ще приведем, ще се убедим, че понятието неразложим полином зависи съществено от това, кое числово поле P се разглежда. Ясно е обаче, че ако $f(x)$ е разложим полином над P, а S е по-широко числово поле, т. е. $P\subseteq S$, то $f(x)$ е разложим и над S. Обратното невинаги е вярно, в което ще се убедим с конкретни примери.

Да напомним, че с $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$ бележим съответно полето на рационалните, реалните и комплексните числа. С $\mathbf{Q}(i)$ ще бележим множеството от всички комплексни числа $a+bi$, където a и

b са произволни рационални числа. С $\mathbf{Q}(\sqrt{2})$ ще бележим множеството от всички реални числа от вида $a+b\sqrt{2}$, където a и b са произволни рационални числа. Лесно се проверява, че $\mathbf{Q}(i)$ и $\mathbf{Q}(\sqrt{2})$ са числови полета, които съдържат $\mathbf{Q}$. Полето $\mathbf{Q}(i)$ се нарича поле на гаусовите числа.

Очевидно, че всеки полином с коефициенти от P и от степен единица е неразложим полином над P. Така например полиномът $x+\sqrt{2}$ е неразложим над всяко числово поле, което съдържа числото $\sqrt{2}$. За разложимост или неразложимост на $x+\sqrt{2}$ над полето $\mathbf{Q}$ на рационалните числа въобще не може да се говори, защото коефициентът $\sqrt{2}$ не е рационално число. Полиномът x^2-2 е разложим над полето $\mathbf{Q}(\sqrt{2})$, защото $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$, но е неразложим над по-малкото числово поле $\mathbf{Q}$. Наистина ако x^2-2 е разложим над $\mathbf{Q}$, то $x^2-2=(ax+b)(cx+d)$, където $a\neq 0$, $c\neq 0$ и $a, b, c, d\in Q$. Оттук ще следва, че полиномът x^2-2 има два рационални корена $x_1=-\frac{b}{a}$ и $x_2=-\frac{d}{c}$, което не е възможно, тъй като неговите корени са ирационалните числа $\sqrt{2}$ и $-\sqrt{2}$. По подобен начин се установява, че полиномът x^2+1 е неразложим над полетата $\mathbf{Q}$, $\mathbf{Q}(\sqrt{2})$ и $\mathbf{R}$. Но този полином е разложим над полето $\mathbf{Q}(i)$ (значи и над $\mathbf{C}$), защото

$$x^2+1=(x-i)(x+i),$$

където i е имагинерната единица и $\pm i\in\mathbf{Q}(i)$.

Някои други по-интересни резултати за разложимост на полиномите ще получим в § 7 и глава VI.

§ 4. Корени на полиномите. Многократни корени

Ако

(1) $$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n \quad (a_i\in\mathbf{C})$$

е произволен полином и c е комплексно число, то числото

$$f(c)=a_0c^n+a_1c^{n-1}+\ldots+a_{n-1}c+a_n$$

се нарича стойност на полинома $f(x)$ при $x=c$. Ако $\varphi(x)=f(x)+g(x)$ $\psi(x)=f(x)g(x)$, непосредствено се проверява, че $\varphi(c)=f(c)+g(c)$, $\psi(c)=f(c)\,g(c)$.

Комплексното число c се нарича *корен* (*нула*) на полинома $f(x)$, ако $f(c)=0$. В този случай се казва също, че c е решение (корен) на уравнението $f(x)=0$. Уравнения от вида

(2) $$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=0 \quad (a_i\in\mathbf{C})$$

се наричат алгебрични. Трябва да се прави разлика между понятието алгебрично уравнение и равенството между един полином и нулевия полином. Уравнението (2) предполага само, че то тряб-

ва да се реши, т. е. трябва да се намерят всички стойности на неизвестното x, които го удовлетворяват.

Ще покажем, че намирането на корените на едно алгебрично уравнение е тясно свързано с въпроса за делимост на полиноми.

Твърдение 6. *Остатъкът от деленето на полинома $f(x)$ с линейния полином $x-c$ ($c \in \mathbf{C}$) е равен на $f(c)$.*

Доказателство. Нека $q(x)$ и $r(x)$ са съответно непълното частно и остатък от деленето на $f(x)$ с $x-c$. Тогава

$$f(x)=q(x)(x-c)+r(x),\ \deg r(x)<1$$

и затова степента на $r(x)$ е нула или $-\infty$, т. е. $r(x)=r \in \mathbf{C}$. За да намерим числото r, полагаме $x=c$ в представянето за $f(x)$ и получаваме $r=f(c)$, което трябваше да се докаже.

Оттук получаваме следната важна теорема.

Теорема 3 (теорема на Безу). *Числото c е корен на полинома $f(x)$ тогава и само тогава, когато $x-c$ дели $f(x)$.*

Наистина полиномът $x-c$ дели $f(x)$ точно тогава, когато остатъкът $f(c)$ от деленето на $f(x)$ с $x-c$ е нула.

Тук следва да отбележим два особени случая: ако $f(x)$ е нулевият полином, всяко число е корен на $f(x)$, а ако $f(x)$ е полином от нулева степен, то $f(x)$ няма нито един корен.

От горните разглеждания се вижда, *че е целесъобразно да намерим един по-прост метод за деление на полинома $f(x)$ с линейния полином $x-c$, отколкото общия алгоритъм за деление на полиноми.* Такъв метод за пръв път е бил публикуван от английския математик Хорнер през 1819 г. и носи неговото име, но той е бил открит преди това от италианския лекар Паоло Руфини през 1804 г. Впрочем същият метод е бил известен на някои китайски математици още през XII в.

Нека $f(x)$ е полиномът (1) и

$$f(x)=(x-c)q(x)+r, \tag{3}$$

където $q(x)=b_0x^{n-1}+b_1x^{n-2}+\ldots+b_{n-2}x+b_{n-1}$. Като сравним коефициентите пред еднаквите степени на x в двете страни на равенството (3), ще получим $a_0=b_0$, $a_1=b_1-cb_0$, $a_2=b_2-cb_1$, $a_3=b_3-cb_2$, $\ldots$, $a_{n-1}=b_{n-1}-cb_{n-2}$, $a_n=r-cb_{n-1}$. Оттук следва, че $b_0=a_0$, $b_1=cb_0+a_1$, $b_2=cb_1+a_2$, $\ldots$, $b_{n-1}=cb_{n-2}+a_{n-1}$, $r=cb_{n-1}+a_n$, т. е. коефициентът b_k се получава чрез умножаване с c на предишния коефициент b_{k-1} и прибавяне към полученото произведение съответния коефициент a_k, при което $b_0=a_0$, а $b_n=r$. По този начин на пресмятане едновременно се получават коефициентите на частното $q(x)$ и стойността $r=f(c)$. Практически пресмятането се извършва чрез еднотипни действия и се подрежда по следната схема:

$$\begin{array}{c|cccccc} & a_0 & a_1 & a_2 & \ldots & a_{n-1} & a_n \\ \hline c & b_0 & b_1 & b_2 & \ldots & b_{n-1} & r=f(c) \end{array}$$

Производна (или *първа производна*) $f'(x)$ на полинома $f(x)$ от вида (1) се нарича полиномът

$$f'(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\ldots+2a_{n-2}x+a_{n-1}.$$

По определение производната на кое да е комплексно число е числото нула.

Производната на $f'(x)$ се нарича *втора производна* на полинома $f(x)$ и се бележи с $f''(x)$ и въобще *k-тата производна* $f^{(k)}(x)$ на $f(x)$ е първата производна на $f^{(k-1)}(x)$. Очевидно $f^{(n)}(x)=n(n-1)\ldots 2.1.a_0=n!a_0$ и затова $f^{(n+1)}(x)=f^{(n+2)}(x)=\ldots=0$.

Не е трудно да се докаже, че производната на полином, или, както се казва още, диференцирането, притежава следните свойства:

1) $[f(x)+g(x)]'=f'(x)+g'(x)$,
2) $[f(x)g(x)]'=f'(x)g(x)+f(x)g'(x)$.

Като следствие се получава *правилото за диференциране на степен:*

$$[f^m(x)]'=mf^{m-1}(x).f'(x). \tag{4}$$

Нека да отбележим, че посочените формули за диференциране са известни в реалния анализ, но тук става думи за полиноми с произволни комплексни коефициенти и за формално алгебричното определение на полином. В анализа производната се определя чрез граничен преход и затова двете определения се различават. По такъв начин доказателствата са принципно различни.

Ако $f(x)$ е полином от n-та степен с комплексни коефициенти и $c\in\mathbb{C}$, то $f(x)$ може да се представи във вида

$$f(x)=d_0+d_1(x-c)+\ldots+d_n(x-c)^n,\ d_i\in\mathbb{C}. \tag{5}$$

Практическото пресмятане на коефициентите d_i се постига с неколкократно прилагане на метода на Хорнер. Наистина от (5) веднага се вижда, че d_0 е остатъкът от делението на $f(x)$ с $x-c$; d_1 е остатъкът от делението на полученото частно с $x-c$; d_2 е остатъкът от делението на новополученото частно с $x-c$ и т. н. За някои от по-нататъшните разглеждания обаче ще ни бъде нужно да знаем как коефициентите $d_0, d_1, \ldots, d_n$ се изразяват чрез полинома $f(x)$ и неговите производни. Като диференцираме k пъти двете страни на равенство (5) и заместим след това x с c, получаваме равенствата $f^{(k)}(c)=k!d_k$ $(k=1, 2, \ldots, n)$. Следователно вярна е формулата

$$f(x)=f(c)+\frac{f'(c)}{1!}(x-c)+\ldots+\frac{f^{(n)}(c)}{n!}(x-c)^n, \tag{6}$$

която се нарича формула на Тейлър.

Определение 4. Ще казваме, че комплексното число c е *k-кратен корен* $(k\geqq 1)$ на полинома $f(x)$, ако $(x-c)^k$ е най-високата степен на $x-c$, която дели $f(x)$, т. е. ако $f(x)$ може да се представи във вида:

$$f(x)=(x-c)^k\varphi(x),$$

където $\varphi(x)$ вече не се дели на $x-c$. Еднократните корени се наричат още *прости* корени на $f(x)$.

Удобно е да приемем числото c за 0-кратен корен на $f(x)$, ако c не е корен на $f(x)$, т. е. c е 0-кратен корен на $f(x)$, ако $f(c)\neq 0$.

Понятието кратност на един корен е тясно свързано с понятието производна на полином. Наистина в сила е следната

Теорема 4. *Ако числото c е k-кратен корен на полинома $f(x)$ и $k\geqq 1$, то c е $(k-1)$-кратен корен на първата производна $f'(x)$ на полинома $f(x)$.*

Доказателство. Нека $f(x)=(x-c)^k\varphi(x)$, където $k\geqq 1$ и $\varphi(c)\neq 0$. Тогава

$$f'(x)=(x-c)^k\varphi'(x)+k(x-c)^{k-1}\varphi(x)=(x-c)^{k-1}q(x),$$

където $q(x)=(x-c)\varphi'(x)+k\varphi(x)$. Тъй като $q(c)=k\varphi(c)\neq 0$, то $x-c$ не дели $q(x)$ и следователно c е $(k-1)$-кратен корен на $f'(x)$. С това теоремата е доказана.

Следствие 3. *Числото c е k-кратен корен $(k\geqq 1)$ на полинома $f(x)$ тогава и само тогава, когато c е корен на всеки от полиномите $f(x), f'(x), \ldots, f^{(k-1)}(x)$ и c не е корен на $f^{(k)}(x)$.*

Доказателство. Ако c е k-кратен корен на $f(x)$, по теорема 17 c е $(k-r)$-кратен корен на $f^{(r)}(x)$, т. е. c е корен на $f(x), f'(x), \ldots, f^{(k-1)}(x)$ и не е корен на $f^{(k)}(x)$.

Обратно, нека c е корен на $f(x), f'(x), \ldots, f^{(k-1)}(x)$ и не е корен на $f^{(k)}(x)$. Ако c е l-кратен корен на $f(x)$, по първата част на доказателството $f^{(l)}(x)$ е първата от производните на $f(x)$, за която c не е корен. Но по условие първата от производните на $f(x)$, за която c не е корен, е $f^{(k)}(x)$. Следователно $l=k$, т. е. c е k-кратен корен на $f(x)$, с което твърдението е доказано.

§ 5. Теорема на Даламбер и основни следствия от нея

Една от основните причини за възникване на необходимостта да бъде разширено полето R на реалните числа до полето C на комплексните числа е фактът, че не всяко алгебрично уравнение над R притежава реални корени. Най-просто такова уравнение е $x^2+1=0$. Обаче това уравнение в полето C вече има решения. Отново възниква естественият въпрос, дали всяко алгебрично уравнение с комплексни коефициенти има решение в C. Ако отговорът на този въпрос би бил отрицателен, то неминуемо би възникнала необходимостта да се разшири множеството на комплексните числа до някаква друга числова система. Оказва се обаче, че е в сила следната важна

Теорема 5 (теорема на Даламбер). *Всеки полином от положителна степен с комплексни коефициенти притежава поне един корен в множеството на комплексните числа.*

Първото строго доказателство на тази забележителна теорема е дадено през 1799 година от немския математик К. Ф. Гаус.

По-рано тя е била доказана от французина Даламбер, но с някои непълноти. Теоремата на Даламбер представлява едно от крупните достижения в цялата математика и намира приложение в най-различни области на науката. В частност на нея се опира цялата по-нататъшна теория на полиномите с числови коефициенти, от която ще разгледаме само някои основни резултати. В съответствие с развитието на алгебрата по-рано теоремата са я наричали „основна теорема на висшата алгебра". В действителност тази теорема не е чисто алгебричен факт. За нея са известни сега твърде много доказателства, но те всички в една или друга степен използуват свойства на полето на комплексните числа, свързани с понятието непрекъснатост. От друга страна, степента на развитие на съвременната алгебра е такава, че теоремата на Даламбер вече не може да претендира за първостепенна роля. В това читателят по-нататък ще може и сам да се убеди. Доказателството на теоремата ще изложим по-късно с цел да бъде сведено до минимум използуването на неалгебрични факти. Сега ще пристъпим направо към извеждането на някои основни следствия от нея.

Твърдение 7. *Полиномите от първа степен и само те са неразложими над полето* C *на комлексните числа.*

Доказателство. Знаем, че полиномите от първа степен са неразложими над C.

Нека $p(x)$ е неразложим полином над C. Тогава степента на $p(x)$ е положителна и по теоремата на Даламбер съществува комплексно число c, което е корен на $p(x)$. По теорема 3 ще бъде изпълнено равенството $p(x)=(x-c)\varphi(x)$, където $\varphi(x)$ е полином с комплексни коефициенти. Ако степента на $\varphi(x)$ е положителна, то $p(x)$ ще се окаже разложим над C. Затова $\deg\varphi(x)=0$, т. е. $\varphi(x)=a\neq 0$ и $a\in C$. Получихме, че $p(x)=a(x-c)$, където $0\neq a\in C$. Следователно $\deg p(x)=1$ и твърдението е доказано.

Теорема 6. *Ако $f(x)$ е произволен ненулев полином от n-та степен с числови коефициенти, то над полето* C *на комплексните числа $f(x)$ се разлага в произведение на n линейни множителя, т. е,*

$$(1)\qquad f(x)=a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),\ a\in C,$$

и това разлагане е еднозначно с точност до номерацията на линейните множители $x-\alpha_i$. В частност полиномът $f(x)$ има точно n корена в полето на комплексните числа, като всеки корен на $f(x)$ се брои толкова пъти, колкото е неговата кратност.

Доказателство. Ако $\deg f(x)=0$, то $f(x)=a\neq 0$, $a\in C$, и твърдението е вярно. Ще проведем индукция по степента n на полинома $f(x)$. Нека $n>0$ и за полиномите от по-ниска степен теоремата да е вярна. От теоремата на Даламбер следва, че $f(x)$ има поне един комплексен корен α_1, а от теоремата на Безу — че $f(x)=(x-\alpha_1)g(x)$, където $g(x)$ е ненулев полином от степен $n-1$

с комплексни коефициенти. По индукционното предположение ще съществува разлагането

$$g(x)=a(x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_n),$$

където $0\neq a\in\mathbf{C}$ и $\alpha_i\in\mathbf{C}$ $(i=2, 3, \ldots, n)$. Следователно и $f(x)$ се представя във вида (1).

Ако c е корен на ненулевия полином $f(x)$, то

$$f(c)=a(c-\alpha_1)(c-\alpha_2)\ldots(c-\alpha_n)=0.$$

Тъй като $a\neq 0$, съществува такова $i(1\leqq i\leqq n)$, че $c=\alpha_i$. Следователно корените на $f(x)$ са сред числата $\alpha_1, \alpha_2, \ldots, \alpha_n$. От друга страна, очевидно е, че числата $\alpha_1, \alpha_2, \ldots, \alpha_n$ са корени на $f(x)$ и че с един корен c на $f(x)$ ще съвпадат толкова от тези числа, колкото е неговата кратност. Теоремата е доказана.

Ако $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$, $a_0\neq 0$, и в разлагането (1) на полинома $f(x)$ разкрием скобите, извършим приведението и сравним коефициентите в двете страни на равенството, ще получим следните зависимости между коефициентите $a_0, a_1, \ldots, a_n$ и корените $\alpha_1, \alpha_2, \ldots, \alpha_n$ на $f(x)$:

$$\begin{aligned}
-\frac{a_1}{a_0}&=\alpha_1+\alpha_2+\ldots+\alpha_n,\\
\frac{a_2}{a_0}&=\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_{n-1}\alpha_n,\\
-\frac{a_3}{a_0}&=\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\ldots+a_{n-2}\alpha_{n-1}\alpha_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
(-1)^n\frac{a_n}{a_0}&=\alpha_1\alpha_2\ldots\alpha_n.
\end{aligned}\tag{2}$$

където $(-1)^k\frac{a_k}{a_0}$ е равно на сумата от всевъзможните произведения от по k корена на $f(x)$. Тези формули са известни под наименованието *формули на Виет* в чест на френския математик (по професия юрист) Франсоа Виет (1540—1630).

В редица случаи, когато са дадени и някои допълнителни зависимости между корените на $f(x)$, уравнението $f(x)=0$ може да се реши и чрез формулите (2). Обаче само с изключването на $\alpha_1, \alpha_2, \ldots, \alpha_n$ от (2) се стига отново до уравнението $f(x)=0$.

Непосредствено от теорема 6 се получава и следното твърдение.

Следствие 4. *Ако полиномът $f(x)$ има степен, не по-голяма от числото m, и $f(x)$ се анулира за повече от m различни значения на x, то $f(x)$ е нулевият полином.*

Наистина ако $f(x)\neq 0$, то по теорема 6 полиномът $f(x)$ ще се анулира за не повече от $n=\deg f(x)$ различни стойности на x. Но по условие $n\leqq m$ и така достигаме до противоречие.

Сега сме в състояние да докажем, че двата подхода — формално алгебричният и теоретико-функционалният — за дефиниране равенство на полиноми с числови коефициенти, съвпадат.

Твърдение 8. *Полиномите $f(x)$ и $g(x)$ са равни тогава и само тогава, когато те съвпадат като функции, т. е. $f(c)=g(c)$ за всяко $c \in \mathbf{C}$.*

Наистина, ако $f(x)$ и $g(x)$ имат еднакви коефициенти, очевидно е, че те съвпадат и като функции. Ако $f(x)$ и $g(x)$ съвпадат като функции, разглеждаме полинома $h(x)=f(x)-g(x)$. Този полином се анулира за всяка стойност на x и от следствие 4 получаваме, че той е нулевият полином, т. е. $f(x)=g(x)$.

Фактически от твърдението получаваме нещо повече: равенството $f(c)=g(c)$ $(c \in \mathbf{C})$ за полиномите $f(x)$ и $g(x)$ е достатъчно да бъде изпълнено само за краен брой (по-голям от $\max\{\deg f(x), \deg g(x)\}$) различни стойности на c. Оттук следва, че съществува най-много един полином от степен, ненадминаваща n, който за $n+1$ различни значения $x_1, x_2, \ldots, x_n, x_{n+1}$ на променливата x приема $n+1$ отнапред дадени стойности $y_1, y_2, \ldots, y_n, y_{n+1}$. Построяването на такъв полином се извършва например чрез така наречената *интерполационна формула на Лагранж*

$$f(x)=\sum_{i=1}^{n+1} y_i \frac{(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_{n+1})}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_{n+1})}.$$

Действително от самата формула се вижда, че $\deg f(x) \leqq n$ и $f(x_i)=y_i$ $(i=1, 2, \ldots, n+1)$.

§ 6. Полиноми с реални коефициенти. Рационални корени на полиномите с цели коефициенти

Твърдение 9. *Ако комплексното число α е корен на полинома*

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n \tag{1}$$

с реални коефициенти, то комплексно-спрегнатото число $\bar{\alpha}$ на α е също корен на $f(x)$.

Доказателство. Нека $f(\alpha)=0$, т. е.

$$a_0\alpha^n+a_1\alpha^{n-1}+\ldots+a_{n-1}\alpha+a_n=0.$$

Ако в последното равенство заменим всички числа с техните комплексно-спрегнати, равенството ще се запази. Но тъй като числата $a_0, a_1, \ldots, a_n$ са реални, ще имаме равенството

$$a_0\bar{\alpha}^n+a_1\bar{\alpha}^{n-1}+\ldots+a_{n-1}\bar{\alpha}+a_n=0,$$

т. е. $f(\bar{\alpha})=0$ и $\bar{\alpha}$ също е корен на $f(x)$.

Следствие 5. *Ако комплексното (но не реално) число α е корен на полинома $f(x)$ с реални коефициенти, то $f(x)$ се дели на квадратния тричлен*

(2) $$p(x)=(x-\alpha)(x-\bar{\alpha})=x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha},$$

коефициентите на който са реални числа.

Доказателство. Тъй като α не е реално число, то $\alpha\neq\bar{\alpha}$ и съгласно твърдение 9, α и $\bar{\alpha}$ ще бъдат два различни корена на $f(x)$. Полиномът $f(x)$ се дели на взаимно простите полиноми $x-\alpha$ и $x-\bar{\alpha}$ и затова тяхното произведение $p(x)=(x-\alpha)(x-\bar{\alpha})$ дели $f(x)$. Непосредствено се вижда, че коефициентите на $p(x)$ са реални.

Следствие 6. *Ако числото α е корен на полинома $f(x)$ с реални коефициенти, то α и $\bar{\alpha}$ са негови корени от една и съща кратност.*

Доказателство. Ако α е реално число, то $\alpha=\bar{\alpha}$ и твърдението е очевидно.

Нека $\alpha\neq\bar{\alpha}$, $p(x)=(x-\alpha)(x-\bar{\alpha})$ и k е най-голямото естествено число, за което $p^k(x)$ дели полинома $f(x)$. Тогава $f(x)=p^k(x)q(x)$, където $q(x)$ е полином с реални коефициенти, понеже $f(x)$ и $p^k(x)$ са с реални коефициенти. Ако α или $\bar{\alpha}$ е корен на $q(x)$, то по следствие 5 полиномът $p(x)$ ще дели $q(x)$, което е невъзможно поради избора на k. Следователно α и $\bar{\alpha}$ не са корени на $q(x)$. По този начин получаваме

$$f(x)=p^k(x)q(x)=(x-\alpha)^k\varphi(x)=(x-\bar{\alpha})^k\psi(x),$$

където $\varphi(x)=(x-\bar{\alpha})^kq(x)$, $\psi(x)=(x-\alpha)^kq(x)$. Тъй като $\varphi(\alpha)=(\alpha-\bar{\alpha})^kq(\alpha)\neq0$ и $\psi(\bar{\alpha})=(\bar{\alpha}-\alpha)^kq(\alpha)\neq0$, то α и $\bar{\alpha}$ са корени на $f(x)$ от една и съща кратност k.

Твърдение 10. *Нормираният полином $h(x)$ с реални коефициенти е неразложим над полето R на реалните числа точно в следните два случая:*

1) $h(x)=x-r$, *където* $r\in R$ *или*

2) $h(x)=(x-\alpha)(x-\bar{\alpha})=x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$, *където* α *е комплексно, но не е реално число.*

Доказателство. Нека $h(x)$ е неразложим над R. Тогава $\deg h(x)>0$. По теоремата на Даламбер $h(x)$ има поне един корен в C.

Да допуснем, че $h(x)$ има реален корен r. Тогава $h(x)=(x-r)\varphi(x)$, където $\varphi(x)$ е полином с реални коефициенти, защото $h(x)$ и $x-r$ имат реални коефициенти. Тъй като $h(x)$ е неразложим над R, то $\deg\varphi(x)=0$ и $\varphi(x)=1$, понеже $h(x)$ е нормиран. Следователно $h(x)=x-r$.

Да допуснем, че $h(x)$ има комплексен (но не реален) корен. Тогава от следствие 5 имаме равенството $h(x)=p(x)\psi(x)$, където $p(x)=(x-\alpha)(x-\bar{\alpha})$. Тук отново $h(x)$ и $p(x)$ са с реални коефициенти и затова $\psi(x)$ е с реални коефициенти. От неразложимостта над R на $h(x)$ следва $\deg\psi(x)=0$, а от това, че $h(x)$ е нормиран, получаваме $\psi(x)=1$. Следователно $h(x)=(x-\alpha)(x-\bar{\alpha})$, където $\alpha\neq\bar{\alpha}$.

Обратно, ако $h(x)=x-r$ $(r\in\mathbf{R})$, то $h(x)$ е неразложим над R, защото е от първа степен. Ако $h(x)=(x-\alpha)(x-\bar{\alpha})$ и $\alpha\neq\bar{\alpha}$, да допуснем, че $h(x)$ е разложим над R. Понеже $\deg h(x)=2$, то $h(x)$ ще се разлага в произведение $h(x)=(ax+b)(cx+d)$ на два полинома от първа степен с реални коефициенти a, b, c и d. Но тогава $h(x)$ ще има реален корен $x=-\frac{b}{a}$, което е невъзможно, защото α и $\bar{\alpha}$ не са реални и са единствени корени на $h(x)$. Следователно $h(x)$ е неразложим над полето R.

Теорема 7. *Всеки ненулев полином с реални коефициенти се представя като произведение на своя старши коефициент, на полиноми от първа степен от вида* $x-r$ $(r\in\mathbf{R})$ *и квадратни тричлени от вида* $x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$ $(\bar{\alpha}\neq\alpha\in\mathbf{C})$. *Това представяне е еднозначно с точност до номерацията на множителите.*

Доказателство. Нека $f(x)$ е ненулев полином с реални коефициенти, а $n=\deg f(x)$. При $n=0$, 1 теоремата е очевидна. Нека $n>1$ и да допуснем, че тя е вярна за полиномите с по-ниска степен от n. По теоремата на Даламбер полиномът $f(x)$ има поне един корен в C. Ако този корен е реалното число r, то $f(x)=(x-r)g(x)$, където $\deg g(x)=n-1$ и коефициентите на $g(x)$ са реални. Ако коренът на $f(x)$ е комплексното (но не реално) число α, то $f(x)=p(x)h(x)$, където $p(x)=(x-\alpha)(x-\bar{\alpha})$, $\deg h(x)=n-2$ и коефициентите на $h(x)$ са реални числа. Към полиномите $g(x)$ и $h(x)$ е приложимо индукционното предположение и затова те се разлагат в произведение на своя старши коефициент и неразложими над R нормирани полиноми. Понеже старшият коефициент на $f(x)$ съвпада със старшите коефициенти на $g(x)$ и $h(x)$, то като се замести $g(x)$ или $h(x)$ с техните разлагания, се получава аналогично разлагане и на $f(x)$.

Нека

$$f(x)=a\prod_{i=1}^{s}(x-r_i)\prod_{j=1}^{t}p_j(x)\quad(a\in\mathbf{R})$$

е едно произволно разлагане на $f(x)$ от разглежданията вид. Тук $r_1, r_2, \ldots, r_s$ са реални числа, а $p_j(x)=(x-\alpha_j)(x-\bar{\alpha}_j)$ и $\alpha_j\neq\bar{\alpha}_j$ $(j=1, 2, \ldots, t)$.

Ако r е реален корен на $f(x)$, то $f(x)=(x-r)g(x)$. Тъй като $a\neq 0$, $f(r)=0$ и $p_j(r)\neq 0$ $(j=1, 2, \ldots, t)$, то r ще бъде равно на едно от числата $r_1, \ldots, r_s$. Можем да считаме, че $r=r_1$. Тогава получаваме разлагането

$$g(x)=a\prod_{i=2}^{s}(x-r_i)\prod_{j=1}^{t}p_j(x).$$

По предположение на индукцията полиномът $g(x)$ има единствено

такова разлагане и затова произволно взетото разлагане на $f(x)$ се оказва единствено.

Ако α е комплексен (но не реален) корен на $f(x)$, то $f(x)=p(x)h(x)$, $p(x)=(x-\alpha)(x-\bar{\alpha})$. В този случай α ще бъде едно от числата $\alpha_1, \bar{\alpha}_1, \ldots, \alpha_t, \bar{\alpha}_t$, тъй като $f(\alpha)=0$ и $\alpha \neq r_i, i=1, 2, \ldots, s$. Можем да считаме, че $\alpha=\alpha_1$. Тогава $p(x)=p_1(x)$ и след съкращаване на $p(x)$ получаваме

$$h(x)=a\prod_{i=1}^{s}(x-r_i)\prod_{j=2}^{t}p_j(x),$$

което е единственото разлагане на $h(x)$ в този вид, понеже $\deg h(x)=n-2<\deg f(x)$. Следователно и в този случай произволно взетото разлагане на $f(x)$ е единствено с точност до номерация на множителите.

Да отбележим, че множителите от първа степен в разлагането на $f(x)$ отговарят на реалните корени на $f(x)$, а множителите от втора степен съответстват на двойка комплексно-спрегнати корени. Следователно неразложимите нелинейни полиноми над полето R на реалните числа са квадратните тричлени с отрицателни дискриминанти и само те. От предните резултати следва, че комплексните корени на полином с реални коефициенти образуват двойки комплексно-спрегнати числа. Следователно, ако степента на полинома $f(x)$ с реални коефициенти е нечетна, $f(x)$ обезателно притежава поне един реален корен.

Теорема 8. *Ако несъкратимата рационална дроб $\frac{p}{q}$ е корен на полинома $f(x)$ с цели коефициенти, то p е делител на свободния член на $f(x)$, а q е делител на старшия коефициент на $f(x)$.*

Доказателство. Нека $\frac{p}{q}$ е корен на полинома (1), т. е

$$a_0\frac{p^n}{q^n}+a_1\frac{p^{n-1}}{q^{n-1}}+\ldots+a_{n-1}\frac{p}{q}+a_n=0.$$

Като умножим последното равенство с q^n, получаваме

$$a_0p^n+a_1p^{n-1}q+\ldots+a_{n-1}pq^{n-1}+a_nq^n=0.$$

Тъй като $\frac{p}{q}$ е несъкратима дроб, то p и q са взамно прости числа и от последното ревенство получаваме p/a_nq^n и q/a_0p^n. Понеже $(p, q)=1$, то $(p, q^n)=1$ и $(p^n, q)=1$. Затова p/a_n и q/a_0.

Следствие 7. *Целите корени на полинома $f(x)$ с цели коефициенти са делители на свободния член на $f(x)$. В частност, ако старшият коефициент на $f(x)$ е равен на единица, рационалните корени на $f(x)$ (ако има такива) са цели числа.*

За да намерим целите корени на полинома (1) с цели коефициенти, проверяваме за кой делител на a_n стойността на $f(x)$ е нула. Ако степента на $f(x)$ е висока, то целесъобразно е да имаме предвид следното: за да бъде цялото число p корен на $f(x)$, необходимо е $x-p$ да дели $f(x)$ и тогава полиномът

$$q(x)=\frac{f(x)}{x-p}$$

ще бъде с цели коефициенти. Следователно числата

$$\frac{f(1)}{p-1}=-q(1),\ \frac{f(-1)}{p+1}=-q(-1)$$

трябва да бъдат цели. Това показва, че целите и различните от ± 1 корени на $f(x)$ трябва да търсим между онези делители p на свободния член a_n, за които $p-1$ дели $f(1)$ и $p+1$ дели $f(-1)$. Ясно е, че тук единицата може да бъде заменена с кое да е цяло число.

§ 7. Разложимост на полиноми с рационални коефициенти

С помощта на теоремата на Даламбер вече установихме, че неразложими над полето на комплексните числа са само полиномите от първа степен, а над полето на реалните числа — само полиномите от първа степен и полиномите от втора степен, които нямат реални корени. В този параграф ще изследваме въпроса за неразложимите полиноми над полето Q на рационалните числа. При решаването на редица въпроси е важно да можем да установим дали даден полином е разложим, или е неразложим над Q. Лесно се вижда, че за да бъде разложим над Q един полином от втора или трета степен, е необходимо и достатъчно той да има рационален корен. За полиноми с коефициенти от Q и степен, по-голяма от три, условието да имат рационален корен е само достатъчно (но не и необходимо) за тяхната разложимост. Съществуват множество от критерии за неразложимост на полиноми над Q. Ще разгледаме само един от тях, който е най-значителният. С помощта на този критерий ще установим, че за всяко естествено число n съществуват неразложими над Q полиноми от степен n.

Полиномът $h(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\ (n\geqq 1)$ с цели коефициенти се нарича *примитивен*, ако коефициентите му са взаимно прости, т. е. няма просто число, което да дели едновременно всички коефициенти на $h(x)$.

Ясно е, че ако $h(x)$ е примитивен полином, то $-h(x)$ е също примитивен полином.

Лема 2. ***Всеки ненулев полином с рационални коефициенти се представя еднозначно като произведение на положително рационално число и примитивен полином.***

Доказателство. Нека $f(x)$ е полином с рационални коефициенти, а k е най-малкото общо кратно на знаменателите им. Тогава $f(x)=\frac{1}{k}g(x)$, където $g(x)$ е полином с цели коефициенти. Като изнесем най-големия общ делител d на коефициентите на $g(x)$ пред скоби, получаваме $f(x)=\frac{d}{k}h(x)$, където $h(x)$

$= \frac{1}{d}\ g(x)$ е примитивен полином. Да отбележим, че рационалното число $\frac{d}{k}$ е положително.

Да допуснем, че $f(x) = \frac{d_1}{k_1} h_1(x)$, където $\frac{d_1}{k_1} > 0$ и $h_1(x)$ е примитивен полином. Тогава получаваме равенството $dk_1 h(x) = d_1 k h_1(x)$. Понеже коефициентите на $h(x)$ са взаимно прости и цялото число $d_1 k$ дели коефициентите на полинома $dk_1 h(x)$, то $d_1 k$ ще дели числото dk_1. По аналогични причини dk_1 дели $d_1 k$. Тъй като и двете числа са с еднакъв знак, то ще е изпълнено равенството $dk_1 = d_1 k$, т. е. $\frac{d}{k} = \frac{d_1}{k_1}$ и $h(x) = h_1(x)$.

Лема 3 (лема на Гаус). *Произведение на примитивни полиноми е примитивен полином.*

Доказателство. Нека

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \ (n \geqq 1),$$
$$g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m \ (m \geqq 1)$$

са два произволни примитивни полинома и

$$h(x) = f(x) g(x) = c_0 x^{n+m} + c_1 x^{n+m-1} + \ldots + c_{n+m}$$

е тяхното произведение. Тъй като коефициентите на $f(x)$ и $g(x)$ са цели числа, то коефициентите на $h(x)$ са също цели числа. Да допуснем, че $h(x)$ не е примитивен полином. Тогава коефициентите $c_0, c_1, \ldots, c_{n+m}$ не са взаимно прости и затова ще съществува просто число p, което дели всички числа $c_0, c_1, \ldots, c_{n+m}$. Полиномите $f(x)$ и $g(x)$ по условие са примитивни и по тази причина p не дели всички коефициенти на $f(x)$, не дели и всички коефициенти на $g(x)$. Нека a_i е първият коефициент на $f(x)$, който не се дели на p $(0 \leqq i \leqq n)$, а b_j е първият коефициент на $g(x)$, който не се дели на p $(0 \leqq j \leqq m)$, т. е. $p \nmid a_i$, $p \nmid b_j$, но p/a_0, $a_1, \ldots, a_{i-1}$ и $p/b_0, b_1, \ldots, b_{j-1}$. Тъй като p дели коефициента

$$c_{i+j} = a_i b_j + a_{i-1} b_{j+1} + \ldots + a_{i+1} b_{j-1} + a_{i+2} b_{j-2} \ldots$$

и в дясната страна на последното равенство p дели всяко събираемо от второто до последното, то $p/a_i b_j$. Понеже p е просто число и $p/a_i b_j$, то p/a_i или p/b_j. И в двата случая достигаме до противоречие. Следователно полиномът $h(x) = f(x) g(x)$ е примитивен. Лемата е доказана.

Следствие 8. *Нека полиномът $g(x)$ е от положителна степен и е с рационални коефициенти. Ако $g(x) = \frac{d}{k} h(x)$, където $\frac{d}{k} > 0$ и $h(x)$ е примитивен полином, то $g(x)$ е разложим над полето Q на рационалните числа тогава и само тогава, когато $h(x)$ е разложим над пръстена Z на целите числа.*

Доказателство. Да допуснем, че $g(x)$ е разложим над Q, т. е. $g(x) = \varphi(x) \psi(x)$. Нека

$$\varphi(x)=\frac{d_1}{k_1}\ h_1(x),\quad \psi(x)=\frac{d_2}{k_2}\ h_2(x),$$

където $\frac{d_1}{k_1}>0$, $\frac{d_2}{k_2}>0$ и $h_1(x)$, $h_2(x)$ са примитивни полиноми. От $g(x)=\varphi(x)\,\psi(x)$ получаваме равенството

$$\frac{d}{k}\,h(x)=\frac{d_1d_2}{k_1k_2}h_1(x)\,h_2(x).$$

От лемата на Гаус следва, че $h_1(x)\,h_2(x)$ е примитивен полином Тогава от лема 2 следва, че $\frac{d}{k}=\frac{d_1d_2}{k_1k_2}$ и $h(x)=h_1(x)\,h_2(x)$. Тъй като $h_1(x)$ и $h_2(x)$ имат положителни степени, полиномът $h(x)=h_1(x)\,h_2(x)$ е разложим над **Z**.

Обратно, ако $h(x)$ е разложим над **Z**, т. е. $h(x)=\varphi_1(x)\,\varphi_2(x)$, то $g(x)=\frac{d}{k}\,h(x)=\frac{d}{k}\ \varphi_1(x)\,\varphi_2(x)$ и следователно $g(x)$ е разложим над Q.

Следствие 9. *Един полином с цели коефициенти е разложим над полето* **Q** *на рационалните числа тогава и само тогава, когато той е разложим над пръстена* **Z** *над целите числа.*

Наистина ако $f(x)$ е с цели коефициенти, то $f(x)=dh(x)$ където $d\in Z$ и $h(x)$ е примитивен полином. Тъй като d е цяло число, то $f(x)$ и $h(x)$ са едновременно разложими или неразложими над **Z**. От друга страна, по следствие 8 $f(x)$ е разложим над **Q** тогава и само тогава, когато $h(x)$ е разложим над **Z**. Следователно полиномът $f(x)$ е разложим над **Q** точно тогава, когато той е разложим над **Z**.

Теорема 9 (критерий на Айзенщайн — Шонеман). *Нека полиномът*

$$f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n\ (n\geqq 1)$$

е с цели коефициенти и съществува поне едно просто число p *със следните три свойства:*

1) p *не дели старшия коефициент* a_n *на полинома* $f(x)$

2) p *дели всички останали коефициенти на* $f(x)$;

3) *числото* p^2 *не дели свободния член* a_0 *на* $f(x)$.

Тогава $f(x)$ *е неразложим полином над полето* **Q** *на рационалните числа.*

Доказателство. Да допуснем, че $f(x)$ е разложим над полето **Q**. Тогава по следствие 9 $f(x)$ ще бъде разложим над Z и нека

$$f(x)=(b_0+b_1x+\ldots+b_rx^r)(c_0+c_1x+\ldots+c_kx^k),$$

където $r>0$, $k>0$, $r+k=n$ и коефициентите $b_0, b_1, \ldots, b_r, c_0, c_1, \ldots, c_k$ са цели числа. Като сравним коефициентите в двете страни на горното равенство, получаваме

$$
\begin{aligned}
&a_0 = b_0 c_0,\\
&a_1 = b_0 c_1 + b_1 c_0,\\
&a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0,\\
&\quad\cdots\cdots\cdots\\
&a_r = \ldots + b_{r-1} c_1 + b_r c_0,\\
&\quad\cdots\cdots\cdots\\
&a_n = b_r c_k.
\end{aligned}
\tag{1}
$$

От условията, че p дели a_0, но p^2 не дели a_0, следва, че само един от множителите b_0 и c_0 се дели на p. Нека p дели b_0; тогава p не дели c_0. Тъй като p/a_1 и p/b_0, от второто равенство на (1) следва, че p дели събираемото $b_1 c_0$. Но щом простото число p не дели c_0, то p ще дели b_1. По същия начин от третото равенство се получава, че p/b_2 и т. н. Накрая от $(r+1)$-вото равенство на (1) получаваме, че p/b_r. Тогава от последното равенство $a_n = b_r c_k$ произтича, че p/a_n, което противоречи на условие 1). Следователно $f(x)$ е неразложим полином над $\mathbf{Q}$ и теоремата е доказана.

Нека n е произволно естествено число, а p е просто число. По критерия на Айзенщайн—Шонеман полиномът $x^n + p$ е неразложим над полето $\mathbf{Q}$ на рационалните числа. Следователно за всяко естествено число n съществува полином от n-та степен, който е неразложим над $\mathbf{Q}$.

Доказаната теорема дава само едно достатъчно условие за неразложимост над $\mathbf{Q}$, което не е необходимо. Наистина ако за даден полином $f(x)$ с цели коефициенти не може да се подбере такова просто число, то $f(x)$ може да се окаже разложим, както е например полиномът $f(x) = x^3 - 3x^2 + 3x - 1$, но може да се окаже и неразложим, например като полинома $f(x) = x^2 + 1$.

Понякога въпросът за неразложимост над $\mathbf{Q}$ на даден полином, към който пряко не е приложим критерият на Айзенщайн—Шонеман, все пак се удава да бъде решен с този критерий, като се използува подходяща редукция. За илюстрация ще покажем, че полиномът

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

е неразложим над $\mathbf{Q}$ за всяко просто число p.

Очевидно в сила е равенството

$$(x-1)\,\Phi_p(x) = x^p - 1.$$

Ако в това равенство положим $x = y + 1$, получаваме

$$y\Phi_p(y+1) = (y+1)^p - 1 = \sum_{i=0}^{p-1} \binom{p}{i} y^{p-i}.$$

Да разгледаме полинома

$$g(y) = \Phi_p(y+1) = y^{p-1} + \binom{p}{1} y^{p-2} + \ldots + \binom{p}{p-1}.$$

Свободният член на $g(y)$ е равен на $\binom{p}{p-1} = p$ и следователно

той се дели на p, но не се дели на p^2. Старшият коефициент на $g(y)$ е единица и затова не се дели на p. За да можем да приложим критерия на Айзенщайн—Шонеман, трябва да покажем че биномните коефициенти $\binom{p}{i}$ при $i=1, 2, \ldots, p-1$ се делят на простото число p.

Действително от равенството

$$p(p-1)(p-2)\ldots(p-i+1)=\binom{p}{i} i!$$

и факта, че $\binom{p}{i}$ е цяло число, следва, че p дели произведението $\binom{p}{i} i!$ Но тъй като просто число p не дели $i!$ при $1\leqq i\leqq p-1$, оттук заключаваме, че p дели числото $\binom{p}{i}$.

По този начин установихме, че полиномът $g(y)$ е неразложим над полето Q. Остава да отбележим, че оттук следва неразложимостта на $\Phi_p(x)$. Наистина ако допуснем, че

$$\Phi_p(x)=\varphi(x)\psi(x),$$

където $\deg\varphi(x)>0$, $\deg\psi(x)>0$ и коефициентите на $\varphi(x)$ и $\psi(x)$ са рационални числа, то

$$g(y)=\Phi_p(y+1)=\varphi(y+1)\psi(y+1).$$

При това $\varphi(y+1)$ и $\psi(y+1)$ са полиноми на y от степени, съответно равни на $\deg\varphi(x)$ и $\deg\psi(x)$, и също имат рационални коефициенти. Получихме, че $g(y)$ е разложим, в противоречие с доказаното. Следователно $\Phi_p(x)$ е неразложим над Q. Полиномът $\Phi_p(x)$ е един от така наречените полиноми на деление на кръга които ще разгледаме в следващия параграф.

Накрая ще отбележим, че съществува метод на Кронекер (вж например [20], стр. 464), който позволява за всеки полином с цели коефициенти да се установи дали той е разложим, или е неразложим над полето Q. Този метод обаче е свързан с твърде дълги изчисления и е практически почти неприложим.

§ 8. Циклотомични полиноми

Корените $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ на полинома x^n-1 $(n\geqq 1)$ нарекохме n-ти корени на единицата. В сила е разлагането

$$x^n-1=\prod_{i=1}^{n}(x-\varepsilon_i). \tag{1}$$

Измежду $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ точно $\varphi(n)$ на брой са примитивните n-ти корени от единицата, където $\varphi(n)$ е функцията на Ойлер (виж глава VII, § 3). Да означим с $\eta_1, \eta_2, \ldots, \eta_{\varphi(n)}$ тези примитивни корени и да разгледаме полинома

(2) $$\Phi_n(x)=(x-\eta_1)(x-\eta_2)\ldots(x-\eta_{\varphi(n)}),$$

корените на който съвпадат с n-тите примитивни корени на единицата. Този полином се нарича *n-ти циклотомичен полином* или още *n-ти полином на деление на кръга.*

Очевидно е, че ако естественото число d дели n, то всеки d-ти корен на единицата се среща измежду n-тите корени. Обратно, всеки n-ти корен на единицата е примитивен s-ти кореи на единицата за някое s, което дели n. Затова, като групираме множителите в дясната страна на равенството (1), получаваме

(3) $$x^n-1=\prod_{d/n}\Phi_d(x),$$

където d пробягва всички положителни делители на n.

Формулата (3) дава възможност да се изчисли $\Phi_n(x)$, при условие че са вече известни всички $\Phi_d(x)$ за $d<n$ и d/n. Наистина $\Phi_n(x)$ е частното от делението на x^n-1 с произведението $f(x)$ на всички $\Phi_d(x)$, където $d<n$ и d/n, т. е.

(4) $$x^n-1=\Phi_n(x)f(x).$$

Твърдение 11. *Коефициентите на циклотомичните полиноми са цели числа.*

Доказателство. Тъй като $\Phi_1(x)=x-1$, за $n=1$ твърдението е вярно. Да допуснем, че $n>1$ и че полиномите $\Phi_d(x)$ за $d<n$ имат цели коефициенти. Тогава произведението $f(x)$ на полиномите $\Phi_d(x)$, където $d<n$ и d/n, ще бъде полином с цели коефициенти. Тъй като циклотомичните полиноми имат старши коефициенти, равни на единица, то и старшият коефициент на $f(x)$ е единица. Като си спомним как се изчислява частното $\Phi_n(x)$ от делението на x^n-1 с $f(x)$, получаваме, че $\Phi_n(x)$ е с цели коефициенти. Твърдението е доказано.

Ако p е просто число, то p има само два естествени делителя — единицата и p, и затова

$$x^p-1=\Phi_1(x)\Phi_p(x)=(x-1)\Phi_p(x).$$

Следователно вярно е равенството

$$\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\ldots+x+1,$$

т. е. $\Phi_p(x)$ е точно полиномът, който разглеждахме в края на предишния параграф. Там доказахме, че за всяко просто число p циклотомичният полином $\Phi_p(x)$ е неразложим над полето Q на рационалните числа. Във връзка с това възниква въпросът, има ли измежду циклотомичните полиноми разложими полиноми над Q. Може да се докаже следната (виж например [16], стр. 235).

Теорема 10. *Циклотомичните полиноми са неразложими над полето* Q *на рационалните числа.*

Лесно се вижда, че $\Phi_4(x)=x^2+1$, $\Phi_6(x)=x^2-x+1$. Следователно първите няколко циклотомични полинома и всички $\Phi_p(x)$ при p — просто число, имат коефициенти, равни на ± 1 или на нула. Но това не е изпълнено за всеки циклотомичен полином $\Phi_n(x)$. Например коефициентите на $\Phi_{105}(x)$ са равни на 0, ± 1 и -2.

§ 9. Уравнения от трета и четвърта степен

Теоремата на Даламбер ни гарантира, че всяко алгебрично уравнение от n-та степен ($n \geqq 1$)

$$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=0 \tag{1}$$

с произволни комплексни коефициенти притежава точно n корена. Да се реши уравнението (1) ще рече да се намерят всичките му корени. В изчислителната математика съществуват множество методи за приблизително пресмятане на корените на произволни уравнения, където лявата страна на уравнението може и да не бъде алгебричен полином, а произволна функция. На тези методи обаче тук не ще се спираме.

Под алгебрично решаване на уравнението (1) се разбира пресмятането на корените му посредством краен брой рационални действия (т. е. събиране, изваждане, умножение и деление) и извличане на корени от коефициентите на уравнението. В този параграф ще посочим методи за алгебрично решаване на уравненията от трета и четвърта степен. Има един общ момент при алгебричното решаване на тези уравнения: *ако даденото уравнение е от степен n, то най-напред се трансформира в уравнение от n-та степен, в което коефициентът пред $(n-1)$-вата степен на неизвестното е нула.* Не е трудно да се види, че това се постига чрез полагането $x=y-\frac{a_1}{na_0}$. Ако можем да решим трансформираното уравнение $f\left(y-\frac{a_1}{na_0}\right)=0$ относно y, като използуваме връзката между x и y, можем да намерим корените и на даденото уравнение.

Общото уравнение от трета степен

$$a_0x^3+a_1x^2+a_2x+a_3=0$$

чрез полагането $x=y-\frac{a_1}{3a_0}$ се трансформира в кубично уравнение относно y, в което коефициентът пред y^2 е нула. Като разделим двете страни на това уравнение с a_0, виждаме, че въпросът за решаването на пълното кубично уравнение се свежда до решаване на уравнение от вида

$$y^3+py+q=0. \tag{2}$$

Докато квадратни уравнения са решавали още древногръцките математици, то едва през 1515 г. за първи път са били решени някои нетривиални уравнения от вида (2) от италианския ма-

тематик Сципионе дел Феро — професор в Болонския университет. Потребностите за решаване на такива уравнения тогава са били свързани с проблема за разделянето на даден ъгъл на три равни части, т. е. със задачата за трисекцията на ъгъла. Формулата за решаване на уравнението (2) с буквени коефициенти е била открита през 1535 г. от италианския математик Никола Тарталиа, но за пръв път е публикувана през 1545 г. от друг италианец — Джеронимо Кардано и носи неговото име. Лобачевски е дал друго решение на уравнението (2) чрез полагането $x = y - \frac{p}{3y}$. Тук ще изведем формулата на Кардано по метода на Хюдѐ, даден през 1639 г.

Кой да е корен y_0 на уравнението (2) търсим във вида

$$y_0 = \alpha + \beta, \tag{3}$$

където α и β подлежат на определяне. Понеже y_0 е корен на уравнението (2), то

$$\alpha^3 + \beta^3 + (\alpha + \beta)(3\alpha\beta + p) + q = 0.$$

Ще искаме освен това неизвестните α и β да удовлетворяват условието $3\alpha\beta + p = 0$, т. е.

$$\alpha\beta = -\frac{p}{3}. \tag{4}$$

Следователно за α и β получаваме следната система:

$$\begin{cases} \alpha^3 + \beta^3 = -q, \\ \alpha^3\beta^3 = -\frac{p^3}{27}. \end{cases}$$

Това показва, че α^3 и β^3 са корени на квадратното уравнение

$$u^2 + qu - \frac{p^3}{27} = 0$$

относно неизвестното u. Понеже ролята на α и β е симетрична, то нека

$$\alpha^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad \beta^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Оттук получаваме търсената формула на Кардано:

$$y_0 = \alpha + \beta = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{5}$$

Тъй като кубичен корен от различно от нула комплексно число има точно три стойности (виж § 4 на глава I), като комбинираме трите стойности на първия кубичен радикал с трите стойности на втория, ще получим по формулата (5) общо девет стойности за y_0. Но лесно се вижда, че само три от тях са корени на даденото уравнение (2), тъй като радикалите α и β трябва да

удовлетворяват условието (4). Действително нека A и B са две стойности съответно на α и β, за които $AB=-\frac{p}{3}$. Тогава всички стойности на радикала α са A, εA, $\varepsilon^2 A$, (виж глава I, § 4), а стойностите на радикала β са B, εB, $\varepsilon^2 B$, където $\varepsilon=\frac{-1+i\sqrt{3}}{2}$ е примитивен трети корен на единицата. Сега е очевидно, че A може да се комбинира само с B, защото произведенията $A(\varepsilon B)$ и $A(\varepsilon^2 B)$ не са равни на $-\frac{p}{3}$. По същия начин εA се комбинира само с $\varepsilon^2 B$, а $\varepsilon^2 A$ се комбинира само с εB. Така за y_0 получаваме следните три стойности:

$$y_1=A+B,$$
$$y_2=\varepsilon A+\varepsilon^2 B,$$
$$y_3=\varepsilon^2 A+\varepsilon B.$$

Като заместим ε и ε^2 с техните стойности

$$\varepsilon=\frac{-1+i\sqrt{3}}{2},\quad \varepsilon^2=\frac{-1-i\sqrt{3}}{2},$$

за корените y_1, y_2 и y_3 на уравнението (2) ще получим

$$y_1=A+B,$$
$$y_2=-\frac{A+B}{2}+i\frac{A-B}{2}\sqrt{3},$$
$$y_3=-\frac{A+B}{2}-i\frac{A-B}{2}\sqrt{3}.$$

С помощта на тези формули би могло да се изследва в зависимост от p и q кога корените на (2) са реални или многократни.

Общото уравнение от четвърта степен

$$a_0x^4+a_1x^3+a_2x^2+a_3x+a_4=0$$

с помощта на полагането $x=y-\frac{a_1}{4a_0}$ се трансформира в уравнение, на което коефициентът пред y^3 е нула. Ако в това уравнение коефициентът пред y е също нула, то решението му се свежда до решаване на две квадратни уравнения, понеже уравнението е биквадратно. Затова е достатъчно да посочим метод за решаване на непълното уравнение

(6) $$x^4+px^2+qx+r=0$$

от четвърта степен, където $q\neq 0$.

За първи път това уравнение е било решено от Людовико Ферари, но решението му е било публикувано от неговия учител Кардано през 1545 г. заедно със споменатата формула на Кардано за уравнения от трета степен. За решаването на уравнението

(6) са известни много методи. Ще посочим само един от тях, даден от Рене Декарт. Даденото уравнение (6) представяме във вида

$$(x^2+ux+v)(x^2-ux+v_1)=0. \tag{7}$$

Коефициентите u, v и v_1 се определят от приравняването на коефициентите на полиномите от (6) и (7), а именно от системата

$$\begin{cases} v+v_1-u^2=p \\ u(v_1-v)=q \\ v\,v_1=r. \end{cases} \tag{8}$$

Оттук получаваме, че $u\neq 0$,

$$\begin{cases} v+v_1=u^2+p \\ v-v_1=-\dfrac{q}{u} \end{cases}$$

и следователно

$$v=\frac{1}{2}\left(p+u^2-\frac{q}{u}\right),\quad v_1=\frac{1}{2}\left(p+u^2+\frac{q}{u}\right).$$

Като заместим тези изрази за v и v_1 в третото уравнение на (8) получаваме уравнението

$$u^6+2pu^4+(p^2-4r)u^2-q^2=0, \tag{9}$$

което чрез полагането $u^2=y$ се свежда до кубичното уравнение

$$y^3+2py^2+(p^2-4r)y-q^2=0.$$

След като намерим поне един корен u_0 на уравнението (9), решаването на даденото уравнение се свежда до решаване на двете квадратни уравнения

$$x^2+u_0x+\frac{1}{2}\left(p+u_0^2-\frac{q}{u_0}\right)=0,$$

$$x^2-u_0x+\frac{1}{2}\left(p+u_0^2-\frac{q}{u_0}\right)=0.$$

Би могло да се изследва броят на реалните и комплексните корени на уравнението (6) в зависимост от стойностите на коефициентите p, q и r (виж [20], стр. 359).

След намиране на методи за алгебрично решаване на уравнения от трета и четвърта степен почти три столетия математиците са правили безуспешни опити да намерят формули, които с помощта на радикали да изразяват корените на произволно уравнение от пета степен. Пръв италианският лекар Паоло Руфини през 1799 г. е показал, че такива формули не съществуват за общи уравнения (с буквени коефициенти), чиято степен е по-голяма от четири. Доказателството на Руфини е съдържало известни пропуски. То не е било разбрано и оценено от съвременниците му, поради което за тях е останало неизвестно. След това нор-

вежкият математик Нилс Хенрих Абел през 1826 г. дава ново строго доказателство на този факт, който сега е прието да се нарича теорема на Руфини — Абел. Близо до тези идеи е стоял и френският математик Лагранж. Той е установил, че общото уравнение от n-та степен при $n \leqq 4$ може да бъде решено алгебрично, защото съществуват рационални функции (дроби, числителят и знаменателят на които са полиноми) от n променливи, които при всевъзможните пермутации на променливите вземат $n-1$ различни значения. Оказва се, че такива рационални функции при $n \geqq 5$ вече не съществуват.

Теоремата на Руфини — Абел обаче не изключва възможността някои конкретни уравнения от по-висока степен да бъдат разрешими алгебрично. Пълното изследване на условията, при които дадено алгебрично уравнение е решимо в радикали, е било дадено през 30-те години на миналия век от двадесетгодишния французин Еварист Галоа (1811—1832). Идеите на този гениален математик са изходният пункт на широко развити днес области на алгебрата — теория на Галоа и теория на групите. Тези идеи са дали дълбоко отражение въобще на цялата съвременна математика.

ГЛАВА III

ПОЛИНОМИ НА ПОВЕЧЕ ПРОМЕНЛИВИ

§ 1. Определение и някои свойства на полиномите на повече променливи над числов пръстен

Наред с полиномите на една променлива в математиката често се налага разглеждането на полиноми, които зависят от две, три или повече променливи. Такива са например линейните и квадратичните форми, познати от линейната алгебра.

Нека P е произволен числов пръстен, а $x_1, x_2, \ldots, x_n$ са n на брой независими неизвестни (променливи). Всеки формален израз от вида

$$\alpha = a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},$$

където степенните показатели са цели неотрицателни числа, а коефициентът a е число от P, се нарича *едночлен* над P на променливите $x_1, x_2, \ldots, x_n$. Едночленът α се нарича *подобен* на едночлена

$$\beta = b x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$$

точно тогава, когато съответните степенни показатели съвпадат, т. е. когато $k_1 = l_1, k_2 = l_2, \ldots, k_n = l_n$. Едночлените α и β по определение са равни, ако са изпълнени следните две условия:

а) коефициентите на α и β са равни, т. е. $a = b$;

б) ако $a = b \neq 0$, то α и β са подобни.

Както и по-рано, ще считаме, че нулевата степен на всяка променлива съвпада с единицата. Тогава едночлените с нулеви коефициенти са равни на числото нула, а всеки едночлен с нулеви степенни показатели се отъждествява с коефициента си. По този начин числата от пръстена P ще разглеждаме и като едночлени над P на $x_1, x_2, \ldots, x_n$.

Произведение на едночлените α и β (означава се с $\alpha\beta$) наричаме едночлена

$$\alpha\beta = ab\, x_1^{k_1+l_1} x_2^{k_2+l_2} \ldots x_n^{k_n+l_n}.$$

Ако α и β са подобни едночлени, тяхна *сума* $\alpha+\beta$ се нарича едночленът

$$\alpha+\beta = (a+b)\, x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}.$$

Ако α, β и γ са три едночлена, то $\alpha\beta = \beta\alpha$ и $(\alpha\beta)\gamma = \alpha(\beta\gamma)$, т. е. умножението на едночлени е комутативна и асоциативна операция. Аналогично, ако α, β и γ са подобни едночлени, изпълнени са и равенствата $\alpha+\beta = \beta+\alpha$ и $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.

Определение 1. Всяка формална сума от вида

(1) $$f(x_1, x_2, \ldots, x_n) = \sum c_t x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n},$$

в която участвуват като събираеми само краен брой едночлени над P, никои два от които не са подобни и редът на записването им е произволен, се нарича *полином на променливите* $x_1, x_2, \ldots, x_n$ над числовия пръстен P.

Тъй като в (1) е възможно да имаме и само едно-единствено събираемо, то едночлените са полиноми над P. Ако в (1) участвуват събираеми само с нулеви коефициенти, то $f(x_1, x_2, \ldots, x_n)$ съвпада с числото нула и казваме, че $f(x_1, x_2, \ldots, x_n)$ е нулевият полином.

В записа на един полином можем да разместваме произволно събираемите, можем да прибавяме или премахваме събираеми, които са едночлени с нулеви коефициенти, и от това самият полином не се изменя. По такъв начин можем да считаме, че в записите на всеки два дадени полинома участвува един и същ набор от подобни едночлени, т. е. тези полиноми бяха могли да се различават само по коефициентите на съответните подобни едночлени. Ще казваме, че два полинома на $x_1, x_2, \ldots, x_n$ са равни, ако са равни коефициентите на съответните подобни едночлени в записите на тези полиноми.

Множеството от всички полиноми над P на променливите $x_1, x_2, \ldots, x_n$ ще означаваме с $P[x_1, x_2, \ldots, x_n]$.

Ако $g = g(x_1, x_2, \ldots, x_n)$ и $h = h(x_1, x_2, \ldots, x_n)$ са два полинома от $P[x_1, x_2, \ldots, x_n]$, под тяхна *сума* $g+h$ ще разбираме полинома, който се получава чрез събиране на съответните подобни едночлени от записите на g и h. *Произведение* gh на полиномите g и h се нарича полиномът, който се получава, като се образува сумата от всевъзможните произведения на едночлените от записа на g и едночлените от записа на h и в тази сума се извърши приведение на подобните събираеми.

Както при полиномите на една променлива, може да се провери, *че така дефинираните операции събиране и умножение в множеството* $P[x_1, x_2, \ldots, x_n]$ *са комутативни, асоциативни и са свързани помежду си чрез дистрибутивния закон.*

Ако едночленът $a = ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ е с коефициент $a \neq 0$, то степенният показател k_i се нарича *степен* на a относно променливата x_i, а сумата $k_1 + k_2 + \ldots + k_n$ на степенните показатели се нарича (*обща*) *степен* на a относно променливите. Ако $f(x_1, x_2, \ldots, x_n)$ е ненулев полином, *степен* на $f(x_1, x_2, \ldots, x_n)$ относно x_i се нарича най-високата степен относно x_i на едночлените, които участвуват в записа на $f(x_1, x_2, \ldots, x_n)$ с ненулеви коефициенти. *Степен на полинома* $f(x_1, x_2, \ldots, x_n)$ се нарича най-високата степен на неговите членове. Например полиномът

$$f(x_1, x_2, x_3) = x_1^5 + x_1 x_2 x_3 + x_1^2 x_2^2 x_3^3$$

има степени относно x_1, x_2 и x_3, съответно равни на 5, 2 и 3, а степента му е равна на 7.

За удобство, както и при полиномите на една променлива, на нулевия полином приписваме степен относно всяка променлива и (обща) степен, равни на символа $-\infty$, който има същите свойства, както и по-рано.

Всеки полином $f(x_1, x_2, \ldots, x_n)$ на n променливи $x_1, x_2, \ldots, x_n$ може да бъде разглеждан като полином на x_n с коефициенти, които са полиноми на $x_1, x_2, \ldots, x_{n-1}$. Оттук с метода на пълната математична индукция може да се докаже, че произведението на два полинома на променливи е равно на нула точно тогава, когато поне един от множителите е равен на нула. Не се спираме на доказателството на този факт, тъй като ще го получим след малко като следствие от една важна лема.

При полиномите на една променлива x използувахме два естествени начина за наредба на техните членове — по растящите или намаляващите степени на x. При полиномите на няколко променливи този начин е вече неприложим, тъй като тези полиноми могат да съдържат по няколко неподобни члена от една и съща степен. За да можем да докажем редица важни факти за полиномите на няколко неизвестни, ще въведем един нов метод за устояване на реда на записване на членовете на полиноми-те. Този метод, наречен лексикографски, зависи от номерацията на неизвестните и напомня за начина на подреждане на думите в речниците: като се считат буквите от азбуката наредени в общоприетия им ред, взаимното разположение на две думи в речника се определя от техните първи букви; ако те съвпадат, сравняват се вторите им букви и т. н.

Нека $f(x_1, x_2, \ldots, x_n)$ е произволен ненулев полином от $P[x_1, x_2, \ldots, x_n]$, а $\alpha = a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ и $\beta = b x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ са два ненулеви различни едночлена от записа на $f(x_1, x_2, \ldots, x_n)$. Тогава поне една от разликите $k_1 - l_1, k_2 - l_2, \ldots, k_n - l_n$ е различна от нула. Ще казваме, че ненулевият едночлен α е по-висок или по-висш от ненулевия едночлен β, което кратко ще означим с $\alpha \succ \beta$, ако първата, различна от нула разлика в редицата $k_1 - l_1, k_2 - l_2, \ldots, k_n - l_n$ е положителна. С други думи, ще бъде изпълнено

$$a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \succ b x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$$

тогава и само тогава, когато съществува такова i $(1 \leqq i \leqq n)$, че

$$k_1 = l_1, \; k_2 = l_2, \ldots, k_{i-1} = l_{i-1}, \; k_i > l_i. \tag{2}$$

Лесно се вижда, че или $\alpha \succ \beta$, или $\beta \succ \alpha$; т. е. всеки два ненулеви различни едночлена от записа на полинома $f(x_1, x_2, \ldots, x_n)$ са сравними лексикографски. Освен това ако

$$\gamma = c x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$$

е такъв трети ненулев член от записа на $f(x_1, x_2, \ldots, x_n)$, че $\alpha \succ \beta$ и $\beta \succ \gamma$, то обезателно ще бъде изпълнено и условието $\alpha \succ \gamma$. Действително за някое j $(1 \leqq j \leqq n)$ ще имаме

(3) $$l_1=m_1,\ l_2=m_2,\ldots,\ l_{j-1}=m_{j-1},\ l_j>m_j.$$

Тогава от (2) и (3) при $i<j$ ще следва, че $k_1=m_1,\ k_2=m_2,\ldots,\ k_{i-1}=m_{i-1},\ k_i>l_i=m_i$, т. е. $\alpha\succ\gamma$. Ако пък $i\geqq j$, то ще бъдат изпълнени условията $k_1=m_1,\ k_2=m_2,\ldots,\ k_{j-1}=m_{j-1},\ k_j\geqq l_j>m_j$, откъдето отново следва, че $\alpha\succ\gamma$.

По този начин можем да подредим едночлените в записа на $f(x_1, x_2,\ldots,x_n)$ в низходящ ред по тяхната височина и да получим напълно определен начин на записване, който наричаме лексикографски. Например членовете на полинома

$$f(x_1, x_2, x_3, x_4)=x_1^2+x_1x_2^2x_3x_4^5+x_2x_3^5x_4^2+x_2x_3^5x_4$$

са лексикографски наредени.

Тук трябва да отбележим, че ако $\alpha\succ\beta$, не следва, че степента на α е по-голяма от степента на β. Това се вижда от приведения по-горе пример — едночленът x_1^2 на $f(x_1, x_2, x_3, x_4)$ е от най-ниска степен, но е най-висш в лексикографската наредба.

При лексикографската наредба един от членовете на ненулевия полином $f(x_1, x_2,\ldots,x_n)$ ще стои на първо място и ще бъде по-висок от всички останали негови членове. Този член ще наричаме *старши член* на полинома $f(x_1, x_2,\ldots,x_n)$.

Лема 1. *Старшият член на произведението на два полинома от $P[x_1, x_2,\ldots,x_n]$ е равен на произведението на старшите членове на тези полиноми.*

Доказателство. Нека $\alpha=a\,x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ и $\beta=b\,x_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$ са старшите членове съответно на $f(x_1, x_2,\ldots,x_n)$ и $g(x_1, x_2,\ldots,x_n)$. Да означим с γ произведението $\alpha\beta$, т. е.

$$\gamma=a\,b\,x_1^{k_1+l_1}x_2^{k_2+l_2}\ldots x_n^{k_n+l_n}.$$

Нека $\delta=c\,x_1^{s_1}x_2^{s_2}\ldots x_n^{s_n}$ е произволен ненулев едночлен от записа на $f(x_1, x_2,\ldots,x_n)$, различен от старшия едночлен α, а $\tau=d\,x_1^{t_1}x_2^{t_2}\ldots x_n^{t_n}$ е произволен ненулев едночлен от записа на $g(x_1, x_2,\ldots,x_n)$, различен от старшия едночлен β. Тогава $\alpha\succ\delta$ $\beta\succ\tau$ и затова съществуват такива индекси $i\,(1\leqq i\leqq n)$ и $j\,(1\leqq j\leqq n)$, че да са изпълнени условията

(4) $$k_1=s_1,\ k_2=s_2,\ldots,\ k_{i-1}=s_{i-1},\ k_i>s_i,$$
$$l_1=t_1,\ l_2=t_2,\ldots,\ l_{j-1}=t_{j-1},\ l_j>t_j.$$

За да покажем, че $\gamma=\alpha\beta$ е старшият член на $\varphi(x_1, x_2,\ldots x_n)=f(x_1,\ldots,x_n)\,g(x_1,\ldots,x_n)$, достатъчно е да установим, че той е по-висок от всевъзможните произведения $\alpha\tau$, $\delta\beta$ и $\delta\tau$. За тази цел удобно е да разгледаме поотделно случаите $i>j$ и $i\leqq j$.

Нека $i>j$. От (4) следва, че са изпълнени условията

$$k_1+l_1=k_1+t_1,\ldots,\ k_{j-1}+l_{j-1}=k_{j-1}+t_{j-1},\ k_j+l_j>k_j+t_j,$$
$$k_1+l_1=s_1+l_1,\ldots,\ k_{i-1}+l_{i-1}=s_{i-1}+l_{i-1},\ k_i+l_i>s_i+l_i,$$
$$k_1+l_1=s_1+t_1,\ldots,\ k_{j-1}+l_{j-1}=s_{j-1}+t_{j-1},\ k_j+l_j>s_j>t_j,$$

откъдето следва, че $\gamma\succ\alpha\tau$, $\gamma\succ\delta\beta$ и $\gamma\succ\delta\tau$.

По аналогичен начин се разглежда и случаят $i \leqq j$. Лемата е доказана.

Следствие 1. *Произведението на два полинома от* $P[x_1, x_2, \ldots, x_n]$ *е равно на нула тогава и само тогава, когато поне един от множителите е нулевият полином.*

Действително ако $f(x_1, x_2, \ldots, x_n)$ и $g(x_1, x_2, \ldots, x_n)$ са ненулеви полиноми, то старшият член на тяхното произведение $\varphi(x_1, x_2, \ldots, x_n)$ съгласно лема 1 ще бъде равен на произведението от старшите членове на множителите и следователно ще бъде отличен от нула, т. е. полиномът $\varphi(x_1, x_2, \ldots, x_n)$ ще бъде ненулев.

§ 2. Симетрични полиноми

Полиномът $f(x_1, x_2, \ldots, x_n)$ се нарича *симетричен,* ако той не се изменя при всевъзможните разместванията на променливите $x_1, x_2, \ldots, x_n$, т. е. ако $f(x_1, x_2, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, където $i_1, i_2, \ldots, i_n$ е произволна пермутация на числата $1, 2, \ldots, n$. Най-прости примери за симетрични полиноми са например сумата на всички неизвестни $x_1 + x_2 + \ldots + x_n$, сумата на техните квадрати $x_1^2 + x_2^2 + \ldots + x_n^2$, произведението им $x_1 x_2 \ldots x_n$ и т. н. Очевидно е, че сумата, разликата и произведението на два симетрични полинома са също симетрични полиноми.

Един полином $f(x_1, x_2, \ldots, x_n)$ се нарича *хомогенен (еднороден)*, ако всички негови членове имат една и съща степен.

Ще казваме, че два едночлена $ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ и $bx_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ имат една и съща система от степенни показатели, ако съществува такава пермутация $i_1, i_2, \ldots, i_n$ на числата от 1 до n, че да са изпълнени равенствата $k_1 = l_{i_1}, k_2 = l_{i_2}, \ldots, k_n = l_{i_n}$.

Определение 2. Симетричният полином $f(x_1, x_2, \ldots, x_n)$ се нарича *прост*, ако всичките му членове са с един и същ коефициент и с една и съща система от степенни показатели.

Очевидно е, че всеки прост полином е хомогенен. Простият симетричен полином $f(x_1, x_2, \ldots, x_n)$ се нарича *k-формен* и се означава с

$$a \sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k},$$

ако във всеки негов член участвуват точно k на брой ненулеви степенни показатели $\alpha_1, \alpha_2, \ldots, \alpha_k$, т. е. ако $f(x_1, x_2, \ldots, x_n)$ е сума на всички различни едночлени, получени от $ax_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$ чрез всевъзможните заместванията на $x_1, x_2, \ldots, x_k$ с различни неизвестни от неизвестните $x_1, x_2, \ldots, x_n$.

Едноформените симетрични полиноми S_α от вида

$$S_\alpha = \sum x_n^\alpha = x_1^\alpha + x_2^\alpha + \ldots + x_n^\alpha$$

се наричат *степенни сборове.* Очевидно е, че всеки степенен сбор

съдържа точно n члена. Броят на членовете на двуформения прост симетричен полином

$$\sum x_1^{\alpha} x_2^{\beta}$$

при $\alpha \neq \beta$ е равен на $n(n-1)$, а при $\alpha = \beta$ този брой намалява наполовина, т. е. той е равен на $\frac{n(n-1)}{2}$. Триформеният прост симетричен полином

$$\sum x_1^{\alpha} x_2^{\beta} x_3^{\gamma},$$

при $\alpha \neq \beta$, $\beta \neq \gamma$, $\gamma \neq \alpha$ има точно $n(n-1)(n-2)$ члена. Ако два от показателите са равни, той ще има $\frac{n(n-1)(n-2)}{2}$ члена; при $\alpha = \beta = \gamma$ този брой се намалява още три пъти, т. е. членовете ще бъдат $\frac{n(n-1)(n-2)}{6}$ на брой. Изобщо, ако ненулевите степенни показатели на един k-формен прост симетричен полином са всички различни помежду си, то броят на членовете му ще бъде равен на броя на вариациите от n елемента по k, т. е. на $n(n-1)(n-2) \ldots (n-k+1)$. Ако обаче s_1 показатели са равни помежду си, s_2 други показатели са също равни помежду си, но различни от първите и т. н., общият брой на членовете ще бъде

$$\frac{n(n-1)(n-2) \ldots (n-k+1)}{s_1! s_2! \ldots}.$$

Твърдение 1. *Всеки симетричен полином е сума от краен брой прости симетрични полиноми.*

Доказателство. Нека

$$a x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \tag{1}$$

е един произволен член на симетричния полином $f = f(x_1, x_2, \ldots, x_n)$. Тъй като f не се променя при пермутиране на променливите, то f съдържа в записа си всички членове, които се получават от (1) чрез произволно разместване на $x_1, x_2, \ldots, x_n$. Следователно полиномът f съдържа в записа всеки член на простия симетричен полином

$$g = a \sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

Тогава $f_1 = f - g$ е пак симетричен полином, но с по-малко на брой членове, отколкото полиномът f. Ако $f_1 \neq 0$, повтаряме разсъжденията за f_1. Ясно е, че с последователното изваждане на прости симетрични полиноми ще достигнем до нулевия полином и следователно f ще се представи като сума на прости симетрични полиноми.

Простите симетрични полиноми, ненулевите степенни показа-

тели на които са равни на единица и членовете на които имат коефициент единица, се наричат *елементарни симетрични полиноми.* Тези полиноми играят важна роля в теорията на симетричните полиноми, поради което за тях въвеждаме специални означения:

$$\sigma_1 = x_1 + x_2 + \ldots + x_n = \sum x_1,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots = \sum x_1x_2,$$

$$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \ldots = \sum x_1x_2x_3,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n = x_1 x_2 \ldots x_n = \sum x_1 x_2 \ldots x_n.$$

Ако разгледаме полинома

$$\varphi_n(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \ldots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n$$

на променливата x и си спомним формулите на Виет за връзката между корените и коефициентите, виждаме, че $x_1, x_2, \ldots, x_n$ могат да се разглеждат като корени на $\varphi_n(x)$. Също така от формулите на Виет следва, че коефициентите на един нормиран полином на x са с точност до знак елементарните симетрични полиноми на неговите корени.

§ 3. Изразяване на симетричните полиноми чрез елементарните симетрични полиноми

Нека $\sigma_1, \sigma_2, \ldots, \sigma_n$ са елементарните симетрични полиноми на променливите $x_1, x_2, \ldots, x_n$. Тъй като сума, разлика и произведение на симетрични полиноми е пак симетричен полином, то *всеки полином над P от елементарните симетрични полиноми* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *е симетричен полином спрямо неизвестните* $x_1, x_2, \ldots, x_n$ Оказва се, че е вярно и обратното твърдение, което съставлява съдържанието на основната теорема за симетричните полиноми. Най-напред ще докажем следната

Лема 2. *Ако* $f(x_1, x_2, \ldots, x_n)$ *е произволен симетричен полином и*

$$\alpha = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$$

е неговият старши член в лексикографската наредба, то степенните показатели $k_1, k_2, \ldots, k_n$ *удовлетворяват неравенствата*

$$k_1 \geqq k_2 \geqq \ldots \geqq k_n.$$

Действително ако допуснем, че за някое i $(1 \leqq i \leqq n-1)$ е изпълнено $k_i < k_{i+1}$, то от едночлена α с разместване на неизвест-

ните x_i и x_{i+1} ще получим, че симетричният полином $f(x_1, x_2, \ldots, x_n)$ съдържа в записа си и едночлена

$$\beta = ax_1^{k_1} \ldots x_{i-1}^{k_{i-1}} x_i^{k_{i+1}} x_{i+1}^{k_i} \ldots x_n^{k_n}.$$

Но лесно се вижда, че β е по-висок от α, което противоречи на предположението, че α е старшият член на $f(x_1, x_2, \ldots, x_n)$.

Теорема 1 (основна теорема за симетричните полиноми). *Всеки симетричен полином на неизвестните $x_1, x_2, \ldots, x_n$ над числовия пръстен P може да се представи като полином на елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ с коефициенти от P.*

Доказателство. Нека $f = f(x_1, x_2, \ldots, x_n)$ е произволен симетричен полином на $x_1, x_2, \ldots, x_n$ с коефициенти от P и $\alpha = a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ е неговият старши член. Съгласно лема 2 разликите $k_1 - k_2$, $k_2 - k_3$, $\ldots$, $k_{n-1} - k_n$ са неотрицателни цели числа. Следователно произведението

$$\varphi_1 = a\sigma_1^{k_1-k_2} \sigma^{k_2-k_3} \ldots \sigma_{n-1}^{k_{n-1}-k_n} \sigma_n^{k_n}$$

е симетричен полином на $x_1, x_2, \ldots, x_n$ над P, понеже φ_1 е едночлен на елементарните симетрични полиноми. Тъй като σ_k има старши член $x_1 x_2 \ldots x_k$ $(k = 1, 2, \ldots, n)$, по лема 1 старшият член на φ_1 ще бъде равен на произведението

$$ax_1^{k_1-k_2} (x_1x_2)^{k_2-k_3} \ldots (x_1 x_2 \ldots x_{n-1})^{k_{n-1}-k_n} (x_1 x_2 \ldots x_n)^{k_n},$$

т. е. старшите членове на f и φ_1 съвпадат. Тогава разликата

$$f - \varphi_1 = f_1$$

е симетричен полином от $P[x_1, x_2, \ldots, x_n]$, чийто старши член е по-нисък от този на f. Ако полиномът f_1 е ненулев, с аналогични разсъждения за симетричния полином f_1 получаваме симетричния полином

$$f_1 - \varphi_2 = f_2,$$

където φ_2 е едночлен на елементарните симетрични полиноми с коефициент от P, а старшият член на f_2 е по-нисък от старшия член на f_1. Така стигаме до равенството

$$f = \varphi_1 + \varphi_2 + f_2.$$

Като продължим този процес, ще получим полиномите $f_1, f_2, f_3, \ldots$ и за някое k $(k \geqq 1)$ ще имаме $f_k = 0$, поради което за f ще бъде изпълнено равенството

$$f = \sum_{i=1}^{k} \varphi_i = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

т. е. f ще се представи като сума на едночлени, а следователно и като полином на $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Действително, ако допуснем, че посоченият процес е безкраен, ще получим безкрайна редица от симетрични полиноми

(1) $$f_1, f_2, \ldots, f_s, \ldots$$

с коефициенти от P, в която старшият член на всеки полином е по-нисък от старшия член на предхождащия го полином. Тогава, ако $\beta = bx_1^{s_1} x_2^{s_2} \ldots x_n^{s_n}$ е старшият член на симетричния полином f_s, съгласно лема 2 и условието $\alpha > \beta$ ще имаме

(2) $$k_1 \geqq s_1 \geqq s_2 \geqq \ldots \geqq s_n \geqq 0.$$

Тъй като k_1 е фиксирано цяло число (първият степенен показател на старшия член на f), лесно е да се съобрази, че системите от цели числа $s_1, s_2, \ldots, s_n$, които удовлетворяват, неравенствата (2), са не повече от $(k_1+1)^n$, т. е. те са краен брой. Оттук следва, че редицата (1) не може да бъде безкрайна, с което теоремата е доказана.

Лема 3. *Всеки ненулев полином* $\psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ *на* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *над числовия пръстен* P *е ненулев полином на* $x_1, x_2, \ldots, x_n$.

Доказателство. Произволен ненулев член $a\sigma_1^{k_1}\sigma_2^{k_2} \ldots \sigma_n^{k_n}$ на полинома $\psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$, разглеждан като полином на $x_1, x_2, \ldots, x_n$, ще има старши член

$$ax_1^{l_1} x_2^{l_2} \ldots x_n^{l_n} = ax_1^{k_1}(x_1 x_2)^{k_2} \ldots (x_1 x_2 \ldots x_n)^{k_n},$$

т. е. ще бъдат изпълнени равенствата

$$\begin{aligned} l_1 &= k_1 + k_2 + k_3 + \ldots + k_n, \\ l_2 &= \quad k_2 + k_3 + \ldots + k_n, \\ l_3 &= \quad\quad k_3 + \ldots + k_n, \\ &\ldots\ldots\ldots\ldots \\ l_n &= \quad\quad\quad\quad k_n. \end{aligned}$$

Тогава равенствата $k_n = l_n$, $k_i = l_i - l_{i+1}$ $(i = 1, 2, \ldots, n-1)$ показват, че всеки член $\alpha = a\sigma_1^{k_1}\sigma_2^{k_2} \ldots \sigma_n^{k_n}$ на полином $\psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ еднозначно се определя от старшия си член $a x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$, ако α се разглежда като полином на $x_1, \ldots, x_n$ и обратно. Следователно различните членове на $\psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ като полиноми на $x_1, x_2, \ldots, x_n$ притежават в лексикографската наредба в $P[x_1, x_2, \ldots, x_n]$ различни старши членове. Но тогава най-високият от тези старши членове няма да има подобни при изразяването на $\psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ като полином на $x_1, x_2, \ldots, x_n$, т. е. няма да може да се унищожи при извършване на приведението и ще се окаже старши член на полинома $f(x_1, x_2, \ldots, x_n) = \psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Следователно $f(x_1, x_2, \ldots, x_n)$ е ненулев полином от $P[x_1, x_2, \ldots, x_n]$. Лемата е доказана.

Теорема 2. *Всеки симетричен полином на променливите* $x_1, x_2, \ldots, x_n$ *над числовия пръстен* P *се представя по единствен начин като полином на елементарните симетрични полиноми* $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Доказателство. Нека $f(x_1, x_2, \ldots, x_n)$ е произволен

симетричен полином от $P[x_1, x_2, \ldots, x_n]$. Да допуснем, че $f(x_1, x_2, \ldots, x_n)$ има две различни представяния като полином на $\sigma_1, \sigma_2, \ldots, \sigma_n$, т. е. $f(x_1, \ldots, x_n) = \varphi(\sigma_1, \ldots, \sigma_n)$ и $f(x_1, \ldots, x_n) = \varphi_1(\sigma_1, \ldots, \sigma_n)$. Това означава, че $\varphi(\sigma_1, \ldots, \sigma_n)$ и $\varphi_1(\sigma_1, \ldots, \sigma_n)$ като полиноми на $\sigma_1, \sigma_2, \ldots, \sigma_n$ са различни. Тогава полиномът

$$\psi(\sigma_1, \ldots, \sigma_n) = \varphi(\sigma_1, \ldots, \sigma_n) - \varphi_1(\sigma_1, \ldots, \sigma_n)$$

е ненулев и съгласно лема 3 $\psi(\sigma_1, \ldots, \sigma_n)$ ще бъде ненулев полином на $x_1, x_2, \ldots, x_n$. Но по допускане имаме

$$\psi(\sigma_1, \ldots, \sigma_n) = \varphi(\sigma_1, \ldots, \sigma_n) - \varphi_1(\sigma_1, \ldots, \sigma_n) = f(x_1, x_2, \ldots, x_n) - f(x_1, x_2, \ldots, x_n) = 0,$$

т. е. $\psi(\sigma_1, \ldots, \sigma_n)$ като полином на $x_1, x_2, \ldots, x_n$ се оказва равен на нулевия полином. Полученото противоречие показва, че $f(x_1, x_2, \ldots, x_n)$ не може да има две различни представяния като полином на $\sigma_1, \sigma_2, \ldots, \sigma_n$. Теоремата е доказана.

Отбелязаната в края на предишния параграф връзка между елементарните симетрични полиноми и формулите на Виет позволява от основната теорема за симетричните полиноми да се получи следното важно

Следствие 2. *Всеки симетричен полином от корените на нормирания полином $f(x)$ може да се представи като полином от коефициентите на $f(x)$.*

Доказателство. Нека $h(\alpha_1, \ldots, \alpha_n)$ е симетричен полином над P на корените $\alpha_1, \alpha_2, \ldots, \alpha_n$ на $f(x)$. Ако $x_1, \ldots, x_n$ са неизвестни, то от теорема 1 следва, че $h(x_1, \ldots, x_n) = \varphi(\sigma_1, \ldots, \sigma_n)$, където $\varphi(\sigma_1, \ldots, \sigma_n)$ е полином на $\sigma_1, \ldots, \sigma_n$ над P. Нека

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n.$$

Ако формулите на Виет за полинома $f(x)$ запишем във вида

$$\sigma_1 = \sigma_1(\alpha_1, \ldots, \alpha_n) = -a_1,$$
$$\sigma_2 = \sigma_2(\alpha_1, \ldots, \alpha_n) = a_2,$$
$$\ldots\ldots\ldots\ldots$$
$$\sigma_n = \sigma_n(\alpha_1, \ldots, \alpha_n) = (-1)^n a_n,$$

от горните равенства получаваме, че

$$h(\alpha_1, \ldots, \alpha_n) = \varphi[\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots, \alpha_n)] = \varphi[-a_1, a_2, \ldots, (-1)^n a_n],$$

т. е. $h(\alpha_1, \ldots, \alpha_n)$ е полином от $a_1, a_2, \ldots, a_n$ с коефициенти от пръстена P (те са с точност до знак коефициентите на $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Следствието е доказано.

Пример. Да се изрази симетричният полином

$$f(x_1, x_2, \ldots, x_n) = \sum x_1^3 x_2$$

чрез елементарните симетрични полиноми.

За решението на този пример ще приложим тъй наречения метод на неопределените коефициенти. Знаем (виж доказателството на теорема 1), че членовете на търсения полином $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ се определят чрез старшите членове на полиномите f_1, $f_2, \ldots$, като при това всеки от тези старши членове е по-нисък от предхождащия го. Следователно трябва да намерим всички произведения $x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$, които удовлетворяват условията: 1) те са по-ниски от старшия член $x_1^3 x_2$ на f; 2) те могат да служат за старши членове на симетрични полиноми, т. е. степенните показатели удовлетворяват неравенствата $l_1 \geqq l_2 \geqq \ldots \geqq l_n$; 3) те имат (обща) степен, равна на 4 (тъй като f е хомогенен от степен 4, то и f_1, $f_2, \ldots$ ще бъдат хомогенни от степен 4). Като запишем само съответните комбинации на степенните показатели, а до тях — тези произведения на $\sigma_1, \sigma_2, \ldots, \sigma_n$, които се определят от съответните степенни показатели, ще получим следната таблица:

$$3\ 1\ 0\ 0\ 0 \ldots \sigma_1^{3-1}\ \sigma_2^{1-0} = \sigma_1^2 \sigma_2,$$

$$2\ 2\ 0\ 0\ 0 \ldots \sigma_1^{2-2}\ \sigma_2^{2-0} = \sigma_2^2,$$

$$2\ 1\ 1\ 0\ 0 \ldots \sigma_1^{2-1}\ \sigma_2^{1-1}\ \sigma_3^{1-0} = \sigma_1 \sigma_3,$$

$$1\ 1\ 1\ 1\ 0 \ldots \sigma_1^{1-1}\ \sigma_2^{1-1}\ \sigma_3^{1-1}\ \sigma_4^{1-0} = \sigma_4.$$

По този начин полиномът f ще има вида

$$f = \sigma_1^2 \sigma_2 + A\sigma_2^2 + B\sigma_1\sigma_3 + C\sigma_4,$$

Положили сме коефициента пред $\sigma_1^2 \sigma_2$ да е равен на единица, тъй като това произведение се определя от старшия член на f и има, както знаем от доказателството на теорема 1, същия коефициент.

Неизвестните коефициенти A, B и C ще намерим по следния начин. Полагаме $x_1 = x_2 = 1$, $x_3 = x_4 = \ldots = x_n = 0$. Лесно се вижда, че при тези стойности на неизвестните полиномът f получава стойност 2, а полиномите σ_1, σ_2, σ_3 и σ_4 — съответно стойности 2, 1, 0 и 0. Затова

$$2 = 2^2 . 1 + A . 1^2 + B . 2 . 0 + C . 0,$$

т. е. $A = -2$. Да положим сега $x_1 = x_2 = x_3 = 1$, $x_4 = x_5 = \ldots = x_n = 0$. Стойностите на полиномите f, σ_1, σ_2, σ_3 и σ_4 ще бъдат равни съответно на 6, 3, 3, 1 и 0. Затова

$$6 = 3^2 . 3 + (-2) . 3^2 + B . 3 . 1 + C . 0,$$

откъдето $B = -1$. Накрая полагаме $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = x_6 = \ldots = x_n = 0$. Стойностите на f, σ_1, σ_2, σ_3 и σ_4 ще бъдат равни съответно на 12, 4, 6, 4 и 1. Тогава

$$12=4^2.6+(-2).6^2+(-1).4.4+C.1$$

и следователно $C=4$. По този начин търсеното изразяване на f ще бъде

$$f=\sigma_1^2\sigma_2-2\sigma_2^2-\sigma_1\sigma_3+4\sigma_4.$$

Често в приложенията се използува едно обобщение на понятието симетричен полином, което ще разгледаме накратко.

Нека $x_1, x_2, \ldots, x_n$ и $y_1, y_2, \ldots, y_n$ са две системи от променливи. Полиномът

$$f=f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) \tag{3}$$

с коефициенти от даден числов пръстен P се нарича симетричен относно двете системи променливи, ако той не се променя при всяка пермутация поотделно на $x_1, x_2, \ldots, x_n$ и на $y_1, y_2, \ldots, y_m$. Да означим със $\sigma_1, \sigma_2, \ldots, \sigma_n$ елементарните симетрични полиноми на $x_1, x_2, \ldots, x_n$, а с $\delta_1, \delta_2, \ldots, \delta_m$ — елементарните симетрични полиноми на $y_1, y_2, \ldots, y_m$.

Теорема 3. *Всеки полином* (3), *който е симетричен по отношение на двете системи променливи* $x_1, x_2, \ldots, x_n$ *и* $y_1, y_2, \ldots, y_m$ *и е с коефициенти от* P, *може да се представи като полином на съответните елементарни симетрични полиноми* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *и* $\delta_1, \delta_2, \ldots, \delta_m$ *с коефициенти от пръстена* P.

Доказателство. Записвайки f като полином $f=h(y_1, y_2, \ldots, y_m)$ на $y_1, y_2, \ldots, y_m$ с коефициенти от $P[x_1, x_2, \ldots, x_n]$, тези коефициенти ще бъдат симетрични полиноми от $P[x_1, x_2, \ldots, x_n]$, защото f е симетричен относно системата $x_1, x_2, \ldots, x_n$. Следователно коефициентите на $h(y_1, y_2, \ldots, y_m)$ могат да се изразят като полиноми на $\sigma_1, \sigma_2, \ldots, \sigma_n$ с коефициенти от P. По този начин f се представя като симетричен полином на $y_1, y_2, \ldots, y_m$ с коефициенти от $P[\sigma_1, \sigma_2, \ldots, \sigma_n]$. Тогава, както в доказателството на теорема 1, може да се докаже, че f се представя като полином на $\delta_1, \delta_2, \ldots, \delta_m$ с коефициенти от $P[\sigma_1, \sigma_2, \ldots, \sigma_n]$. Но това означава в крайна сметка, че f се представя като полином на $\sigma_1, \sigma_2, \ldots, \sigma_n, \delta_1, \delta_2, \ldots, \delta_m$ с коефициенти от P. Теоремата е доказана.

Може да се докаже, че представянето в току-що доказаната теорема е единствено. Освен това теоремата може да бъде обобщена и за повече от две системи променливи.

Без да се впускаме в подробности, ще завършим този параграф с някои резултати за дробно рационалните симетрични функции.

Израз от вида

$$\varphi(x_1, x_2, \ldots, x_n)=\frac{f(x_1, x_2, \ldots, x_n)}{g(x_1, x_2, \ldots, x_n)}, \tag{4}$$

където $f(x_1, x_2, \ldots, x_n)$ и $g(x_1, x_2, \ldots, x_n)$ са полиноми над числовото поле P на неизвестните $x_1, x_2, \ldots, x_n$ и $g(x_1, x_2, \ldots$

$x_n) \neq 0$, се нарича дробна рационална функция над P на x_1, $x_2, \ldots, x_n$. Ако $\varphi = \frac{f}{g}$ и $\psi = \frac{h}{u}$ са две дробни рационални функции на $x_1, x_2, \ldots, x_n$, ще считаме, че те съвпадат тогава и само тогава, когато съвпадат полиномите fu и gh. Това определение не съвпада с теоретико-функционалното определение за равенство на две функции. Например дробните рационални функции

$$\varphi(x_1, x_2) = \frac{x_1^2}{x_1^2 - x_1 x_2}, \quad \psi(x_1, x_2) = \frac{x_1}{x_1 - x_2}$$

съвпадат по току-що приетото алгебрично определение, но те са различни в теоретико-функционален смисъл, защото функцията $\varphi(x_1, x_2)$ не е определена при $x_1 = 0$ и $x_2 \neq 0$, а функцията $\psi(x_1, x_2)$ е определена.

Множеството от всички дробни рационални функции над числовото поле P на неизвестните $x_1, x_2, \ldots, x_n$ ще бележим с $P(x_1, x_2, \ldots, x_n)$. По естествен начин в $P(x_1, x_2, \ldots, x_n)$ могат да бъдат въведени операции събиране и умножение, за които лесно се показва, че не зависят от представянето на отделните функции. Освен това тези операции са комутативни, асоциативни и са свързани с дистрибутивния закон. Очевидно е, че $P[x_1, x_2, \ldots, x_n]$ се съдържа в $P(x_1, x_2, \ldots, x_n)$.

Дробно рационалната функция (4) се нарича *симетрична*, ако тя не се променя при всяка пермутация на $x_1, x_2, \ldots, x_n$. Ако $g = g_1, g_2, \ldots, g_k$ $(1 \leqq k \leqq n!)$ са всички различни полиноми, които се получават от g чрез всевъзможните разместванията на променливите, то за φ ще имаме представянето

$$\varphi = \frac{f g_2 g_3 \ldots g_k}{g_1 g_2 \ldots g_k},$$

в което не е трудно да се съобрази, че числителят и знаменателят са симетрични полиноми на $x_1, x_2, \ldots, x_n$ с коефициенти от P. Следователно *всяка симетрична дробно рационална функция от* $P(x_1, x_2, \ldots, x_n)$ *може да се представи като дробно рационална функция на елементарните симетрични полиноми* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *с коефициенти от* P.

§ 4 Степенни сборове

Както вече бе отбелязано, едноформените симетрични полиноми от вида

$$S_\alpha = \sum x_1^\alpha = x_1^\alpha + x_2^\alpha + \ldots + x_n^\alpha \quad (\alpha = 1, 2, \ldots)$$

се наричат степенни сборове. В този параграф ще изведем формули за изразяване на степенните сборове чрез елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Да положим

(1) $$f(x)=(x-x_1)\,(x-x_2)\,\ldots\,(x-x_n)$$

и да разгледаме $f(x)$ като полином на x. От формулите на Виет за зависимостта между корените и коефициентите знаем, че

(2) $$f(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$

където

$$a_k=(-1)^k\sigma_k\ (k=1,\ 2,\ \ldots,\ n).$$

От равенство (1) чрез диференциране относно x получаваме

$$f'(x)=\frac{f(x)}{x-x_1}+\frac{f(x)}{x-x_2}+\ldots+\frac{f(x)}{x-x_n}.$$

За да пресметнем коефициентите на полинома $\frac{f(x)}{x-x_k}$, извършваме деление на полинома (2) с $x-x_k$ по схемата на Хорнер. Получаваме следната таблица:

	1	a_1	a_2	$\ldots$	a_{n-1}	a_n
x_k	1	x_k+a_1	$x_k^2+a_1x_k+a_2$	$\ldots$	$x_k^{n-1}+a_1x_k^{n-2}+\ldots+a_{n-1}$	$f(x_k)$

Следователно

$$\frac{f(x)}{x-x_k}=x^{n-1}+(x_k+a_1)x^{n-2}+\ldots+(x_k^{n-1}+a_1x_k^{n-2}+\ldots+a_{n-1}).$$

Ако в предишното равенство поставим $k=1,\ 2,\ \ldots,\ n$ и съберем получените n равенства, ще имаме

$$f'(x)=nx^{n-1}+(S_1+na_1)\,x^{n-2}+(S_2+a_1S_1+na_2)x^{n-3}+$$
$$+\ldots+(S_{n-1}+a_1S_{n-2}+\ldots+a_{n-2}S_1+na_{n-1}).$$

От друга страна, ако диференцираме двете страни на равенство (2), ще получим

$$f'(x)=nx^{n-1}+(n-1)a_1x^{n-2}+\ldots+2a_{n-2}x+a_{n-1}.$$

Като сравним коефициентите пред равните степени на x в двата израза за $f'(x)$, стигаме до следните равенства:

(3)
$$\begin{aligned}
&S_1+a_1=0,\\
&S_2+a_1S_1+2a_2=0,\\
&S_3+a_1S_2+a_2S_1+3a_3=0,\\
&\ldots\ldots\ldots\ldots\\
&S_{n-1}+a_1S_{n-2}+\ldots+a_{n-2}S_1+(n-1)a_{n-1}=0.
\end{aligned}$$

След като заместим в (3) a_k с неговото равно $(-1)^k\sigma_k$ за $k=1,\ 2,\ \ldots,\ n-1$, ще получим следните формули на Нютон за връзката между степенните сборове и елементарните симетрични полиноми:

(4)
$$\begin{aligned}
&S_1-\sigma_1=0,\\
&S_2-\sigma_1S_1+2\sigma_2=0,\\
&S_3-\sigma_1S_2+\sigma_2S_1-3\sigma_3=0,\\
&\ldots\ldots\ldots\ldots\\
&S_{n-1}-\sigma_1S_{n-2}+\ldots+(-1)^{n-2}\sigma_{n-2}S_1+(-1)^{n-1}\,(n-1)\sigma_{n-1}=0,
\end{aligned}$$

откъдето последователно могат да бъдат намерени $S_1, S_2, \ldots, S_{n-1}$.

Формулите за $S_n, S_{n+1}, \ldots$ се получават лесно, като в полиномите $f(x), xf(x), x^2 f(x), \ldots$ поставим $x = x_1, x_2, \ldots, x_n$ и съберем получените n равенства. Тъй като $f(x_i) = 0$, от (2) следва, че

$$0 = x_i^k f(x_i) = x_i^{n+k} + a_1 x_i^{n+k-1} + \ldots + a_{n-1} x_i^{k+1} + a_n x_i^k,$$

където $k \geqq 0$ и $i = 1, 2, \ldots, n$. За фиксирано k събираме по i получените n равенства и намираме

$$S_{n+k} + a_1 S_{n+k-1} + \ldots + a_n S_k = 0,$$

където при $k = 0$ полагаме $S_0 = n$. Така получаваме равенствата

$$\begin{aligned} &S_n + a_1 S_{n-1} + \ldots + a_{n-1} S_1 + n a_n = 0, \\ &S_{n+1} + a_1 S_n + \ldots + a_{n-1} S_2 + a_n S_1 = 0, \\ &S_{n+2} + a_1 S_{n+1} + \ldots + a_{n-1} S_3 + a_n S_2 = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{5}$$

Като заместим $a_1, a_2, \ldots, a_n$ съответно със $-\sigma_1, \sigma_2, -\sigma_3, \ldots, (-1)^n \sigma_n$, получаваме

$$\begin{aligned} &S_n - \sigma_1 S_{n-1} + \ldots + (-1)^{n-1} \sigma_{n-1} S_1 + (-1)^n n \sigma_n = 0, \\ &S_{n+1} - \sigma_1 S_n + \ldots + (-1)^{n-1} \sigma_{n-1} S_2 + (-1)^n \sigma_n S_1 = 0, \\ &S_{n+2} - \sigma_1 S_{n+1} + \ldots + (-1)^{n-1} \sigma_{n-1} S_3 + (-1)^n \sigma_n S_2 = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{6}$$

Очевидно е, че формулите (5) и (6) могат да се разглеждат като продължение съответно на формулите (3) и (4), като е положено $0 = a_{n+1} = a_{n+2} = \ldots$ и $0 = \sigma_{n+1} = \sigma_{n+2} = \ldots$.

Ако от (3) и (5) вземем първите k ($k \geqq 1$) равенства и ги разгледаме като система от k уравнения с k неизвестни $S_1, S_2, \ldots, S_k$, по формулите на Крамер S_k може да се представи като детерминанта

$$S_k = -\begin{vmatrix} 1 & 0 & 0 & \ldots & 0 & a_1 \\ a_1 & 1 & 0 & \ldots & 0 & 2a_2 \\ a_2 & a_1 & 1 & \ldots & 0 & 3a_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{k-2} & a_{k-3} & a_{k-4} & \ldots & 1 & (k-1)a_{k-1} \\ a_{k-1} & a_{k-2} & a_{k-3} & \ldots & a_1 & ka_k \end{vmatrix},$$

където $a_r = (-1)^r \sigma_r$ и е положено $\sigma_{n+1} = \sigma_{n+2} = \ldots = 0$.

Нека числовият пръстен P да е поле. Тъй като в числовото поле P е възможно делението на произволно естествено число, то от равенства (4) и от първото равенство на (6) елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ могат да се изразят чрез степенните сборове $S_1, S_2, \ldots, S_n$. Оттук и от основната теорема за симетричните полиноми непосредствено се получава следният резултат.

Теорема 4. *Ако P е произволно числово поле, то всеки симетричен полином от $P[x_1, x_2, \ldots, x_n]$ може да се представи като полином на степенните сборове $S_1, S_2, \ldots, S_n$ с коефициенти от P.*

Тази теорема може да се докаже и директно, като се покаже първо по индукция, че простите симетрични полиноми се изразяват като полиноми на $S_1, S_2, \ldots, S_n$ с коефициенти от P, а после се приложи твърдение 1.

§ 5. Резултанта на полиноми

Нека са дадени полиномите

$$(1)\qquad \begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \quad (n \geqq 1), \\ g(x) &= b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m \quad (m \geqq 1) \end{aligned}$$

с коефициенти от числовото поле P. Естествено възниква въпросът, при какви условия за коефициентите на $f(x)$ и $g(x)$ тези полиноми имат общи корени. Очевидно е, че корените на НОД $(f(x), g(x))$ и само те са общи корени на $f(x)$ и $g(x)$. Следователно поставеният въпрос може да бъде решен с помощта на алгоритъма на Евклид. С оглед на приложенията тук ще посочим друг подход за решаване на разглежданият въпрос.

Лема 4. *Ако поне един от коефициентите a_0 и b_0 на полиномите* (1) *е различен от нула, то тези полиноми притежават общи корени тогава и само тогава, когато съществуват полиноми*

$$(2)\qquad \begin{aligned} \varphi(x) &= c_0x^{n-1} + c_1x^{n-2} + \ldots + c_{n-2}x + c_{n-1}, \\ \psi(x) &= d_0x^{m-1} + d_1x^{m-2} + \ldots + d_{m-2}x + d_{m-1}, \end{aligned}$$

от които поне един е ненулев и

$$(3)\qquad f(x)\,\psi(x) = g(x)\,\varphi(x).$$

Доказателство: Достатъчно е да разгледаме случая когато $a_0 \neq 0$.

Ако $g(x) = 0$, то твърдението на лемата е очевидно, защото всеки корен на $f(x)$ е корен и на $g(x)$. В този случай избираме $\psi(x) = 0$, а $\varphi(x)$ може да бъде произволен ненулев полином от степен $\leqq n-1$.

Затова ще предполагаме, че $g(x) \neq 0$.

Ако $x = \alpha_1$ е общ корен на $f(x)$ и $g(x)$, то полагаме

$$\frac{f(x)}{x-\alpha_1} = \varphi(x), \quad \frac{g(x)}{x-\alpha_1} = \psi(x),$$

където $\deg \varphi(x) \leqq n-1$ и $\deg \psi(x) \leqq m-1$. Оттук, като изключим $x-\alpha_1$, получаваме равенството (3) с $\varphi(x) \neq 0$ и $\psi(x) \neq 0$.

Обратно, да предположим, че поне един от полиномите (2) е ненулев и е изпълнено равенството (3). Понеже $f(x) \neq 0$ и $g(x) \neq 0$,

то оттук ще следва, че $\varphi(x) \neq 0$ и $\psi(x) \neq 0$. Ако $\alpha_1, \alpha_2, \ldots, \alpha_n$ са корените на $f(x)$, то от (3) получаваме, че

$$0 = f(\alpha_i)\psi(\alpha_i) = g(\alpha_i)\varphi(\alpha_i), \quad i = 1, 2, \ldots, n.$$

Тъй като $\varphi(x)$ има най-много $n-1$ корена, то от последните равенства следва, че съществува такова $i (1 \leqq i \leqq n)$, че $g(\alpha_i) = 0$. Следователно α_i е общ корен за полиномите (1). Лемата е доказана.

Ако $f(x)$ и $g(x)$ от (1) са произволни полиноми с числови коефициенти, то детерминантата от $(n+m)$-ти ред

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 & 0 \\ 0 & a_0 & \ldots & a_{n-1} & a_n & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_0 & \ldots & \ldots & a_{n-1} & a_n \\ b_0 & b_1 & \ldots & b_m & 0 & \ldots & 0 & 0 \\ 0 & b_0 & \ldots & b_{m-1} & b_m & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_0 & \ldots & \ldots & b_{m-1} & b_m \end{vmatrix}$$

се нарича *резултанта* на полиномите $f(x)$ и $g(x)$.

Теорема 5. *Ако поне един от коефициентите a_0 и b_0 на полиномите* (1) *е различен от нула, то тези полиноми притежават общи корени тогава и само тогава, когато тяхната резултанта е равна на нула.*

Доказателство. Съгласно предната лема полиномите (1) притежават общи корени точно тогава, когато съществуват полиномите (2), от които поне единият не е нулев и е изпълнено равенството (3). Като сравним в (3) коефициентите пред еднаквите степени на x, ще получим равенствата

$$(4) \quad \begin{cases} a_0 d_0 = b_0 c_0, \\ a_1 d_0 + a_0 d_1 = b_1 c_0 + b_0 c_1, \\ a_2 d_0 + a_1 d_1 + a_0 d_2 = b_2 c_0 + b_1 c_1 + b_0 c_2, \\ \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\ a_n d_{m-2} + a_{n-1} d_{m-1} = b_m c_{n-2} + b_{m-1} c_{n-1}, \\ a_n d_{m-1} = b_m c_{n-1}. \end{cases}$$

Системата от равенства (4) може да се разглежда като система от $n+m$ линейни хомогенни уравнения с $n+m$ неизвестни $d_0, d_1, \ldots, d_{m-1}, -c_0, -c_1, \ldots, -c_{n-1}$, която притежава поне едно ненулево решение, защото или $\varphi(x) \neq 0$, или $\psi(x) \neq 0$. Но тъй като $R(f, g)$ е транспонираната детерминанта на детерминантата на хомогенната система (4), то оттук следва, че $f(x)$ и $g(x)$ имат общи корени точно тогава, когато $R(f, g) = 0$. Теоремата е доказана.

Следствие 3. *Резултантата $R(f, g)$ на полиномите* (1) *е равна на нула тогава и само тогава, когато или $a_0 = b_0 = 0$, или $f(x)$ и $g(x)$ имат поне един общ корен.*

Може да се докаже (вж. [20], стр. 199), че ако $a_0 \neq 0$ и $b_0 \neq 0$, то

$$(5) \qquad R(f, g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j),$$

където $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta_1, \beta_2, \ldots, \beta_m$ са съответно корените на $f(x)$ и $g(x)$.

С помощта на детерминантата $R = R(f, g)$ и някои нейни минори могат да се намерят необходими и достатъчни условия, при които полиномите (1) имат точно k общи корена, където k не надминава m и n. Действително нека k_1 е минорът от $(m+n-2)$-ри ред, който се получава от R след зачеркване на първия и последния ред и първия и последния стълб. По същия начин от R_1 получаваме минора R_2 от $(m+n-4)$-ти ред и т. н. Оказва се, че е вярна следната теорема (вж. [20], стр. 207).

Теорема 6. *Полиномите $f(x)$ и $g(x)$ от (1) при $a_0 \neq 0$ и $b_0 \neq 0$ имат точно k $(1 \leqq k \leqq \min\{m, n\})$ общи корена тогава и само тогава, когато $R = R_1 = \ldots = R_{k-1} = 0$ и $R_k \neq 0$.*

Ако

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \quad (a_0 \neq 0)$$

е полином от степен $n \geqq 1$ с корени $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $f'(x)$ е неговата първа производна, то изразът

$$(6) \qquad \Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{n-2} f'(\alpha_1) f'(\alpha_2) \ldots f'(\alpha_n)$$

се нарича *дискриминанта* на полинома $f(x)$.

Очевидно е, че равенството $\Delta(f) = 0$ е необходимо и достатъчно условие, при което $f(x)$ има многократни корени. Освен това $\Delta(f)$ е симетричен полином на корените $\alpha_1, \alpha_2, \ldots, \alpha_n$ и следователно $\Delta(f)$ се изразява чрез коефициентите на $f(x)$. Едно такова изразяване може да се получи, като използуваме формулата (5) за резултантата $R(f, f')$ на полиномите $f(x)$ и $f'(x)$, откъдето съгласно (6) лесно получаваме, че

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} R(f, f').$$

Следователно дискриминантата $\Delta(f)$ може да се представи като детерминанта от $(2n-1)$-ви ред, на която елементите зависят само от коефициентите на $f(x)$. Ще посочим още едно представяне за $\Delta(f)$ във вид на детерминанта, която е от n-ти ред.

Чрез диференциране на равенството

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_n)$$

и полагане $x = \alpha_i$ получаваме, че

$$f'(\alpha_i) = a_0(\alpha_i-\alpha_1)(\alpha_i-\alpha_2) \ldots (\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1}) \ldots (\alpha_i-\alpha_n)$$

за всяко $i = 1, 2, \ldots, n$. Тогава от (6) следва, че

$$\Delta(f)=(-1)^{\frac{n(n-1)}{2}}a_0^{2n-2}(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_n)\cdot$$
$$(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_n)\cdot$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$(\alpha_n-\alpha_1)(\alpha_n-\alpha_2)\ldots(\alpha_n-\alpha_{n-1})=$$
$$=a_0^{2n-2}\prod_{1\leqq i<j\leqq n}(\alpha_i-\alpha_j)^2=a_0^{2n-2}\,\Delta_n^2,$$

ьдето

$$\Delta_n=\begin{vmatrix}1 & 1 & \ldots & 1\\ \alpha_1 & \alpha_2 & \ldots & \alpha_n\\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2\\ \ldots & \ldots & \ldots & \ldots\\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1}\end{vmatrix}=\prod_{1\leqq i<j\leqq n}(\alpha_i-\alpha_j).$$

Ако умножим Δ_n със себе си по правилото „ред по ред“ ще получим формулата

$$\Delta(f)=a_0^{2n-2}\begin{vmatrix}S_0 & S_1 & \ldots & S_{n-1}\\ S_1 & S_2 & \ldots & S_n\\ \ldots & \ldots & \ldots & \ldots\\ S_{n-1} & S_n & \ldots & S_{2n-2}\end{vmatrix},$$

където S_k ($k=0, 1, \ldots, 2n-2$) са степенните сборове на корените $\alpha_1, \alpha_2, \ldots, \alpha_n$ и могат да се изразят чрез коефициентите на полинома $f(x)$ по формулите на Нютон.

Задача. Проверете, че дискриминантата на квадратния тричлен $f(x)=ax^2+bx+c$ в $\Delta(f)=b^2-4ac$.

Ще отбележим още едно приложение на дискриминантата на два полинома.

Нека $f(x, y)$ и $g(x, y)$ са полиноми на неизвестните x и y с коефициенти от числовото поле P. Решение на системата уравнения

$$(7)\qquad \begin{vmatrix} f(x, y)=0\\ g(x, y)=0\end{vmatrix}$$

е нарича всяка двойка от комплексни числа α и β, за които $f(\alpha, \beta)=g(\alpha, \beta)=0$.

Да запишем $f(x, y)$ и $g(x, y)$ във вида

$$f(x, y)=a_0(y)x^r+a_1(y)x^{r-1}+\ldots+a_r(y)\quad (r\geqq 1),$$
$$g(x, y)=b_0(y)x^s+b_1(y)x^{s-1}+\ldots+b_s(y)\quad (s\geqq 1),$$

където коефициентите $a_i(y)$ и $b_j(y)$ са полиноми от $P[y]$.

Нека $R(y)=R(f, g)$ е резултантата на f и g, разглеждани като полиноми на x с коефициенти от $P[y]$. Очевидно е, че $R(y)\in P[y]$. Ако (α, β) е решение на системата (7), то полиномите $f(x, \beta)$ и $g(x, \beta)$ имат общ корен $x=\alpha$. Тогава от следствие 3 получаваме, че тяхната резултанта $R(\beta)$ е равна на нула.

Обратно, ако $y=\beta$ е корен на резултантата $R(y)$, то пак от следствие 3 следва, че или $a_0(\beta)=b_0(\beta)=0$, или $f(x, \beta)$ и $g(x, \beta)$ имат общ корен $x=\alpha$. Във втория случай (α, β) ще бъде решение на системата (7). Когато $a_0(\beta)=b_0(\beta)=0$, полиномите могат да имат, а могат и да нямат общ корен.

По този начин намирането на решенията на системата (7) се свежда, първо, до намиране на корените на полинома $R(y)=R(f, g)$, получен, както се казва, чрез изключване на неизвестното x, и, второ — до намиране на общите корени на полиномите $f(x, \beta)$ и $g(x, \beta)$ за всеки корен β на полинома $R(y)$.

Ще отбележим, че по подобен начин може да се разглежда въпросът за решенията на произволна система, левите страни на която са полиноми на n неизвестни. Обаче този въпрос е предмет на изучаване на отделна математична дисциплина, наречена *алгебрична геометрия.*

ГЛАВА IV

ГРУПИ

§ 1. Определение на група. Примери

Ще пристъпим към изучаването на един от основните раздели на алгебрата — теорията на групите.

Определение 1. Ще казваме, че в множеството M е определена *бинарна (двуместна) алгебрична операция*, ако на всеки два (различни или еднакви) елемента a и b от това множество, взети в определен ред, е съпоставен по някакъв закон еднозначно определен трети елемент c от M.

Тази операция можем да наречем *събиране* и тогава елементът c наричаме *сума* на елементите a и b и го означаваме със символа $c=a+b$; операцията можем да наречем *умножение* — тогава c наричаме *произведение* на елементите a и b и пишем $c=a.b$; операцията можем да записваме и по някакъв друг начин, например „$*$“, т. е. $c=a*b$, със символа „$\circ$“, т. е. $c=a\circ b$ и т. н. Ако разглеждаме дадено множество M спрямо операцията „$*$“, често ще пишем $M=M(*)$.

Събирането и умножението се нарича съответно *адитивна* и *мултипликативна* бинарна операция, а самото им записване *адитивно* и *мултипликативно*. Бинарната алгебрична операция в множеството M може да се разглежда като двуаргументова функция f, аргументите на която се изменят в M, и област от стойностите ѝ — същото множество, т. е. това би могло да се запише, както е прието, $c=f(a, b)$.

Виждаме, че в определението на понятието алгебрична операция се изисква еднозначност на операцията, изпълнимостта ѝ за всеки два елемента, указанието на реда, в който се вземат конкретните елементи от множеството M при изпълнението на операцията, т. е. не е изключена възможността на двойката елементи a, b от M и на двойката b, a да са съпоставени различни елементи c и d от M или, по друг начин казано, разглежданата операция да е некомутативна. Това означава, че в общия случай са възможни условията $a.b\neq b.a$, $a+b\neq b+a$, $a*b\neq b*a$, $a\circ b\neq b\circ a$.

Като примери за алгебрични операции можем да посочим умножението на субституции, умножението на матрици, на линейни преобразувания, изваждането на цели числа, събирането на вектори, събирането на числа и т. н. Първите четири от посочените операции са некомутативни.

Стойността c на бинарната операция f върху двойката елементи a, b ще записваме обаче не във вида $c=f(a, b)$, както в анализа, а във вида $c=ab$, $c=a+b$ и т. н. С това се икономисват

три символа и едновременно се получава аналогия с означенията на числовите операции: пишем $-2+6=4$, а не $f(-2, 6)=4$.

Обикновено бинарните операции ще записваме мултиплика-тивно (точката почти винаги ще изпускаме), тъй като разглежда-нията за умножението се пренасят автоматично и за другояче записаните бинарни алгебрични операции. Понякога ще използу-ваме и адитивното записване, а ако се налагат и други означе-ния, това изрично ще посочваме. Вместо бинарна алгебрична опе-рация за краткост ще казваме само алгебрична операция, тъй като няма да въвеждаме други алгебрични операции, например унарна (едноместна), тернарна (триместна), n-арна (n-местна).

Определение 2. Множеството G се нарича *група* (мултипли-кативно записана), а в него е въведена алгебрична операция ум-ножение, която е асоциативна, т. е.

$$(ab)c=a(bc)\ (a, b, c\in G)$$

и за всеки два елемента a и b от G уравненията

$$ax=b,\ ya=b \tag{1}$$

притежават единствени решения x и y в G. Ще казваме още че G е *група спрямо умножението.*

Ще отбележим изрично, че горните две уравнения не са ед-ни и същи, тъй като умножението не е задължително комута-тивно.

Ако групата G има краен брой елементи, то тя се нарича *крайна*, броят $|G|$ на елементите ѝ — *ред* или *мощност* на група-та. В противен случай G се нарича *безкрайна* група. Групата G се нарича *комутативна* или *абелева* (в чест на норвежкия ма-тематик Н. Х. Абел), ако операцията в G е комутативна, т. е. $ab=ba$ за всеки два елемента a и b от G. Ако операцията в G е наречена събиране, то за G се казва, че е адитивно записана група. Ако $ab=ba$ за $a, b\in G$, казваме, че елементите а и b на G комутират.

Преди да посочим някои елементарни следствия от опреде-лението на група, ще отбележим, че не всяка алгебрична опера-ция е асоциативна. Например операцията $*$, дефинирана в мно-жеството $\mathbf{R}$ на реалните числа по следния начин: $a*b=a^2b^2$, къ-дето a и b са реални числа, не е асоциативна. Неасоциативна е например и операцията изваждане на реални числа.

1. Следствия от асоциативния закон. Асоциативният закон $a(bc)=(ab)c$ ни позволява да говорим за еднозначно определено произведение abc на три елемента и за трета степен на елемент в групата G*. Въобще може да се докаже по индукция, че произведението на n елемента $a_1, a_2, \ldots, a_n$ е еднозначно опре-делено, т. е. не зависи от разположението на скобите. Това произ-

*Именно кой да е от двата съвпадащи елемента $a(bc)$ и $(ab)c$ наричаме произведение на a, b и c и го означаваме с abc.

ведение бележим с $a_1a_2\ldots a_n$. Специално при $a_1=a_2=\ldots=a_n=a$ получаваме степента a^n на елемента a.

2. **Съществуване и единственост на единичен елемент в групата** G. Нека a е произволен елемент на групата G. Да разгледаме уравнението $ax=a$. Съгласно определението за група това уравнение притежава единствено решение e_a, т. е.

$$ae_a=a.$$

Индексът a в e_a означава, че e_a зависи евентуално от елемента a. Ще покажем обаче, че $be_a=b$ и за произволен друг елемент b от G, т. е. e_a е *дясна единица* в G. Наистина уравнението $ya=b$ притежава единствено решение y в групата G и следователно

$$be_a=(ya)e_a=y(ae_a)=ya=b,$$

т. е. елементът e_a е дясна единица в G. Да я означим с e'. По същия начин от еднозначната решимост на уравнението $ya=a$ получаваме, че в групата G има и *лява единица* e'', т. е. $e''b=b$ за всяко b от G. Но всяка лява единица съвпада с всяка дясна единица в групата. Наистина, тъй като e'' е лява единица, то $e''e'=e'$ и понеже e' е дясна единица, то $e''e'=e''$. Следователно $e'=e''$. По такъв начин във всяка група G съществува такъв единствен елемент e, че

$$ea=ae=a$$

за всяко a от G. Елементът e се нарича *единица* на групата G (*единичен елемент, неутрален елемент*) и се означава даже със символа 1 (да не се бърка с числото 1!).

3. **Съществуване и единственост на обратен елемент.** От определението на понятието група следва, че уравненията $ax=1$ и $ya=1$ притежават съответно единствени решения a' и a'', т. е.

$$aa'=1,\quad a''a=1.$$

Обаче от равенствата

$$a''aa'=a''(aa')=a''\cdot 1=a'',$$
$$a''aa'=(a''a)a'=1\cdot a'=a'$$

следва, че $a'=a''$. Този елемент се нарича *обратен* на a и се означава с a^{-1}, т. е.

$$aa^{-1}=a^{-1}a=1. \tag{2}$$

Следователно a^{-1} е онзи единствен елемент от групата G, за който са изпълнени равенствата (2). Тогава от тези равенства следва, че обратен на a^{-1} е елементът a, т. е.

$$(a^{-1})^{-1}=a.$$

От очевидното равенство

$$(a_1a_2\ldots a_n)(a_n^{-1}a_{n-1}^{-1}\ldots a_2^{-1}a_1^{-1})=1$$

следва, че произведението на елементите във вторите скоби е елемент, обратен на $a_1a_2\ldots a_n$, т. е.

$$(a_1a_2\ldots a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\ldots a_2^{-1}a_1^{-1}.$$

Следователно обратният елемент на произведение от няколко елемента е произведение от обратните елементи на множителите взети в обратен ред.

4. Ако групата G е абелева, то ясно е, че във всяко произведение на елементи от G местата на множителите може да се разместят по произволен начин.

Ще отбележим, че ако операцията в групата G е записана адитивно, то вместо за единичен елемент e и обратен елемент a^{-1} в G ще говорим съответно за нулев елемент 0 и противоположен елемент $-a$ на a и следователно ще бъдат изпълнени равенствата $a+0=a$, $a+(-a)=0$, $-(-a)=a$ за всеки елемент a от G.

Твърдение 1. *Множеството G с една асоциативна операция умножение е група тогава и само тогава, когато в G съществува единичен елемент и всяко a от G притежава в G обратен елемент a^{-1}.*

Доказателство. Необходимостта беше установена по-горе. Ще докажем достатъчността. Нека в групата G съществува единица и всеки елемент има обратен. Непосредствено се проверява, че уравненията (1) притежават решения $x=a^{-1}b$ и $y=ba^{-1}$. Единствеността на решенията на (1) следва също тривиално: ако например първото уравнение на (1) притежава решения x_1 и x_2, то $ax_1=ax_2$ и като умножим двете части на това равенство отляво с a^{-1}, получаваме $x_1=x_2$.

Задача. Да се покаже, че във всяка група G е в сила законът за съкращение, т. е. от $aa_1=aa_2$ или от $a_1a=a_2a$ следва $a_1=a_2$.

Примери.

1. Множествата **Z**, **Q**, **R** и **C** съответно на целите, рационалните, реалните и комплексните числа са групи спрямо обикновената операция събиране на числа. Тези групи се наричат съответно *адитивни групи* на целите, рационалните, реалните и на комплексните числа и се означават съответно $\mathbf{Z}(+)$, $\mathbf{Q}(+)$, $\mathbf{R}(+)$ и $\mathbf{C}(+)$.

Спрямо събирането обаче не всяко числово множество образува група. Например множествата на положителните реални числа и на нечетните числа не са групи относно събирането.

2. Множествата на рационалните, реалните и комплексните числа не са групи спрямо умножението, обаче същите множества без нулата образуват абелеви групи спрямо умножението, които ще означаваме съответно с $\mathbf{Q}^*$, $\mathbf{R}^*$ и $\mathbf{C}^*$, т. е. $\mathbf{Q}^*=(\mathbf{Q}\setminus\{0\})(.)$, $\mathbf{R}^*=(\mathbf{R}\setminus\{0\})(.)$ и $\mathbf{C}^*=(\mathbf{C}\setminus\{0\})(.)$. Положителните реални числа образуват група спрямо умножението на числа, която ще означаваме с $\mathbf{R}^+$ и ще наричаме *мултипликативна група* на положителните числа. Множествата на целите и на отрицателните числа не са групи спрямо умножението.

В множеството **Z** на целите числа числата 1 и -1 образуват група спрямо умножението, която ще означаваме със $\mathbf{Z}^*$. Тази група е от ред 2.

3. Множеството U на всички комплексни числа x, за които $|x|=1$, т. е. числата от единичната окръжност образуват абелева група спрямо умножението. Наистина ако x и x_1 са от U, то $xx_1 \in U$, тъй като $|xx_1|=|x|\,|x_1|=1$. Асоциативният и комутативният закон са изпълнени, $1 \in U$ и $x^{-1} \in U$, тъй като $|x^{-1}|=|x|^{-1}=1$.

4. Множеството $C(n)$ на комплексните числа, които удовлетворяват уравнението $x^n=1$, е абелева група спрямо умножението, наречена *мултипликативна група на корените на единицата от степен n*. Наистина ако x_1 и x_2 са два корена на това уравнение, т. е. корени на единицата от n-та степен, то x_1x_2 и x_1^{-1} са също корени на горното уравнение и тъй като асоциативният и комутативният закон за умножението са изпълнени, то $C(n)$ е крайна абелева група от ред n. По такъв начин за всяко естествено число n съществува крайна група от ред n.

5. Всяко реално линейно пространство V е абелева група относно операцията събиране на вектори.

6. Множеството $M(n, \mathbf{C})$ на всички квадратни матрици от ред n, елементите на които са комплексни числа, е абелева група относно операцията събиране на матрици. Това множество спрямо операцията умножение на матрици не е група, тъй като не всяка матрица от $M(n, \mathbf{C})$ притежава обратна.

7. Множеството $GL(n, \mathbf{C})$ на всички неособени квадратни матрици от n-ти ред, елементите на които са комплексни числа, е група спрямо умножението на матрици. Наистина произведението на неособени матрици е неособена матрица, асоциативният закон за умножение на матрици е изпълнен, единичната матрица е неособена и за всяка неособена матрица съществува обратна, която също е неособена. Групата $GL(n, \mathbf{C})$ се нарича *обща линейна* или *обща матрична група*. Не е трудно да се види, че при $n \geqq 2$ групата $GL(n, \mathbf{C})$ е некомутативна.

Групи относно умножението на матрици образуват и следните подмножества на $GL(n, \mathbf{C})$: подмножеството $SL(n, \mathbf{C})$, което се състои от матриците, чиито детерминанти са равни на единица; подмножеството $D(n, \mathbf{C})$ от неособените диагонални матрици; подмножеството $T(n, \mathbf{C})$ от неособените матрици с нулеви елементи под главния диагонал; подмножеството $UT(n, \mathbf{C})$ от матриците с нули под главния диагонал и с единици по диагонала. Тези групи се наричат съответно *специална линейна група, диагонална група, триъгълна група* и *унитриъгълна група*.

8. Множеството $GL(V)$ на неособените линейни преобразувания на реалното линейно пространство V е група спрямо умножението на преобразувания.

9. Множеството $O(V)$ на ортогоналните линейни преобразувания на реалното евклидово пространство V е група спрямо умножението на преобразувания.

§ 2. Група от взаимно еднозначните преобразувания на едно множество. Изоморфизъм на групи

Определение 3. Казваме, че е дадено *изображение* (*съответствие*, *функция*) φ на множеството M в множеството W (символично пишем $\varphi: M \to W$), ако на всеки елемент a от M е съпоставен еднозначно определен елемент u от W, наречен образ на a при изображението φ, което ще записваме по следния начин: $\varphi(a)=u$ или $a \xrightarrow{\varphi} u$. Самият елемент a се нарича *първообраз* на u при изображението φ.

Ако всеки елемент от множеството W има първообраз при това изображение, то φ се нарича изображение на M върху W. Ако φ е изображение на множеството M в същото множество M, то φ се нарича преобразуване на M.

Определение 4. Изображението φ на множеството M върху множеството W се нарича *взаимно еднозначно* (*еднозначно обратимо* или (1, 1)-*значно*), ако всеки два различни елемента от M имат различни образи в W при изображението φ.

Казваме, че множествата M и W са *равномощни*, ако може да се установи взаимно еднозначно съответствие на едното множество върху другото. Символично това записваме така: $M \equiv W$.

Например изображението φ, което съпоставя на всяко положително число p неговия десетичен логаритъм q, т. е. $\varphi(p)=q$, където $q=\lg p$, е взаимно еднозначно изображение на множеството $\mathbf{R}^+$ на положителните реални числа върху множеството $\mathbf{R}$ на реалните числа. Също така изображението φ, което съпоставя на всяко реално число x числото $ax+b$, където $a \neq 0$ и b са фиксирани числа от $\mathbf{R}$, е взаимно еднозначно изображение на $\mathbf{R}$ върху $\mathbf{R}$ или преобразуване на $\mathbf{R}$.

Нека M е произволно множество и S_M е множеството от взаимно еднозначните изображения на M върху себе си. Тези изображения, т. е. преобразувания на M, ще означаваме с буквите $f, g, h, \ldots$ Произведение gf на такива изображения f и g се нарича резултатът от тяхното последователно изпълнение, т. е. под gf се разбира изображението, което действува на всеки елемент x от M по следния начин:

$$gf(x)=g[f(x)].$$

Ясно е, че gf е взаимно еднозначно изображение, т. е. елемент на S_M. По този начин в множеството S_M е определена алгебрична операция умножение. Ще покажем, че S_M е група спрямо тази операция.

а) *Умножението в S_M е асоциативно*, т. е.

$$h(gf)=(hg)f,$$

където f, g и h са произволни преобразувания от S_M. Наистина ако x е произволен елемент от M и $x \xrightarrow{f} x_1 \xrightarrow{g} x_2 \xrightarrow{h} y$, то $h(gf)(x)=h(x_2)=y$ и $(hg)f(x)=hg(x_1)=y$, т. е. $h(gf)=(hg)f$, тъй като образите на всяко x от M чрез $h(gf)$ и $(hg)f$ съвпадат.

б) *В S_M съществува поне една единица.* Наистина тъждественото преобразуване e на множеството M, което оставя всеки елемент на място, т. е. $e(x)=x$, $x \in M$, е очевидно взаимно еднозначно. Това преобразуване е единица на S_M, т. е. $fe=ef=f$ за всяко f от S_M. Наистина

$$fe(x)=f[e(x)]=f(x),$$

$$ef(x)=e[f(x)]=f(x),$$

откъдето $fe=ef=f$.

в) *Всяко преобразуване f от S_M притежава обратно преобразуване пак от S_M.* Наистина, тъй като f е взаимно еднозначно изображение на M върху себе си, то за произволен елемент x от M съществува единствен първообраз y от M при изображението f, за който

$$f(y)=x.$$

Дефинираме

$$f^*(x)=y.$$

В такъв случай $f^* \in S_M$ и

$$ff^*=f^*f=e,$$

т. е. f^* е обратен елемент на f. От твърдение 1 следва, че S_M е група, която ще наричаме *група от взаимно еднозначните преобразувания* на множеството M или *симетрична група* на M.

Ако множеството M има повече от два елемента, то S_M не е абелева група. Действително нека a, b и c са три различни елемента от M. Нека f_1 оставя всички елементи на M на място, освен a и b, като при това $f_1(a)=b$ и $f_1(b)=a$. Нека f_2 оставя всички елементи на M на място, освен a и c, като $f_2(a)=c$ и $f_2(c)=a$. Тогава f_1 и f_2 принадлежат на S_M и

$$f_2f_1 \neq f_1f_2,$$

тъй като $f_2f_1(b)=c$, но $f_1f_2(b)=a$ и $a \neq c$.

Ако M се състои от n елемента $a_1, a_2, \ldots, a_n$, то преобразуването f от S_M се означава чрез

$$f=\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1' & a_2' & \ldots & a_n' \end{pmatrix},$$

където $a_i'=f(a_i)$, а групата S_M — със S_n. Тъй като естеството на елементите $a_1, a_2, \ldots, a_n$ не е от значение, можем да считаме, че M се състои от числата $1, 2, \ldots, n$ и тогава

$$f=\begin{pmatrix} 1 & 2 & \ldots & n \\ i_2 & i_2 & \ldots & i_n \end{pmatrix}, \tag{1}$$

където $i_s=f(s)$. В този случай, както е известно, преобразуването f се нарича *субституция от n-та степен*, а групата S_n — *симетрична група от n-та степен*. Тъждествената субституция и обратната субституция f^{-1} в този случай са

(2) $$e=\begin{pmatrix}1 & 2 \dots n\\ 1 & 2 \dots n\end{pmatrix} \text{ и } f^{-1}=\begin{pmatrix}i_1 & i_2 \dots i_n\\ 1 & 2 \dots n\end{pmatrix}.$$

Една субституция се нарича *четна*, ако в горния и долния ред пермутациите ѝ са едновременно четни или едновременно нечетни, т. е. ако общият брой на инверсиите ѝ в горния и долния ред е четен. В противен случай субституцията се нарича *нечетна*.

Очевидно е, че при разместването на два стълба в една субституция четността ѝ не се променя, тъй като и двете пермутации променят едновременно четността си. Тогава ако всички субституции от n-та степен запишем по растящ ред на числата от първите им пермутации, то тяхната четност ще се определя от четността на вторите им пермутации. Следователно броят на четните субституции от n-та степен е равен на броя на нечетните т. е. този брой е равен на $\frac{n!}{2}$ при $n \geqq 2$.

Елементите на множеството M ще наричаме още *символи* на субституциите на M. Ще разглеждаме един специален начин на записване на субституциите, от който лесно може да се установи дали те са четни или нечетни.

Ако $i_1, i_2, \dots, i_s (s \geqq 1)$ са s различни елемента от M, то с $(i_1\ i_2 \dots i_s)$ се означава субституцията, която изобразява i_j в i_{j+1} за $j=1, 2, \dots, s-1$, i_s изобразява в i_1, а на всички останали елементи на M действува тъждествено. Субституцията $(i_1\ i_2 \dots i_s)$ се нарича *цикъл с дължина* s. Очевидно всеки цикъл с дължина 1 съвпада с тъждествената субституция. Циклите с дължина 2 се наричат транспозиции. Например

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 2 & 4 & 3 & 5 & 7 & 6 & 9 & 8 & 1\end{pmatrix}=(1\ 2\ 4\ 5\ 7\ 9).$$

Два цикъла $\sigma=(i_1\ i_2 \dots i_s)$ и $\tau=(j_1\ j_2 \dots j_t)$ се наричат *независими*, ако $i_k \neq j_r$ за $k=1, 2, \dots, s$ и $r=1, 2, \dots, t$, т. е. символите в записите на посочените цикли образуват две непресичащи се множества. Очевидно е, че *независимите цикли комутират*, т. е. ако σ и τ са независими цикли, то $\sigma\tau=\tau\sigma$.

Ще посочим някои свойства на субституциите, в които се използува записването им във вид на цикли.

1) *Всяка негединична субституция се разлага в произведение на независими цикли с дължина, по-голяма от 1; и това разлагане е еднозначно с точност до реда на записване на множителите.*

Доказателство. Нека σ е негединична субституция на симетричната група S_n. Доказателството ще проведем с индукция спрямо броя на разместваните от σ символи, т. е. относно броя на естествените числа i, за които $\sigma(i) \neq i$, $1 \leqq i \leqq n$. Тъй като σ не е тъждествената субституция, съществува такова i, че $\sigma(i) \neq i$. Също така съществува такова j, че $\sigma(j)=i$. Тъй като $i \neq j$, то σ

размества най-малко два символа. Ако σ размества само символите i и j, то $\sigma(i)=j$ и $\sigma=(i\,j)$ е транспозиция! Следователно, когато σ размества само два символа, σ има посоченото разлагане (с един множител).

Нека σ размества k символа ($k>2$) и i_1 е един от тях. Тъй като редицата $i_1, i_2, \ldots, i_{n+1}$, където $i_r=\sigma(i_{r-1})(r=2, 3, \ldots, n+1)$ има $n+1$ члена и i_j са естествени числа, не по-големи от n, то поне два члена на тази редица съвпадат. Нека i_s е първият член от редицата, който съвпада с някой от следващите го, т. е. $i_s=i_t$ за $s<t\leqq n+1$ и s е минималното число с това свойство. Ако $s>1$, то $\sigma(i_{s-1})=i_s=i_t=\sigma(i_{t-1})$ и затова $i_{s-1}=i_{t-1}$ $(s-1<t-1)$, което противоречи на избора на i_s. Следователно $i_1=i_t$ за някое t $(3\leqq t\leqq n+1)$. Нека τ_1 е цикълът $(i_1\ i_2 \ldots i_{t-1})$, който има дължина $t-1\geqq 2$. Лесно се вижда, че субституцията $\sigma_1=\tau_1^{-1}\cdot\sigma$ оставя неподвижни числата $i_1, i_2, \ldots, i_{t-1}$ и всички числа, които σ оставя неподвижни, т. е. σ_1 размества $k-t+1$ символа. Ако $k-t+1=0$, то σ_1 е тъждествената субституция и $\sigma=\tau_1$ е разлагане на σ от посочения вид. Ако $k-t+1>0$, поради $k>k-t+1$ прилагаме предположението на индукцията и получаваме разлагане $\sigma_1=\tau_2\tau_3\ldots\tau_m$ на σ_1 в произведение на независими цикли с дължина, по-голяма от 1. Понеже σ_1 оставя неподвижни числата $i_1, i_2, \ldots, i_{t-1}$, то $\sigma=\tau_1\tau_2\ldots\tau_m$ е разлагане на σ в произведение на независими цикли с дължина, по-голяма от 1.

Еднозначността на разлагането се доказва с индукция спрямо броя m на множителите. Нека $\sigma=\pi_1\pi_2\ldots\pi_s$ е друго разлагане на σ в произведение на независими цикли с дължина, по-голяма от 1. Тъй като σ размества символа i_1, то i_1 ще участвува в един от циклите $\pi_1, \pi_2, \ldots, \pi_s$. След евентуална смяна на номерацията на циклите от второто разлагане можем да считаме, че i_1 се съдържа в цикъла π_1. Но тогава непосредствено от проведените по-горе разсъждения следва, че $\tau_1=\pi_1$ и $\sigma_1=\tau_2\ldots\tau_m=\pi_2\ldots\pi_s$. Тъй като σ_1 има разлагане на $m-1$ на брой независими цикли, то по предположението на индукцията $m-1=s-1$ и след евентуална смяна на номерацията на $\pi_2, \ldots, \pi_s$ ще имаме $\tau_2=\pi_2, \ldots, \tau_m=\pi_m$. Твърдението е доказано.

2) *Всяка субституция е произведение на транспозиции.*

Наистина всяка субституция е произведение на цикли, а всеки цикъл е произведение на транспозиции, което се вижда от равенството

$$(i_1\ i_2\ldots i_n)=(i_1\ i_2)(i_2\ i_3)\ldots(i_{n-1}\ i_n).$$

Разлагането на субституциите в произведения на транспозиции не е еднозначно, защото във всяко такова разлагане може да се добави произведението на две транспозиции от вида $(i\,j)$ и $(j\,i)$. По-нетривилен пример е разлагането

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(13)(12)=(12)(13)(12)(13).$$

3) *Ако една субституция* σ *се умножи с транспозицията* $(i\,j)$, *то новополучената субституция има четност, противоположна на четността на* σ.

Действително ако

$$\sigma=\begin{pmatrix}1 & \dots & i & \dots & j & \dots & n\\ k_1 & \dots & k_i & \dots & k_j & \dots & k_n\end{pmatrix},$$

то

$$\sigma(i\,j)=\begin{pmatrix}1 & \dots & i & \dots & j & \dots & n\\ k_1 & \dots & k_j & \dots & k_i & \dots & k_n\end{pmatrix},$$

т. е. $\sigma(i\,j)$ се получава от σ, като във втория ред на σ са сменени местата на k_i и k_j, което сменя четността на пермутацията от втория ред. Аналогично се разглежда произведението $(i\,j)\,\sigma$.

4) *Четността на броя на множителите във всички разлагания на една субституция в произведение на транспозиции е винаги една и съща и съвпада с четността на самата субституция.*

Това свойство следва непосредствено от 3).

5) *Произведението* $\sigma\tau$ *на две субституции е четна субституция точно тогава, когато* σ *и* τ *са едновременно четни или нечетни субституции.*

Наистина ако σ допуска разлагане в произведение на k транспозиции, а τ — на l транспозиции, то $\sigma\tau$ има разлагане в произведение на $k+l$ транспозиции.

Тъй като $k+l$ е четно число точно тогава, когато k и l имат еднаква четност, свойство 5) следва от свойство 4).

Подмножеството A_n на S_n, което се състои от четните субституции, образува група спрямо умножението на субституции. Наистина произведението на две четни субституции според свойство 5) е четна субституция.

Единичната субституция е четна и ако f е четна субституция, то f^{-1}, както се вижда от (1) и (2), е също четна. Разглежданата група A_n се нарича *алтернативна* или *знакопроменлива група* от степен n и има ред $\frac{n!}{2}$. Лесно може да се провери, че множеството на нечетните субституции от n-та степен не е група спрямо умножението на субституции.

Определение 5. Изображението φ на мултипликативно записаната група G върху мултипликативно записаната група H се нарича *изоморфизъм (изоморфно изображение)*, ако φ е взаимно еднозначно и φ изобразява произведението на всеки два елемента a и b от G в произведението от образите им, т. е.

$$\varphi(a\,b)=\varphi(a)\,\varphi(b). \tag{3}$$

Групите G и H се наричат *изоморфни* и записваме $G\cong H$, ако съществува изоморфизъм на едната група върху другата.

Ще отбележим, че ако операцията в групата G е означена с

„$\circ$“, а в H — със $*$, свойството (3) на изоморфизма φ се записва във вида

$$\varphi(a\circ b)=\varphi(a) * \varphi(b).$$

Задача. Докажете, че релацията „изоморфни“ е релация на еквивалентност.

Алгебрата е наука, която изучава главно алгебричните операции. За алгебрата е съществен въпросът, как се извършват алгебричните операции в дадени множества, при което тя може да не се интересува от естеството на множествата, в които те са дефинирани. Омаловажаването на втория факт ни дава основание изоморфните групи да считаме за неразлични от алгебрична гледна точка, макар че самите групи могат да имат съвършено различни по естество елементи.

Примери

1. Мултипликативната група $\mathbf{R}^+$ на положителните реални числа е изоморфна на адитивната група $\mathbf{R}(+)$ на реалните числа. Наистина нека $a>1$ е произволно фиксирано реално число. Известно е, че за всяко число $x\in\mathbf{R}^+$ съществува такова число $y\in\mathbf{R}(+)$, че $x=a^y$. Тогава да разгледаме изображението $\varphi:\mathbf{R}^+\to\mathbf{R}(+)$, където $\varphi(x)=y$. От свойствата на показателната функция следва, че φ е взаимно еднозначно изображение на R^+ върху $\mathbf{R}(+)$ и освен това

$$\varphi(x_1\ x_2)=\varphi(a^{y_1}\ a^{y_2})=\varphi(a^{y_1+y_2})=y_1+y_2=\varphi(x_1)+\varphi(x_2),$$

т. е. изображението φ е съгласувано с операциите в $\mathbf{R}^+$ и $\mathbf{R}(+)$ Следователно $\mathbf{R}^+\cong\mathbf{R}(+)$. Лесно е да се види, че в действителност изображението φ е операцията логаритмуване при основа a, т. е. логаритмуването е изоморфизъм на $\mathbf{R}^+$ върху $\mathbf{R}(+)$ и това негово свойство го прави така широко приложимо в математиката.

2. Адитивната група Z на целите числа е изоморфна на адитивната група $2Z$ на четните числа. Наистина изображението $\varphi:Z\to 2Z$, за което $\varphi(n)=2n$, е взаимно еднозначно изображение на Z върху $2Z$ и тъй като

$$\varphi(n+k)=2n+2k=\varphi(n)+\varphi(k),$$

то $Z(+)\cong 2Z(+)$. Този случай показва, че една безкрайна група може да бъде изоморфна на група, съдържаща се строго в нея.

Задача. Да се докаже, че мултипликативната група $\mathbf{C}^*$ е изоморфна на групата на всички неособени матрици от вида

$$\begin{pmatrix} a & b\\ -b & a\end{pmatrix},$$

където a и b са реални числа, снабдена с операцията умножение на матрици.

§ 3. Подгрупи

Определение 6. Непразнато подмножество A на групата G се нарича нейна *подгрупа*, ако A е група относно операцията, спрямо която G е група.

Съгласно това определение мултипликативната група R^+ на положителните реални числа не е подгрупа на адитивната група R на реалните числа, макар че R^+ е подмножество на R и R^+ е група.

Твърдение 2. *Ако A е непразно подмножество на групата G, то следните условия са еквивалентни:*

(*i*) *подмножеството A е подгрупа на групата G;*

(*ii*) *ако a и b са произволни елементи от A, то ab и a^{-1} също принадлежат на A;*

(*iii*) *подмножеството A съдържа заедно с всеки два свои елемента a и b и произведението ab^{-1}.*

Доказателство. Очевидно от (*i*) следват (*ii*) и (*iii*).

От (*ii*) следва (*iii*), тъй като ако $a,\ b \in A$, то $b^{-1} \in A$ и следователно $ab^{-1} \in A$.

От (*iii*) следва (*i*). Наистина нека a и b са произволни елементи от A. Тогава $1 = aa^{-1} \in A$ и $a^{-1} = 1.\ a^{-1} \in A$ за всяко $a \in A$. Така получаваме, че $b^{-1} \in A$ и затова $ab = a(b^{-1})^{-1} \in A$. Асоциативният закон за умножение е изпълнен за всички елементи на G, т. е. и за елементите на A. Следователно A е подгрупа на G. Твърдението е доказано.

Ясно е, че ако G е адитивна група, условието (*iii*) се заменя с изискването $a+(-b)$ да принадлежи на A.

Определение 7. Под *произведение*

$$AB = \{ab \mid a \in A,\ b \in B\}$$

на две подмножества A и B на групата G разбираме множеството от всевъзможните произведения ab, на G, където $a \in A$, $b \in B$, т. е. AB е множеството от онези елементи g на групата G, които могат да се представят поне по един начин във вида $g = ab$, където $a \in A$, $b \in B$.

В частност едно от множествата може да се състои от един единствен елемент. Разбира се, не е изключена възможността елементът g от AB да притежава и други представяния от такъв вид, т. е. освен $g = ab$ да имаме и $g = a_1 b_1$, $a_1 \in A$, $b_1 \in B$.

Като се използува последното определение, условието (*ii*) непразното подмножество A на групата G да бъде нейна подгрупа се записва във вида $AA \subseteq A$, $A^{-1} \subseteq A$, където

$$A^{-1} = \{a^{-1} \mid a \in A\}.$$

Тъй като е в сила асоциативният закон за умножение на елементите на групата G, този закон важи и за умножение на подмножества в групата G, т. е. за всеки три подмножества A, B и C на G е изпълнено условието

$$(AB)C = A(BC).$$

Примери

1. Подмножеството на групата G, което се състои само от единицата, е подгрупа на G, наречена *единична подгрупа*. Освен това самата група G е една от своите подгрупи. Тези две подгрупи ще наричаме тривиални (неистински, несобствени).

2. Всяка група от редицата

$$\mathbf{Z}(+) \subset \mathbf{Q}(+) \subset \mathbf{R}(+) \subset \mathbf{C}(+)$$

е подгрупа на всяка от следващите групи.

3. Същото се отнася и за редиците

$$\mathbf{Z}^* \subset \mathbf{Q}^* \subset \mathbf{R}^* \subset \mathbf{C}^*, \quad C(i) \subset U \subset \mathbf{C}^*.$$

4. Алтернативната група A_n е подгрупа на симетричната група S_n.

5. При $n \geqq 1$ специалната линейна група $SL(n, \mathbf{C})$ е подгрупа на общата линейна група $GL(n, \mathbf{C})$, диагоналната група $D(n, \mathbf{C})$ — на триъгълна група $T(n, \mathbf{C})$, унитриъгълната група $UT(n, \mathbf{C})$ е подгрупа на триъгълната група $T(n, \mathbf{C})$, а последната от своя страна — на групата $GL(n, \mathbf{C})$.

Твърдение 3. *Сечението на краен или безкраен брой подгрупи на групата G е подгрупа на G.*

Доказателство. Нека A и B са подгрупи на групата G. Сечението $A \cap B$ е затворено спрямо умножението и спрямо вземането на обратен елемент. Наистина ако g и h са два произволни елемента на $A \cap B$, то $g \in A$, $h \in A$ и следователно $gh \in A$ и $g^{-1} \in A$, понеже A като подгрупа на G е затворена спрямо умножението и спрямо вземането на обратен елемент. По същия начин се доказва, че $gh \in B$, и $g^{-1} \in B$, т. е. $gh \in A \cap B$ и $g^{-1} \in A \cap B$. Следователно $A \cap B$ е подгрупа на G.

Общият случай се доказва по аналогичен начин.

Благодарение на асоциативния закон можем да говорим за положителна степен g^n на елемента g като произведение на n елемента, равни на g. Под g^0 се условяме да разбираме единицата на G. За въвеждането на отрицателна степен на g предварително ще докажем, че при $n > 0$ имаме

$$(g^n)^{-1} = (g^{-1})^n. \tag{1}$$

Наистина

$$g^n (g^{-1})^n = gg \ldots g \cdot g^{-1} g^{-1} \ldots g^{-1} = 1,$$

откъдето виждаме, че вторият елемент $(g^{-1})^n$ е обратен на g^n. С това равенството (1) е установено. Под g^{-n} ще разбираме или $(g^n)^{-1}$, или неговото равно $(g^{-1})^n$.

Ако операцията в групата G е записана адитивно, т. е. $G = G(+)$, то вместо за степени на елемента g ще говорим за кратни ng на този елемент.

Задача. Да се покаже, че във всяка група G са в сила равенствата

(2) $$g^n g^m = g^{n+m},$$

(3) $$(g^n)^m = g^{nm},$$

където n и m са произволни цели числа, а $g \in G$.

Нека $\langle g \rangle$ е подмножеството на групата G, което се състои от всички степени на елемента g. Това подмножество е подгрупа на G, тъй като, произведението на две степени на g поради (2) е степен на g, т. е. подмножеството $\langle g \rangle$ е затворено спрямо умножението и освен това обратният елемент $(g^n)^{-1}$ на елемента g^n поради (3) е степента g^{-n} от $\langle g \rangle$, т. е. $\langle g \rangle$ е затворено и спрямо вземането на обратен елемент. Подгрупата $\langle g \rangle$ се нарича *циклична подгрупа* на групата G, породена от елемента g. Самият елемент g се нарича *образуващ* или *пораждащ елемент* на цикличната група $\langle g \rangle$.

Очевидно

$$g^n \cdot g^m = g^{n+m} = g^m \cdot g^n,$$

т. е. $\langle g \rangle$ е абелева група дори в случая, когато изходната група G е некомутативна.

Ако в мултипликативната група C^* разгледаме степените на числото 3, виждаме, че всички те са различни, а от степените на числото i само четири са различни. Подобна картина може да се наблюдава и в общия случай, за който разглеждаме следните две възможности.

1. Всички степени на елемента g са различни. В този случай цикличната група $\langle g \rangle$ е безкрайна.

2. Поне две степени на елемента g са равни. Нека например $g^k = g^l$ и $k > l$. Тогава получаваме

$$g^{k-l} = 1,$$

т. е. съществуват положителни степени на g, равни на 1.

Нека n е най-малкото цяло положително число, за което $g^n = 1$, т. е. ако $t > 0$, $g^t = 1$, то $t \geqq n$. Ще покажем, че цикличната подгрупа $\langle g \rangle$ се изчерпва с елементите

$$1, g, g^2, \ldots, g^{n-1},$$

които са различни помежду си. Наистина ако допуснем, че

$$g^k = g^l \quad (0 \leqq l < k < n),$$

то получаваме

$$g^{k-l} = 1 \quad (0 < k-l < n),$$

което е невъзможно. Всяка друга степен g^k на елемента g съвпада с някой от посочените елементи. Действително имаме

$$k = nq + r, \quad 0 \leqq r < n,$$

и следователно

$$g^k = g^{nq+r} = (g^n)^q \cdot g^r = g^r.$$

Определение 8. Казваме, че елементът g на групата G *има*

безкраен ред, ако всички негови степени са различни помежду си, т. е. ако равенството $g^m = 1$ е възможно само тогава, когато $m = 0$. Казваме, че елементът g *има ред* n, ако n е най-малкото естествено число, за което $g^n = 1$.

Реда на елемента g означаваме с $|g|$. Когато g има безкраен ред, пишем $|g| = \infty$.

Групата G притежава един-единствен елемент от ред 1, а именно елемента 1 и очевидно цикличната група $\langle 1 \rangle$ съвпада с единичната подгрупа.

Следствие 1. *Ако елементът* g *има краен ред* n, *то цикличната група* $\langle g \rangle$ *има ред* n.

Наистина всички елементи на цикличната група $\langle g \rangle$ в този случай ще бъдат елементите $1, g, g^2, \ldots, g^{n-1}$, които са различни помежду си.

Следствие 2. *Ако елементът* g *има краен ред* n, *то* $g^m = 1$ *тогава и само тогава, когато* n *дели* m.

Действително нека $g^m = 1$ и $m = nq + r (0 \leqq r < n)$. Тогава

$$1 = g^m = g^{nq+r} = (g^n)^q g^r = g^r,$$

откъдето следва, че $r = 0$ и затова n/m. Обратно, ако n дели m, т. е. $m = nq$, то очевидно $g^m = 1$.

Определение 9. Групата G се нарича *периодична*, ако всички нейни елементи имат крайни редове, и *група без торзии* — ако всички нейни неединични елементи имат безкраен ред. Групата G се нарича *смесена*, ако тя притежава както елементи от безкраен ред, така и неединични елементи от крайни редове.

Очевидно всяка крайна група е периодична. Без торзии са например мултипликативната група $\mathbf{R}^+$ и адитивните групи $\mathbf{Z}(+)$, $\mathbf{Q}(+)$, $\mathbf{R}(+)$ и $\mathbf{C}(+)$. Смесени групи са мултипликативните групи $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ и $\mathbf{U}$, тъй като те съдържат както елементи от безкраен ред (например числото $\cos \pi^2 + i \sin \pi^2$), така и елементи от краен ред (например числото -1).

Твърдение 4. *Ако* A *и* B *са подгрупи на групата* G, *то произведението* AB *е подгрупа на групата* G *тогава и само тогава, когато* $AB = BA$.

Доказателство. Нека за подгрупите A и B на групата G е изпълнено равенството $AB = BA$, а g и h са два произволни елемента на подмножеството AB. Тогава $g = ab$ и $h = a_1 b_1$ за някои елементи $a, a_1 \in A$ и $b, b_1 \in B$. Елементът ba_1 се съдържа в $BA = AB$ и затова съществуват такива елементи a_2 от A и b_2 от B, че $ba_1 = a_2 b_2$. Тогава

$$gh = (ab)(a_1 b_1) = a(ba_1)b_1 = a(a_2 b_2) b_1 = (aa_2)(b_2 b_1),$$

т. е. $gh \in AB$. Елементът $g^{-1} = b^{-1} a^{-1}$ е елемент от подмножеството $BA = AB$ и затова $g^{-1} \in AB$. Следователно според твърдение 2 AB е подгрупа на G.

Обратно, да допуснем, че подмножеството AB е подгрупа на G. Ще покажем, че $BA \subseteq AB$. Наистина, ако g е произволен елемент от BA, то

$$g=ba=(1\,.\,b)\,.\,(a\,.\,1).$$

Тъй като $1\,.\,b\in AB$, $a\,.\,1\in AB$ и AB е подгрупа на G, то AB съдържа произведението на двата свои елемента $1\,.\,b$ и $a\,.\,1$, т. е. $g\in AB$ и затова $BA\subseteq AB$.

Ще покажем, че $AB\subseteq BA$. Действително ако h е произволен елемент от AB, то

$$h=ab=(b^{-1}\,a^{-1})^{-1}, \tag{3}$$

Обаче $b^{-1}\,a^{-1}=(1\,.\,b^{-1})\,(a^{-1}\,.\,1)\in AB$, тъй като подгрупата AB съдържа произведението на двата свои елемента $1\,.\,b^{-1}$ и $a^{-1}\,.\,1$. Понеже $b^{-1}\,a^{-1}\in AB$, съществуват такива елементи $a_1\in A$ и $b_1\in B$, че

$$b^{-1}\,a^{-1}=a_1b_1.$$

Като заместим $b^{-1}\,a^{-1}$ с неговото равно в (3), получаваме

$$h=ab=(a_1b_1)^{-1}=b_1^{-1}a_1^{-1}\in BA,$$

т. е. $AB\subseteq BA$, с което твърдението е доказано.

Задача. Да се покаже, че ако A и B са крайни подгрупи на групата G, то

$$|AB|=\frac{|A|\,.\,|B|}{|A\cap B|}.$$

§ 4. Циклични групи

Определение 10. Групата G се нарича *циклична*, ако тя се състои от степените на един от своите елементи g, т. е. ако съвпада с цикличната подгрупа $\langle g\rangle$. Елементът g се нарича *образуващ* или *пораждащ елемент* на G.

Разбира се, адитивната група G е циклична, ако тя се състои от кратните на един от своите елементи g. В предишния параграф показахме, че всяка циклична група е абелева.

Адитивната група Z на целите числа е циклична, тъй като всеки елемент на Z е кратен на числото 1, т. е. $Z=\langle 1\rangle$. Освен числото 1 за образуващ елемент може да се вземе числото -1, т. е. $Z=\langle -1\rangle$.

Като пример за крайна циклична група от ред n служи мултипликативната група $C(n)$ на n-тите корени на единицата. Именно ако $\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$, то $C(n)$ се състои от елементите $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$. Оказва се, че с точност до изоморфизъм групите $Z(+)$ и $C(n)$ при $n=1, 2, \ldots$ изчерпват всички циклични групи.

Теорема 1. *Всички безкрайни циклични групи са изоморфни на адитивната група Z на целите числа. Всички крайни циклични групи от даден ред n са изоморфни на мултпликативната група $C(n)$ на n-тите корени на единицата.*

Доказателство. Нека G е безкрайна циклична група с образуващ елемент g. Очевидно съответствието $\varphi: G \to Z$, за което $\varphi(g^k) = k$, е взаимно еднозначно изображение на G върху Z. Тъй като

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = k + l = \varphi(g^k) + \varphi(g^l),$$

то φ изобразява произведение на два елемента от G в сумата от образите им в Z. Следователно φ е изоморфизъм, т. е. $G(\,.\,) \simeq Z(+)$.

Нека сега G е крайна циклична група от ред n с образуващ елемент g и нека $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Групите G и $C(n)$ се състоят съответно от елементите g^k и ε^k, където $k = 0, 1, \ldots, n-1$. Съответствието $\varphi: G \to C(n)$, за което

$$\varphi(g^k) = \varepsilon^k \quad (k = 0, 1, \ldots, n-1)$$

е взаимно еднозначно изображение на G върху $C(n)$. Ако $0 \leqq l < n$ и

$$k + l = nq + r, \quad 0 \leqq r < n,$$

то

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = \varphi(g^{nq+r}) = \varphi(g^r) =$$
$$= \varepsilon^r = \varepsilon^{nq+r} = \varepsilon^{k+l} = \varepsilon^k \cdot \varepsilon^l = \varphi(g^k)\,\varphi(g^l),$$

т. е. φ е изоморфизъм на групата G върху групата $C(n)$. Теоремата е доказана.

Благодарение на тази теорема можем да говорим просто за безкрайна циклична група и за крайна циклична група от даден ред n.

Теорема 2. *Всяка подгрупа H на една циклична група $G = \langle g \rangle$ е циклична. Ако H е неединична подгрупа и k е най-малкото естествено число, за което $g^k \in H$, то $H = \langle g^k \rangle$.*

Доказателство. Ако H е единичната подгрупа на G, то H е циклична. Нека $H \neq \langle 1 \rangle$. Подгрупата H на групата G съдържа и положителни степени на g, защото H съдържа заедно с елемента g^l и неговия обратен $(g^l)^{-1} = g^{-l}$. Нека k е най-малкото естествено число, за което $g^k \in H$. Ще покажем, че H е циклична група с образуващ елемент g^k. Наистина нека g^l е произволен елемент на H и $l = kq + r$, $0 \leqq r < k-1$. Тогава $g^l = (g^k)^q g^r$. Тъй като $g^r = (g^k)^{-q} g^l$ и g^l, $g^k \in H$, то $g^r \in H$. Ако допуснем, че $r \neq 0$, то $g^r \in H$ при $0 < r < k$, което противоречи на избора на k. Следователно $r = 0$ и $l = kq$, т. е. $g^l = (g^k)^q$ и $H = \langle g^k \rangle$. Теоремата е доказана.

Теорема 3. *Ако $G = \langle g \rangle$ е циклична група от ред n, то нейната подгрупа $H = \langle g^m \rangle$, породена от g^m, е от ред $\frac{n}{d}$, където d е най-големият общ делител на n и m.*

Доказателство. От следствие 1 е известно, че редът на H съвпада с реда на елемента g^m ($m \in Z$) и следователно трябва да докажем, че редът на g^m е $\frac{n}{d}$. Ако g^m е елемент от ред s, то s е най-малкото естествено число, за което $(g^m)^s = g^{ms} = 1$. Съ-

гласно следствие 2 това означава, че s е най-малкото естествено число, при което $\frac{sm}{n}$ е цяло число. Нека d е НОД на n и m, т. е.

$$n = dn_1,\ m = dm_1,\ (n_1,\ m_1) = 1.$$

Тогава

$$\frac{sm}{n} = \frac{s\,d\,m_1}{dn_1} = \frac{s\,m_1}{n_1} \in \mathbf{Z},$$

откъдето заключаваме, че $s = n_1 = \frac{n}{d}$.

Следствие 3. *Ако $G = \langle g \rangle$ е циклична група от ред n, то елементът g^m $(m \in \mathbf{Z})$ е също образуващ елемент на групата G тогава и само тогава, когато m и n са взаимно прости.*

Това твърдение ни напомня за теорема 3 от глава I за примитивните n-ти корени на единицата. То никак не е случайно, защото, както бе вече установено, групите $G = \langle g \rangle$ и $C(n)$ са изоморфни. Този изоморфизъм (или само следствие 3) показва, че всяка циклична група от ред n притежава точно $\varphi(n)$ различни пораждащи елемента. Те съответстват на примитивните n-ти корени на единицата.

§ 5. Разлагане на една група по нейна подгрупа

Нека H е подгрупа на групата G и x е елемент от G. Като имаме предвид определението за произведение на две подмножества в G, за произведението xH получаваме

$$xH = \{x\,h \mid h \in H\}.$$

Подмножеството xH наричаме *ляв съседен клас* на групата G по подгрупата H, породен от елемента x, а елемента x — представител на съседния клас xH. Произведението Hx наричаме *десен съседен клас* на групата G по подгрупата H, породен от елемента x.

Всеки елемент x на групата G принадлежи на някой съседен клас на подгрупата H, именно на съседния клас xH, тъй като $1 \in H$ и $x = x \cdot 1$.

Твърдение 5. *Всеки ляв съседен клас на групата G по подгрупата H се поражда от всеки свой елемент, т. е. ако $y \in xH$, то $xH = yH$. Нещо повече, равенството $xH = yH$ е изпълнено точно тогава, когато $x^{-1}y \in H$.*

Доказателство. Ако $y \in xH$, то $y = xh$ $(h \in H)$ и $x = yh^{-1}$. За да установим, че $xH = yH$, достатъчно е да проверим, че са в сила включванията $yH \subseteq xH$ и $xH \subseteq yH$. Произволен елемент g от yH има вида $g = yh_1$ $(h_1 \in H)$. Тогава

$$g = yh_1 = (xh)\,h_1 = x\,(hh_1) \in xH,$$

т. е. наистина $yH \subseteq xH$. От друга страна, ако $f \in xH$, то $f = xh_2$ $(h_2 \in H)$ и

$$f = xh_2 = (yh^{-1})\,h_2 = y\,(h^{-1}h_2) \in H.$$

Следователно изпълнено е и условието $xH \subseteq yH$.

Втората част на твърдението сега се получава съвсем лесно. Ако $x^{-1}y \in H$, то съгласно доказаното $x^{-1}yH = H$ и чрез умножаване отляво с x ще получим $yH = xH$. Обратно, от равенството $xH = yH$ следва, че $y \in xH$, поради което $y = xh$ $(h \in H)$ и затова $x^{-1}y = h \in H$. Твърдението е доказано.

Твърдение 6. *Два леви съседни класа на групата G по подгрупата H или съвпадат, или нямат общ елемент.*

Доказателство. Да допуснем, че съседните класове xH и yH имат общ елемент z. Тогава от предното твърдение се получава, че

$$xH = zH,\ yH = zH$$

и затова $xH = yH$.

От доказаните твърдения следва, че групата G се разпада на непресичащи се леви съседни класове по подгрупата H. Това разлагане се нарича *ляво разлагане* на групата G по подгрупата H. По аналогичен начин може да се разглежда *дясно разлагане* на G по H.

От очевидното равенство $1 \cdot H = H \cdot 1 = H$ следва, че самата подгрупа H е също ляв (десен) клас, а от твърдение 5 заключаваме, че всеки елемент h от H поражда съседния клас H, т. е. $hH = H = Hh$ $(h \in H)$.

Ако групата G е абелева, то умножението на всеки две подмножества в G е комутативно и специално $xH = Hx$. Следователно левите и десните съседни класове по H съвпадат, съвпадат също лявото и дясното разлагане на G по H, т. е. можем да говорим просто за разлагане на групата G по подгрупата H.

Примери

1. Числата, които са кратни на цялото положително число n, образуват циклична подгрупа $\langle n \rangle = n\mathbf{Z}$ на адитивната група $\mathbf{Z}$ на целите числа. Левите и десните класове на $\mathbf{Z}$ по $n\mathbf{Z}$ съвпадат, понеже $\mathbf{Z}$ е абелева група.

Всеки два от съседните класове

$$n\mathbf{Z} = 0 + n\mathbf{Z},\ 1 + n\mathbf{Z},\ 2 + n\mathbf{Z},\ \ldots,\ (n-1) + n\mathbf{Z}$$

са различни. Ще покажем, че това са всички съседни класове на $\mathbf{Z}$ по $n\mathbf{Z}$. Наистина нека $m + n\mathbf{Z}$ е произволен съседен клас на $\mathbf{Z}$ по $n\mathbf{Z}$ и $m = nq + r$ $(0 \leqq r < n)$. Тъй като $nq + n\mathbf{Z} = n\mathbf{Z}$, то $m + n\mathbf{Z} = r + nq + n\mathbf{Z} = r + n\mathbf{Z}$, т. е. съседният клас $m + n\mathbf{Z}$ е един от разглежданите класове.

2. В симетричната група S_3 подгрупата H, породена от цикъла (12), е циклична от ред 2. Ще намерим лявото и дясното разлагане на S_3 по H. Групата S_3 има 6 елемента, които чрез цикли могат да се запишат във вида e, (12), (13), (23), (123) и (132). Левите съседни класове на S_3 по H ще бъдат следните:

$$H = \{e, (12)\},\ (13)H = \{(13), (123)\},\ (23)H = \{(23), (123)\}.$$

От друга страна, десните класове на S_3 по H ще бъдат

$$H = \{e, (12)\},\ H(13) = \{(13), (132)\},\ H(23) = \{(23), (123)\}.$$

Очевидно лявото и дясното разлагане на S_3 по H не съвпадат.

Твърдение 7. *Ако G е произволна група, а H — нейна подгрупа, то всеки два съседни класа на G по H са равномощни.*

Доказателство. Ще построим взаимно еднозначно изображение φ на множеството H върху множеството xH по следния начин. Ако h е произволен елемент на H, нека

$$\varphi(h) = xh \in xH.$$

Очевидно φ е изображение на H в xH. Ако $h \neq h_1$ са два елемента от H, техните образи $\varphi(h)$ и $\varphi(h_1)$ са различни, тъй като равенството $xh = xh_1$ влече $h = h_1$. Ако g е произволен елемент от xH, то $g = xh$ за някое h от H. Тогава $\varphi(h) = g$, т. е. g има първообраз при φ. Следователно φ е взаимно еднозначно изображение на подгрупата H върху съседния клас xH. По аналогичен начин се построява взаимно еднозначно съответствие между H и Hy. Следователно $|xH| = |H| = |Hy|$.

Следствие 4. *Ако H е крайна подгрупа на групата G, то всеки два съседни класа на G по H имат равен брой елементи.*

Твърдение 8. *Ако H е подгрупа на групата G, то множеството от левите съседни класове на G по H е равномощно на множеството от десните съседни класове на G по H.*

Доказателство. Очевидно изображението φ, което на всеки ляв съседен клас xH съпоставя десния съседен клас Hx^{-1}, е изображение на множеството от левите съседни класове върху множеството от десните класове по H. Изображението φ е взаимно еднозначно. Наистина ако допуснем, че два леви класа gH и g_1H са различни, но техните образи чрез φ са равни, т. е.

$$Hg^{-1} = Hg_1^{-1},$$

то ще получим, че съществува елемент h от H, такъв, че

$$g^{-1} = hg_1^{-1}.$$

Следователно

$$g = g_1 h^{-1} \in g_1 H$$

и затова $gH = g_1H$ (виж твърдение 5), което е противоречие.

Следствие 5. *Броят на левите съседни класове на крайната група G по подгрупата H съвпада с броя на десните съседни класове по тази подгрупа.*

Определение 11. *Броят на левите съседни класове на крайната група G по нейната подгрупа H (или броят на десните съседни класове на G по H) се нарича индекс на подгрупата H в групата G и се означава с $|G:H|$.*

Теорема 4 (теорема на Лагранж). *Редът на всяка подгрупа H на една крайна група G дели реда на групата G. Точно в сила е равенството $|G| = |G:H| . |H|$.*

Доказателство. Нека G е крайна група от ред n, H е нейна подгрупа от ред k и индексът на H в G е j. По следст-

вие 4 всеки съседен клас се състои от k елемента, откъдето $n=kj$, т. е. редът k на подгрупата H дели реда n на групата G.

Следствие 6. *Редът на всеки елемент на една крайна група дели реда на самата група.*

Доказателство. Редът на елемента g от групата G е равен на реда на цикличната подгрупа $\langle g\rangle$, който според теоремата на Лагранж дели реда на G.

Следствие 7. *Всяка крайна група G, редът на която е просто число, е циклична и се поражда от всеки свой неединичен елемент.*

Доказателство. Нека групата G има ред p, където p е просто число. Ако g е произволен неединичен елемент на G, цикличната подгрупа $\langle g\rangle$ не е единична и по теоремата на Лагранж нейният ред трябва да дели простото число p. Следователно редът на $\langle g\rangle$ е p, т. е. цикличната подгрупа $\langle g\rangle$ съвпада с G.

Следствие 8. *За всяко просто число p съществува единствена, с точност до изоморфизъм група от ред p, а именно цикличната група от ред p.*

Доказателство. По следствие 7 всички групи от ред p са циклични. Следователно те са изоморфни помежду си като циклични групи с еднакви редове.

Задача. Нека H е подгрупа на G и $x, y\in G$. Ще казваме, че x и y са сравними по модул H и ще пишем $x\equiv y \pmod H$ тогава и само тогава, когато $x^{-1}y\in H$. Докажете, че релацията „$\equiv$“ е релация на еквивалентност, която разбива групата G на класове и те са точно левите съседни класове на G по H. Коя релация разбива G на десни съседни класове по H?

§ 6. Нормални делители

Определение 12. Подгрупата H на групата G се нарича *нормален делител* или *нормална подгрупа* на G, ако лявото разлагане на групата G по подгрупата H съвпада с дясното й разлагане.

С $H\triangleleft G$ ще означаваме, че подгрупата H е нормален делител на G.

Ако $H\triangleleft G$, то

$$xH=Hx \tag{1}$$

за всяко $x\in G$. Наистина ако $xH=Hy$, то $x\in xH=Hy$ и следователно класът Hy ще се породи и от x, т. е. $Hy=Hx$. Обратно, ако равенството (1) е изпълнено за всяко $x\in G$, то очевидно лявото разлагане на G по H съвпада с дясното й разлагане. Затова равенство (1) може да се вземе за определение на понятието нормален делител на G.

Лема 1. *Подгрупата H на групата G е нормален делител на G тогава и само тогава, когато за всяко $x\in G$ и за всяко $h\in H$ съществуват такива елементи h_1 и h_2 от H, че*

(2) $$xh = h_1 x,\ hx = xh_2.$$

Доказателство. Ако $H \lhd G$, то $xH = Hx$, откъдето следват равенствата (2). Обратно, нека са изпълнени равенствата (2). Тогава първото равенство на (2) е еквивалентно на включването $xH \subseteq Hx$, а второто — на включването $Hx \subseteq xH$ и затова $xH = Hx$.

Примери

1. Всяка подгрупа H на една абелева група G е неин нормален делител, защото лявото и дясното разлагане на G по H съвпадат.

Ако G е произволна група, двете разлагания на G по единичната ѝ подгрупа $\langle 1 \rangle$ съвпадат с разлагането на групата на отделни елементи, а двете разлагания на G по G съдържат само един клас, а именно самата група G, т. е. $\langle 1 \rangle \lhd G$ и $G \lhd G$.

2. $A_n \lhd S_n$. Наистина тъй като $|S_n : A_n| = 2$, то лявото и дясното разлагане на S_n по A_n са разлагане на S_n на четни и нечетни субституции.

Задача. Да се покаже, че всяка подгрупа на групата G, която има индекс 2 в G, е неин нормален делител.

Определение 13. *Нека a и b са елементи на групата G. Казваме, че елементът b е спрегнат на a в групата G, ако съществува такъв елемент g от G, че $b = g^{-1} a g$. Казваме още, че b се получава от a чрез трансформиране с елемента g.*

Ако елементът b е спрегнат на a, то и a е спрегнат с b, тъй като от горното равенство следва $a = (g^{-1})^{-1} b g^{-1}$, т. е.: елементът a се получава от b чрез трансформиране с елемента g^{-1}. По този начин елементите a и b можем да наречем просто спрегнати.

Релацията спрегнатост е релация на еквивалентност, т. е.:

1. Всеки елемент a е спрегнат със себе си (рефлексивност).

2. Ако a е спрегнат на b, то и b е спрегнат на a (симетричност).

3. Ако a е спрегнат на b и b е спрегнат на c, то a е спрегнат на c (транзитивност).

Например свойство 3 можем да докажем по следния начин: от $a = g_1^{-1} b g_1$, $b = g_2^{-1} c g_2$ следва $a = (g_2 g_1)^{-1} c (g_2 g_1)$.

Твърдение 9. *Ако A е подгрупа на групата G, то за всеки елемент g от G подмножеството $B = g^{-1} A g$ е подгрупа на G.*

Действително ако $g^{-1} a_1 g$ и $g^{-1} a_2 g$ са елементи от B, то

$$g^{-1} a_1 g (g^{-1} a_2 g)^{-1} = g^{-1} a_1 g g^{-1} a_2^{-1} g = g^{-1} (a_1 a_2^{-1}) g \in B$$

и твърдението следва от твърдение 2.

Определение 14. Ако A е подгрупа на групата G, то подгрупата $B = g^{-1} A g$ се нарича *спрегната* на A.

Както по-горе се проверява, че релацията спрегнатост на подгрупи е релация на еквивалентност. По този начин множеството от всички подгрупи на групата G се разлага на класове от спрегнати подгрупи. Самостоятелни класове образуват например, от-

една страна, едничната подгрупа, а, от друга страна — самата група G. Със следната теорема се показва, че свойството една подгрупа да образува самостоятелен клас от спрегнати подгрупи е характерно за нормалните делители на групата и само за тях.

Теорема 5. *Подгрупата H на групата G е нормален делител на G тогава и само тогава, когато всяка спрегната подгрупа на H съвпада с H.*

Доказателство. По дефиниция $H \lhd G$ тогава и само тогава, когато $xH = Hx$ за всяко $x \in G$. Последното равенство е еквивалентно на съвпадането на всяка спрегната подгрупа $x^{-1}Hx$ с H. Действително, като умножим $Hx = xH$ с x^{-1} отляво, получаваме $x^{-1}Hx = H$. Обратно, от последното равенство се получава $Hx = xH$ за всяко $x \in G$.

Теорема 6. *Подгрупата H на групата G е нормален делител на G тогава и само тогава, когато H съдържа заедно с всеки свой елемент и всички негови спрегнати елементи в G.*

Доказателство. Нека $H \lhd G$. Тогава $H = x^{-1}Hx$ за всяко $x \in G$. Ако h е елемент от H, то всеки негов спрегнат елемент $x^{-1}hx$ се съдържа в $x^{-1}Hx = H$, т. е. $x^{-1}hx \in H$ за всяко x.

Обратно, нека подгрупата H съдържа заедно с всеки свой елемент и спрегнатите му в G. Ако x е произволен елемент на G, то подгрупата $x^{-1}Hx$ се състои от елементи, спрегнати на елементи от H и поради това $x^{-1}Hx \subseteq H$. Аналогично $(x^{-1})^{-1}Hx^{-1} = xHx^{-1} \subseteq H$. Като използуваме тези две включвания, получаваме

$$H = x^{-1}(xHx^{-1})x \subseteq x^{-1}Hx \subseteq H,$$

т. е. $H = x^{-1}Hx$ за всяко x от G. По предишното твърдение H е нормален делител на G.

Пример. Специалната линейна група $SL(n, \mathbf{C})$ е нормален делител на общата линейна група $GL(n, \mathbf{C})$. Наистина нека $A \in SL(n, \mathbf{C})$ (т. е. A е такава матрица, че нейната детерминанта $|A| = 1$) и X е произволна матрица от $GL(n, \mathbf{C})$. Тогава $X^{-1}AX \in SL(n, \mathbf{C})$, защото $|X^{-1}AX| = |X|^{-1} \cdot |A| \cdot |X| = 1$.

Твърдение 10. *Сечението на краен или безкраен брой нормални делители на групата G е нормален делител на G.*

Доказателство. Ако A и B са нормални делители на групата G, то $A \cap B$ е подгрупа на G (твърдение 3). Ако x е произволен елемент на G, а h — произволен елемент на $A \cap B$, то $x^{-1}hx$ се съдържа и в A, и в B, тъй като A и B са нормални делители, на които принадлежи h, т. е. $x^{-1}hx \in A \cap B$. По теорема 6 $A \cap B$ е нормален делител на G.

Доказателството в общия случай не се различава принципно от горното.

Задача. Да се докаже, че ако A и B са подгрупи на групата G и поне една от тях е нормален делител на G, то AB е подгрупа на групата G. Ако $A \lhd G$ и $B \lhd G$, то $AB \lhd G$.

Упътване. Докажете, че $AB = BA$. Използувайте твърдение 4 и теорема 6.

§ 7. Фактор-групи

Нека H е подгрупа на групата G. Ще покажем, че $H.H=H$. Наистина произволен елемент от множеството HH е от вида h_1h_2 и тъй като множеството H е затворено спрямо умножението, то $h_1h_2 \in H$, т. е. $H.H \subseteq H$. Но $H=1.H \subseteq H.H$ и поради това $H.H=H$.

Нека H е нормален делител на групата G. Тогава за всеки елемент y от G е изпълнено равенството $yH=Hy$. Ще покажем, че множеството от съседните класове на G по H образува група спрямо умножението на подмножества на G. За тази цел ще проверим, че са изпълнени условията на твърдение 1.

1) Произведението на два съседни класа на групата G по нормалния делител H е съседен клас на G по H. Наистина

$$xHyH=x(Hy)H=x(yH)H=xy(HH)=xyH,$$

където са използувани асоциативният закон за умножение на подмножества на групата G и равенствата $HH=H$, $yH=Hy$. По този начин имамс

$$xHyH=xyH.$$

Едновременно получаваме и следното правило: *произведението на два съседни класа по нормален делител е съседен клас, породен от произведението на произволни представители на тези класове.*

2) В сила е асоциативният закон за умножение на съседни класове на G по H, тъй като умножението на подмножества на G е асоциативно.

3) Единичен елемент при умножението на съседни класове на G по H е самият нормален делител H. Наистина

$$xH.H=xH,\ H.xH=xH.H=xH.$$

4) Всеки съседен клас xH притежава обратен клас, а именно $x^{-1}H$. Наистина

$$xHx^{-1}H=xx^{-1}H=H,\ x^{-1}HxH=x^{-1}xH=H.$$

От твърдение 1 следва, че множеството от всички съседни класове на групата G по нормалния делител H е група, която ще наричаме *фактор-група* на G по H и ще я означаваме с G/H. Изрично ще посочим, че xH е подмножество на групата G, но за фактор-групата G/H той е просто един неин елемент. Фактор-групата G/G съдържа един-единствен елемент G и затова G/G е единичната група, т. е. $G/G \cong \langle 1 \rangle$. Тъй като разлагането на G по нейната единична подгрупа $\langle 1 \rangle$ е разлагане на G на отделни елементи, то $G/\langle 1 \rangle \cong G$.

Теорема 7. *Всяка фактор-група на абелева група е абелева.*

Доказателство. Нека G е произволна абелева група и H е нейна подгрупа, т. е. неин нормален делител. Нека xH и yH са произволни елементи на фактор-групата G/H. Тогава

$$xHyH=xyH=yxH=yHxH,$$

където второто равенство следва от комутативния закон в G.

Теорема 8. *Всяка фактор-група на циклична група е циклична.*

Доказателство. Нека H е подгрупа на циклична група $G=\langle g\rangle$. Можем да разглеждаме фактор-групата G/H, тъй като G е абелева група и всяка нейна подгрупа е неин нормален делител. Ако xH е произволен елемент на фактор-групата G/H, $x\in G$, то $x=g^k$, тъй като всеки елемент на G е степен на g. Следователно

$$xH=g^kH=(gH)^k.$$

Получихме, че елементите на фактор-групата G/H са степени на елемента gH, т. е. $\langle g\rangle/H=\langle gH\rangle$.

Твърдение 11. *Ако G е крайна група, то редът на всяка нейна фактор-група G/H е делител на реда на групата G.*

Действително от теоремата на Лагранж знаем, че $|G|=|G:H|.|H|$, където $|G:H|$ е индексът на H в G. Но редът $|G/H|$ е равен на индекса $|G:H|$ и затова $|G/H|$ дели реда $|G|$ на групата G.

Примери

1. Ако Z е адитивната група на целите числа, а nZ — цикличната подгрупа, породена от естественото число n, то факторгрупата Z/nZ е циклична с образуващ елемент $1+nZ$.

2. Фактор-групата S_n/A_n се състои от два елемента, т. е. нейният ред е простото число 2. Следователно S_n/A_n е циклична група (следствие 7).

§ 8. Хомоморфизми. Теорема за хомоморфизмите

Определение 15. Нека G и H са две мултипликативно записани групи. Изображението φ на G в H се нарича *хомоморфизъм* на групата G в групата H, ако $\varphi(ab)=\varphi(a)\varphi(b)$ за всеки два елемента a и b от G. Ако хомоморфизмът φ на G в H изобразява G върху H, т. е. всеки елемент от H има първообраз при φ от G, тогава ще говорим за хомоморфизъм на G върху H, а H ще наричаме *хомоморфен образ* на G.

Очевидно ако хомоморфизмът φ на G върху H е взаимно едновначно изображение, то φ е изоморфизъм, а групата H е изоморфен образ (изоморфна) на G.

Твърдение 12. *Ако φ е хомоморфизъм на групата G в групата H, 1 и e са съответно единиците на G и H и a е произволен елемент на G, то*

$$\varphi(1)=e,\ \varphi(a^{-1})=[\varphi(a)]^{-1}.$$

Доказателство. Нека $\varphi(1)=x$, $x\in H$. Ще покажем, че $x=e$. Наистина $x=\varphi(1)=\varphi(1.1)=\varphi(1)\varphi(1)=xx$ и затова $x=e$. Освен това

$$e=\varphi(1)=\varphi(aa^{-1})=\varphi(a)\,\varphi(a^{-1}),$$

т. е. $[\varphi(a)]^{-1}=\varphi(a^{-1})$.

От доказаното твърдение следва, че множеството от тези елементи на групата G, които при хомоморфизма φ на G в групата H се изобразяват в единицата, не е празно (например единицата на G е такъв елемент).

Определение 16. Подмножеството от всички елементи на групата G, които при хомоморфизма φ на групата G в групата H се изобразяват в единицата на H, се нарича *ядро* на φ и се означава с $\ker\varphi$, т. е.

$$\ker\varphi=\{a\mid\varphi(a)=1,\ a\in G\}.$$

Твърдение 13. *Ядрото на всеки хомоморфизъм φ на групата G в групата H е нормален делител на групата G.*

Доказателство. Ако $a,\ b\in A=\ker\varphi$, то $\varphi(ab^{-1})=\varphi(a)\,\varphi(b^{-1})=\varphi(a)\,[\varphi(b)]^{-1}=1\,.\,1=1$, т. е. $ab^{-1}\in A$ и от твърдение 2 следва, че A е подгрупа на G.

Подгрупата A е нормален делител на групата G. Наистина ако $g\in G$ и $a\in A$, то

$$\varphi(g^{-1}ag)=\varphi(g^{-1})\,\varphi(a)\,\varphi(g)=[\varphi(g)]^{-1}[\varphi(g)]=1,$$

откъдето $g^{-1}ag\in A$, т. е. подгрупата A заедно с всеки свой елемент a съдържа и всички спрегнати с него елементи в G.

Твърдение 14. *Всеки нормален делител A на групата G е ядро на някакъв хомоморфизъм на групата G.*

Доказателство. Да дефинираме изображението $\eta: G\to G/A$ с равенството $\eta(g)=gA$, където g е произволен елемент от G. Очевидно η е изображение на групата G върху фактор-групата G/A. Изображението η е хомоморфизъм на групата G върху фактор-групата G/A, тъй като за всеки два елемента g и g_1 от G имаме

$$\eta(gg_1)=gg_1A=gA\,.\,g_1A=\eta(g)\,\eta(g_1).$$

Ще покажем, че ядрото на η е A. Наистина ако $g\in G$, то $g\in\ker\eta$ точно тогава, когато $\eta(g)=gA=A$ (A е единицата в G/A), т. е. $g\in\ker\eta$ точно тогава, когато $g\in A$.

По този начин имаме $A=\ker\eta$.

Определение 17. Изображението η на групата G върху фактор-групата G/A, което съпоставя на всеки елемент g от G съседния клас gA на G по A, се нарича *естествен хомоморфизъм* на групата G върху групата G/A.

Ако φ е хомоморфизъм на групата G в групата H, то с $\operatorname{Im}\varphi=\varphi(G)$ ще означаваме подмножеството на H, съставено от всички елементи $\varphi(g)$, $g\in G$, и ще го наричаме *образ на G* при хомоморфизма φ.

Ясно е, че $\operatorname{Im}\varphi=H$ точно тогава, когато φ е хомоморфизъм на G върху H.

Твърдение 15. *Нека φ е хомоморфизъм на групата G в*

групата H. Тогава образът $\operatorname{Im}\varphi$ *на G в H е подгрупа на H.*

Наистина по твърдение 12 имаме $\varphi(a)[\varphi(b)]^{-1}=\varphi(a)\varphi(b^{-1})=\varphi(ab^{-1})\in\operatorname{Im}\varphi$ за всеки два елемента $a, b\in G$, откъдето съгласно твърдение 2 $\operatorname{Im}\varphi$ ще бъде подгрупа на G.

Твърдение 13 и твърдение 14 показват, че ядрата на хомоморфизмите на групата G се изчерпват с нормалните делители на G.

Следната теорема показва, че крайните групи с точност до изоморфизъм се изчерпват с подгрупите на симетричните групи.

Теорема 9 (теорема на Кели). *Всяка група от ред n е изоморфна на някоя подгрупа на симетричната група* S_n *от n-та степен.*

Доказателство. Нека $a_1, a_2, \ldots, a_n$ са елементите на групата G, взети в определен ред, a е произволен елемент на G и

$$aa_i=a_{\alpha_i}\ (i=1, 2, \ldots, n).$$

Ако $i\neq j$, то $\alpha_i\neq\alpha_j$. В противен случай се получава $a_{\alpha_i}=a_{\alpha_j}$, т. е. $aa_i=aa_j$, което води до противоречието $a_i=a_j$. Определяме изображение $\varphi: G\to S_n$, като за всяко a от G полагаме

$$\varphi(a)=\begin{pmatrix}1 & 2 & \ldots & n\\ \alpha_1 & \alpha_2 & \ldots & \alpha_n\end{pmatrix}.$$

Ако $b\in G$ и $b\neq a$, то $\varphi(a)\neq\varphi(b)$, тъй като $aa_i\neq ba_i$ за всяко $i=1, 2, \ldots, n$. Затова φ изобразява различни елементи от G в различни елементи на S_n.

Нека $a, b\in G$ и

$$\varphi(b)=\begin{pmatrix}1 & 2 & \ldots & n\\ \beta_1 & \beta_2 & \ldots & \beta_n\end{pmatrix}.$$

Ако $aa_{\beta_i}=a_{\gamma_i}$, то

$$\varphi(a)=\begin{pmatrix}\beta_1 & \beta_2 & \ldots & \beta_n\\ \gamma_1 & \gamma_2 & \ldots & \gamma_n\end{pmatrix}.$$

Затова

$$\varphi(a)\varphi(b)=\begin{pmatrix}1 & 2 & \ldots & n\\ \gamma_1 & \gamma_2 & \ldots & \gamma_n\end{pmatrix}.$$

Понеже $(ab)a_i=a(ba_i)=aa_{\beta_i}=a_{\gamma_i}$, то $\varphi(ab)=\varphi(a)\varphi(b)$, т. е. φ е хомоморфизъм на G в S_n, който изобразява различни елементи от G в различни елементи от S_n. Затова φ е изоморфизъм на G върху $\varphi(G)$, което съгласно твърдение 15 е подгрупа на S_n. Теоремата е доказана.

Тъй като подгрупите на групите S_n са краен брой, от горната теорема следва, че за всяко естествено число n съществуват само краен брой неизоморфни групи от ред n.

С всяка група G свързахме две серии от групи: нейните фактор-групи и нейните хомоморфни образи. В доказателството на твърдение 14 видяхме, че всяка фактор-група на G е неин хомо-

морфен образ. Обратно, оказва се, че хомоморфните образи на една група с точност до изоморфизъм се изчерпват с нейните фактор-групи.

Теорема 10. *Ако φ е хомоморфизъм на групата G върху групата H и A е ядрото на този хомоморфизъм, то факторгрупата G/A е изоморфна на групата H. Нещо повече, съществува такъв изоморфизъм σ на фактор-групата G/A върху групата H, че произведението $\sigma\eta$ на σ с естествения хомоморфизъм η на G върху G/A съвпада с хомоморфизма φ.*

Доказателство. Ако $g_1, g_2 \in G$, то равенството $\varphi(g_1) = \varphi(g_2)$ е изпълнено точно тогава, когато $\varphi(g_2^{-1}g_1) = 1$, което е еквивалентно с условието $g_2^{-1}g_1 \in A$, т. е. $\varphi(g_1) = \varphi(g_2)$ е изпълнено точно тогава, когато $g_1A = g_2A$. Затова равенството $\sigma(gA) = \varphi(g)$ $(g \in G)$ дефинира коректно изображение σ на фактор-групата G/A в групата H, което изобразява различни елементи от G/A в различни елементи от H. Тъй като са изпълнени равенствата

$$\sigma(g_1A \cdot g_2A) = \sigma(g_1g_2A) = \varphi(g_1g_2) =$$

$$= \varphi(g_1)\varphi(g_2) = \sigma(g_1A) \cdot \sigma(g_2A),$$

то σ е хомоморфизъм на G/A в H. Ако b е произволен елемент от H, то $b = \varphi(g)$ за някое $g \in G$. Тогава $b = \varphi(g) = \sigma(gA)$. Следователно σ е изоморфизъм на G/A върху H.

Равенството $\varphi = \sigma\eta$ следва от факта че

$$\sigma\eta(g) = \sigma[\eta(g)] = \sigma(gA) = \varphi(g)$$

за всяко $g \in G$. Теоремата е доказана.

Следствие 9. *Ако φ е хомоморфизъм на групата G в групата H и $\operatorname{Im}\varphi$ е образът на G при φ, то $G/\ker\varphi \cong \operatorname{Im}\varphi$.*

Задача. Нека N е нормален делител в групата G, а H е подгрупа на G. Докажете, че фактор-групите $H/(H \cap N)$ и HN/N са изоморфни.

Примери

1. Изображението $\varphi: GL(n, \mathbf{C}) \to \mathbf{C}^*$, което на всяка матрица X от $GL(n, \mathbf{C})$ съпоставя нейната детерминанта $|X|$, т. е. $\varphi(X) = |X|$, е хомоморфизъм на първата група върху втората.

Наистина всяка матрица X от $GL(n, \mathbf{C})$ е неособена и следователно $|X| \neq 0$, т. е. $|X| \in \mathbf{C}^*$. За всяко число α от $\mathbf{C}^*$ може да се построи матрица (например $\sqrt[n]{\alpha}\,E$) от $GL(n, \mathbf{C})$, която има детерминанта, равна на α. Поради това φ е изображение на $GL(n, \mathbf{C})$ върху $\mathbf{C}^*$ и даже хомоморфизъм на едната група върху другата, тъй като за X и Y от $GL(n, \mathbf{C})$ е в сила равенството $\varphi(XY) = |XY| = |X| \cdot |Y| = \varphi(X)\varphi(Y)$. Ще покажем, че $\ker\varphi = SL(n, \mathbf{C})$. Наистина за $X \in GL(n, \mathbf{C})$ е в сила условието $X \in \ker\varphi$ тогава и само тогава, когато $\varphi(X) = |X| = 1$, т. е. точно тогава, когато $X \in SL(n, \mathbf{C})$. Следователно $\ker\varphi = SL(n, \mathbf{C})$ и от теоремата за хомоморфизмите следва, че

$$GL(n, \mathbf{C})/SL(n, \mathbf{C}) \cong \mathbf{C}^*.$$

Тук $GL(n, \mathbf{C})$ при $n>1$ е некомутативна група, а нейният хомоморфен образ $\mathbf{C}^*$ е абелева група. Това показва, че свойството некомутативност при хомоморфните изображения невинаги се запазва.

2. Изображението $\varphi: \mathbf{C}^* \to U$, което на всяко комплексно число $z \neq 0$ съпоставя числото $\frac{z}{|z|}$ от U, т. е.

$$\varphi(z) = \frac{z}{|z|},$$

е хомоморфизъм на групата $\mathbf{C}^*$ върху U.

Наистина ако z_1 е също комплексно число от $\mathbf{C}^*$, то

$$\varphi(zz_1) = \frac{zz_1}{|zz_1|} = \frac{z}{|z|} \cdot \frac{z_1}{|z_1|} = \varphi(z)\varphi(z_1).$$

Ще покажем, че $\ker \varphi = \mathbf{R}^+$, където $\mathbf{R}^+$ е мултипликативната група на положителните реални числа. Действително за $z \in \mathbf{C}^*$ е изпълнено условието $z \in \ker \varphi$ тогава и само тогава, когато $\varphi(z) = \frac{z}{|z|} = 1$, т. е $z = |z| \in \mathbf{R}^+$ и затова $\ker \varphi = \mathbf{R}^+$. От теоремата за хомоморфизмите следва, че

$$\mathbf{C}^*/\mathbf{R}^+ \cong U.$$

3. Изображението $\varphi: U \to U$, за което

$$\varphi(z) = z^n$$

(n е естествено число), е изображение на U върху U. Действително ако $\alpha \in U$ и β е едно от решенията на уравнението $x^n = \alpha$, то β също принадлежи на U и затова $\varphi(\beta) = \alpha$. Изображението φ е хомоморфизъм, тъй като

$$\varphi(zz_1) = (zz_1)^n = z^n z_1^n = \varphi(z)\varphi(z_1).$$

Освен това $\ker \varphi = C(n)$, понеже $z \in \ker \varphi$ тогава и само тогава когато $\varphi(z) = z^n = 1$, т. е. точно тогава, когато $z \in C(n)$. Следователно $U/C(n) \cong U$.

§ 9. Действие на група в множество

Нека G е мултипликативно записана група, а M — произволно множество.

Определение 18. Ще казваме, че групата G *действува* в множеството M, ако за всеки елемент g от G и всеки елемент m от M по някакво правило се съпоставя еднозначно определен елемент от M, който ще наричаме произведение на g по m и ще го означаваме с gm (в някои случаи $g \circ m$ или $g * m$), като при това са изпълнени следните аксиоми:

1) $(g_1 g_2)m = g_1(g_2 m)$ за всеки два елемента g_1, g_2 от G и за всяко m от M;

2) $em = m$, където e е единицата на G, а m е произволен елемент от M.

Примери

1. Нека M е реално линейно пространство, а $G = \mathbf{R}^*$ е мултиплпкативната група на полето на реалните числа. Всеки вектор от M можем да умножаваме с реални числа. Освен това $(r_1 r_2)v = r_1(r_2 v)$ и $1 \cdot v = v$ за всеки вектор v от M и за всеки две реални числа r_1 и r_2. Следователно групата $G = \mathbf{R}^*$ действува по естествен начин в M.

2. Общата линейна група $G = GL(M)$ от неособените линейни преобразувания на линейното пространство M също действува по естествен начин в M: ако $\varphi \in G$ и $m \in M$, под $\varphi \circ m$ разбираме образа $\varphi(m)$ на m чрез φ. Тогава $(\varphi_1\varphi_2) \circ m = \varphi_1[\varphi_2(m)] = \varphi_1(\varphi_2 \circ m) = \varphi_1 \circ (\varphi_2 \circ m)$ и $\varepsilon \circ m = \varepsilon(m) = m$, където $\varphi_1, \varphi_2 \in G$ и ε е тъждественото (единичното) линейно преобразуване на M.

3. Ако M е реално евклидово пространство, а $G = O(M)$ е групата на ортогоналните линейни преобразувания на M, то G действува в M: $\varphi \circ m = \varphi(m)$ за всяко $\varphi \in G$ и всяко $m \in M$. При това действие, както знаем, ортонормиран базис преминава в ортонормиран базис.

4. Нека G е мултипликативно записана група, H е произволна подгрупа на G, а $M_k(G)$ е съвкупността от всички подмножества на G, които съдържат точно по k различни елемента. Ако $m \in M_k(G)$, то $m = \{g_1, g_2, \ldots, g_k\}$, където $g_i \in G$ и $g_i \neq g_j$ при $i \neq j$. Под произведение hm на елемента h от групата H с елемента m ще разбираме подмножеството $\{hg_1, hg_2, \ldots, hg_k\}$ на групата G. Очевидно hm се състои от k различни елемента на G и затова $hm \in M_k(G)$. Лесно се проверява, че така получаваме действие на групата H в множеството $M_k(G)$.

5. Друго действие на групата H от предния пример в множеството $M_k(G)$ се получава, като положим

$$h \circ m = \{hg_1h^{-1}, hg_2h^{-1}, \ldots, hg_kh^{-1}\}$$

за всяко $h \in H$ и $m = \{g_1, g_2, \ldots, g_k\} \in M_k(G)$.

Особено интересни са последните два примера при $k = 1$. Тогава $M_1(G)$ е множеството от едноелементните подмножества на G, т. е. можем да считаме, че $M_1(G) = G$. Подгрупата H на G в този случай действува в множеството G по два начина: 1) умножаване отляво елементите на G с елементи от H, т. е. на $h \in H$ и $g \in G$ се съпоставя елементът hg; 2) спрягане на елементите от G с елементи от H — в този случай на $h \in H$ и $g \in G$ се съпоставя елементът $h \circ g = hgh^{-1} = (h^{-1})^{-1}gh^{-1}$.

Определение 19. Нека групата G действува в множеството M. Ако m е елемент от M, множеството $S_G(m)$ на всички елементи g от G, за които е изпълнено равенството $gm = m$, се нарича *стабилизатор* (или в някои конкретни случаи — *централизатор*) на m в G, т. е.

$$S_G(m) = \{g \mid g \in G,\ gm = m\}.$$

Твърдение 16. *Ако групата G действува в множеството M, то стабилизаторът на всеки елемент от M е подгрупа в G.*

Доказателство. Стабилизаторът $S_G(m)$ е непразно подмножество на G, тъй като $e \in S_G(m)$. Освен това ако $g_1, g_2 \in S_G(m)$, то $g_1 m = m$, $g_2 m = m$ и $(g_1 g_2^{-1})\, m = (g_1 g_2^{-1})\,(g_2 m) = g_1 (g_2^{-1} (g_2 m)) = g_1 (g_2^{-1} g_2)\, m = g_1 m = m$, т. е. $g_1 g_2^{-1} \in S_G(m)$. Следователно съгласно твърдение 2 $S_G(m)$ е подгрупа на G.

Определение 20. Ако групата G действува в множеството M и m е елемент на M, то множеството от всички елементи на M от вида gm $(g \in G)$ се нарича *орбита*, определена от m, и се бележи с $O(m)$ или с Gm.

Твърдение 17. *Ако групата G действува в множеството M, то всеки елемент m от M се съдържа в орбитата $O(m)$. Две орбити $O(m_1)$ и $O(m_2)$ или не се пресичат, или съвпадат.*

Доказателство. Тъй като $em = m$, то $m \in O(m)$. Да допуснем, че $m \in O(m_1) \cap O(m_2)$. Тогава $m = g_1 m_1$, $m = g_2 m_2$ за някои елементи g_1 и g_2 на G. От равенството $g_1 m_1 = g_2 m_2$ с умножение на g_1^{-1} и g_2^{-1} получаваме равенствата

$$m_1 = e m_1 = g_1^{-1} (g_1 m_1) = g_1^{-1} (g_2 m_2) = (g_1^{-1} g_2)\, m_2,$$

$$m_2 = e m_2 = g_2^{-1} (g_2 m_2) = g_2^{-1} (g_1 m_1) = (g_2^{-1} g_1)\, m_1.$$

Нека $x \in O(m_1)$, т. е. $x = g m_1$, $g \in G$. Тогава $x = g m_1 = g[(g_1^{-1} g_2)\, m_2] = (g g_1^{-1} g_2)\, m_2 \in O(m_2)$. Следователно $O(m_1) \subseteq O(m_2)$. Ако $y \in O(m_2)$, то $y = h m_2$ $(h \in G)$ и $y = h m_2 = h[(g_2^{-1} g_1)\, m_1] = (h g_2^{-1} g_1)\, m_1 \in O(m_1)$. Следователно $O(m_2) \subseteq O(m_1)$. От получените две включвания следва, че орбитите $O(m_1)$ и $O(m_2)$ съвпадат което се дължи на допускането, че тези орбити съдържат общ елемент. Твърдението е доказано.

Твърдение 18. *Нека групата G действува в множеството M и $S = S_G(m)$ е стабилизаторът на елемента m от M в групата G. Тогава между елементите на орбитата $O(m)$, определена от m, и левите съседни класове на G по подгрупата S съществува взаимно еднозначно съответствие.*

Доказателство. Нека G/S е множеството от левите съседни класове на групата G по стабилизатора S на елемента m. Да допуснем, че g_1 и g_2 от G са в един и същ съседен клас, т. е. $g_1 S = g_2 S$. Тогава $g_1 = g_2 s$, $s \in S$. Тъй като $sm = m$, то $g_1 m = (g_2 s)\, m = g_2 (sm) = g_2 m$ и следователно g_1 и g_2 действуват на m по един и същ начин. Този факт ни дава възможност да дефинираме изображение φ на множеството G/S в множеството $O(m)$, като положим

$$\varphi(gS) = gm.$$

Ще докажем, че φ е взаимно еднозначно изображение.

Нека gS и hS са два елемента от G/S. Да допуснем, че $\varphi(gS) = \varphi(hS)$, т. е. $gm = hm$. От последното равенство с умноже-

ние на h^{-1} получаваме $(h^{-1}g)m=m$. Затова $h^{-1}g \in S=S_G(m)$ и тогава, както знаем, ще имаме $gS=hS$. По този начин проверихме, че φ изобразява различни елементи от G/S в различни елементи на $O(m)$.

Нека $m_1 \in O(m)$. Тогава $m_1=gm$ за някой елемент g от G. Затова $m_1=\varphi(gS)$ и следователно φ е взаимно еднозначно изображение на G/S върху множеството $O(m)$. Твърдението е доказано.

Следствие 10. *Ако групата G действува в крайното множество M, то броят на елементите на орбитата $O(m)$ на елемента m от M е равен на индекса на стабилизатора $S_G(m)$ на m в групата G.*

Следствие 11. *Ако крайната група G действува в множеството M, то всяка орбита има краен брой елементи и този брой е делител на реда $|G|$ на групата G. По-точно ако m е елемент от M, то произведението на броя на елементите от орбитата $O(m)$ и реда $|S_G(m)|$ на стабилизатора на m в G е равно на реда $|G|$ на групата G.*

Действително редът на групата G е равен на произведението $j|S_G(m)|$ на индекса j на подгрупата $S_G(m)$ в G по нейния ред $|S_G(m)|$. Но по следствие 10 $j=|O(m)|$ и затова

$$|G|=|O(m)| \cdot |S_G(m)|.$$

В § 6 видяхме, че релацията спрегнатост на елементи в една група G е релация на еквивалентност и затова групата G се разбива на непресичащи се класове от спрегнати елементи. Ако G е крайна група, тя ще се разбие на краен брой различни класове $C_1, C_2, \ldots, C_s$ от спрегнати елементи. Ако c_i е броят на елементите на класа C_i $(i=1, 2, \ldots, s)$, в сила е равенството

$$|G|=c_1+c_2+\ldots+c_s. \tag{1}$$

Поне едно от числата c_i е равно на 1, тъй като единицата на групата G образува едноелементен клас от спрегнати елементи. Възможно е и други неединични елементи на групата G да образуват едноелементни класове от спрегнати елементи. Например ако групата G е абелева, то всеки неин елемент е спрегнат само на себе си и затова в G ще имаме $|G|$ на брой едноелементни класа от спрегнати елементи, т. е. абелевата група G относно релацията спрегнатост се разбива на своите едноелементни подмножества.

Нека елементът g на групата G образува едноелементен клас от спрегнати елементи, т. е. g е спрегнат само на себе си. Тогава $h^{-1}gh=g$ и следователно $gh=hg$ за всяко $h \in G$.

Тъй като последните две равенства са еквивалентни, то g е спрегнат само със себе си тогава и само тогава, когато g комутира с всички елементи на групата G.

Определение 21. *Център $C(G)$* на групата G се нарича подмножеството от тези елементи на G, които комутират с всички елементи на G, т. е.

$$C(G)=\{g \mid g \in G,\ xg=gx \text{ за всяко } x \in G\}.$$

Задача. Докажете, че центърът на всяка група е неин нормален делител.

Ясно е, че G е абелева група тогава и само тогава, когато $G=C(G)$.

Ще казваме, че групата G има тривиален център, ако $C(G)$ е единичната подгрупа на G.

Задача. Докажете, че симетричната група S_n при $n \geqq 3$ има тривиален център.

Задача. Докажете, че центърът на общата линейна група $GL(n, P)$ от неособените матрици с елементи от числовото поле P се състои от скаларните матрици αE, където $\alpha \in P$ и $\alpha \neq 0$.

Тъй като един елемент g на групата G образува едноелементен клас от спрегнати елементи точно тогава, когато $g \in C(G)$, то в дясната страна на равенството (1) за крайната група G ще имаме толкова събираеми c_i, равни на 1, колкото е редът $|C(G)|$ на $C(G)$. Затова ако $C_1, C_2, \ldots, C_k$ са класовете спрегнати елементи на G, които съдържат повече от един елемент, т. е. $c_i \geqq 2$ за $i=1, 2, \ldots, k$, то $G=C_1 \cup C_2 \cup \ldots \cup C_k \cup C(G)$, където в обединението участвуват непресичащи се подмножества на G. Сега равенството (1) добива вида

$$|G|=|C(G)|+c_1+c_2+\ldots+c_k, \tag{2}$$

където $c_1, c_2, \ldots, c_k$ са редовете на различните класове спрегнати елементи в G, които имат поне два елемента. Допълнителна информация за числата c_i ни дава следното

Твърдение 19. *Ако C е клас от спрегнати елементи в крайната група G, то броят c на елементите в C дели реда $|G|$ на групата G.*

Доказателство. Групата G действува в множеството G от своите елементи чрез спрягане, т. е. $h \circ g=hgh^{-1}$ за $h, g \in G$ (в пример 5 е взето $H=G$ и $k=1$, т. е. $M_1(G)=G$). Орбитите относно това действие са точно класовете спрегнати елементи в G. В частност C е орбита спрямо това действие. По следствие 11 броят c на елементите на C дели реда на групата G. Твърдението е доказано.

Определение 22. Ако редът на неединичната крайна група G е равен на някоя степен на простото число p, ще казваме, че G е *p-група*.

Теорема 11. *Центърът на всяка* крайна *p-група е нетривиален.*

Доказателство. Нека $|G|=p^n$, $n \geqq 1$. Ако C е клас от спрегнати елементи в G, който съдържа $c \geqq 2$ елемента, по предишното твърдение c е неединичен делител на p^n. Тъй като p е просто число, то $c=p^t$, $1 \leqq t < n$. Затова в този случай формула (2) добива вида

$$p^n=|C(G)|+p^{t_1}+p^{t_2}+\ldots+p^{t_k},$$

където $t_i \geqq 1$ $(i = 1, 2, \ldots, k)$. От това равенство следва, че простото число p дели реда $|C(G)|$ на центъра на G. Затова $|C(G)| \geqq p \geqq 2$, т. е. центърът на p-групата G е неединична подгрупа в G. Теоремата е доказана.

§ 10. Теореми на Силов

В този параграф ще докажем три теореми за строежа на крайните групи. Поради своята важност и приложимост тези теореми лежат в основите на теорията на крайните групи. Те са доказани от норвежкия математик Л. Силов в 1872 г. и сега носят неговото име.

Нека G е крайна група и $n = |G|$ е нейният ред. Подгрупата H на G се нарича p-подгрупа на G (p — просто число), ако H е p-група. Ако G има p-подгрупа H, то редът $|H|$ на H е равен на някоя степен на p с положителен показател и по теоремата на Лагранж той дели реда n на G. Следователно, за да има групата G p-подгрупа, необходимо е нейният ред да се дели на простото число p. А вярно ли е обратното твърдение?

Ще казваме, че подгрупата H на G е *силовска p-подгрупа* на G (или че H е *максимална p-подгрупа* на G), ако H е p-подгрупа на G и H не се съдържа в друга p-подгрупа на G, т. е. всяка p-подгрупа на G, която съдържа H, съвпада с H.

Ако групата G има поне една p-подгрупа, то G има и силовски p-подгрупи — такива ще бъдат p-подгрупите на G от максимален ред, избрани измежду p-подгрупите на G. Но ако H_1 и H_2 са две силовски p-подгрупи на G за едно и също просто число p, могат ли H_1 и H_2 да имат различни редове? На поставените и на редица други естествено възникващи въпроси, които се отнасят до p-подгрупите на дадена крайна група, ще получим отговор от теоремите на Силов.

Лема 2. *Нека G е множество от n елемента и $n = p^r l$ $(r \geqq 1)$, където p е просто число и l е взаимно просто с p. Ако $M = M_{p^t}(G)$ е множеството от всички различни подмножества на G, които имат точно по p^t елемента $(t \leqq r)$, то най-високата степен на p, която дели броя $|M|$ на елементите на M, е p^{r-t}.*

Доказателство. Числото $|M|$ е равно на

$$\binom{n}{p^t} = \binom{p^r l}{p^t} = \frac{p^r l (p^r l - 1) \ldots (p^r l - p^t + 1)}{p^t!} = p^{r-t} l \binom{p^r l - 1}{p^t - 1}.$$

Тъй като $(l, p) = 1$, за да докажем лемата, трябва да покажем, че цялото число $\binom{p^r l - 1}{p^t - 1}$ не се дели на p. Това число се записва по следния начин:

$$\binom{p^r l - 1}{p^t - 1} = \frac{(p^r l - 1)(p^r l - 2) \ldots (p^r l - p^t + 1)}{(p^t - 1)!} = \prod_{j=1}^{p^t - 1} \frac{p^r l - j}{j}.$$

Тъй като $1 \leqq j \leqq p^t - 1$, то най-високата степен на p, която дели числителя на дробта $\frac{p^r l - j}{j}$, е равна на най-високата степен на p, която дели знаменателя ѝ j. Следователно в несъкратимия вид на тази дроб числителят и знаменателят не се делят на p. Така цялото число $\binom{p^r l - 1}{p^t - 1}$ се представя като произведение на рационални дроби, числителите и знаменателите на които не се делят на p. Затова то също не се дели на p. Лемата е доказана.

Теорема 12 (първа теорема на Силов). *Нека G е крайна група от ред n и p е просто число. Ако числото p^t $(t \geqq 0)$ дели n, то в G има подгрупа от ред p^t. Ако p^{t+1} дели n, то всяка подгрупа на G от ред p^t се съдържа в някоя подгрупа на G от ред p^{t+1}.*

Доказателство. Нека $n = |G| = p^r l$, $(p, l) = 1$ и p^t дели n. Тогава $t \leqq r$. Да означим с M множеството от всички подмножества на G, които имат точно по p^t различни елемента. Съгласно лема 2 броят $|M|$ на тези подмножества се дели на p^{r-t} и не се дели на p^{r-t+1}. Групата G действува в M, както това е показано в пример 4 от предния параграф, по следния начин: ако $m = \{g_1, g_2, \ldots, g_{p^t}\} \in M$ и $g \in G$, то $gm = \{gg_1, gg_2, \ldots, gg_{p^t}\}$. Ако броят на елементите на всяка орбита на M относно това действие на G се дели на p^{r-t+1}, то и $|M|$ ще се дели на p^{r-t+1}, защото $|M|$ е равно на сумата на броевете елементи на различните орбити. Но p^{r-t+1} не дели $|M|$ и затова съществува орбита $O(m) = \{m_1 = m, m_2, \ldots, m_s\}$ от s елемента, където s не се дели на p^{r-t+1}.

Да означим с H стабилизатора $S_G(m)$ на m в G. Съгласно твърдение 16 и H е подгрупа на G, а по следствие 11 ще бъде вярно равенството $n = p^r l = s|H|$. Тъй като p^r дели $n = s|H|$ и p^{r-t+1} не дели s, то p^t ще бъде делител на реда $|H|$ на подгрупата H. Затова ще бъде изпълнено неравенството $|H| \geqq p^t$.

Нека g е елемент от подмножеството m на G. Тъй като $hm = m$ за всяко $h \in H$, съседният клас Hg ще бъде подмножество на m и затова

$$|H| = |Hg| \leqq |m| = p^t.$$

От получените две неравенства следва, че $|H| = p^t$, т. е. H е подгрупа на G от ред p^t.

Нека p^{t+1} дели n и P е подгрупа на G от ред p^t. Да означим с N множеството от всички подгрупи на G от ред p^t. Ако Q е подгрупа на G от ред p^t, а $g \in G$, то gQg^{-1} е подгрупа на G, спрегната с Q. Тъй като gQg^{-1} има ред, равен на $p^t = |Q|$, то gQg^{-1} е елемент на N. Това показва, че група G действува в N чрез спрягане: $g \circ Q = gQg^{-1}$ за $g \in G$ и $Q \in N$. Нека S е стабилизаторът на P в G относно това действие, а

$$O(P) = \{P_1 = P, P_2, \ldots, P_k\}$$

е класът от спрегнатите с P подгрупи на G, т. е. орбитата, опре-

делена от $\bar{P}$ в N относно действието на G. Знаем, че k е равно на индекса $|G:S|$ на S в G. Подгрупата S на G се състои от всички елементи h на G, за които е изпълнено равенството $hPh^{-1}=P$. Затова $P\subseteq S$ и P е нормален делител в S. С други думи, S е максималната подгрупа на G, в която P се съдържа като нормален делител. (Подгрупата S се нарича още нормализатор на P в G.)

Ако индексът k на S в G не се дели на p, то p^{t+1} ще дели реда на S, тъй като $n=k|S|$ и p^{t+1} дели n. Тогава p ще дели реда на фактор-групата S/P. По първата част на теоремата в S/P ще имаме подгрупа от ред $\bar{p}$, на която пълният първообраз $\bar{P}$ в S ще бъде подгрупа на S (и на G) от ред $p|P|=p^{t+1}$. Тъй като $P\subset\bar{P}$, получихме, че в разглеждания случай P се съдържа в подгрупа от ред p^{t+1}.

Да допуснем сега, че p дели числото k и да разгледаме действието спрягане на групата P в множеството $O(P)$. Относно това действие $P_1=P$ образува едноелементна орбита $\zeta_1=\{P\}$. Нека $\zeta_2, \zeta_3, \ldots, \zeta_q$ са другите орбити на $O(P)$ относно разглежданото действие на P. Тогава

$$k=1+|\zeta_2|+|\zeta_3|+\ldots+|\zeta_q|.$$

Тъй като $|P|=p^t$ и p е просто число, а броят $|\zeta_i|$ на елементите от орбитата ζ_i дели реда p^t на P, то $|\zeta_i|=p^{s_i}$ ($s_i\geqq 0$, $i=2, 3, \ldots, q$), т. е.

$$k=1+p^{s_2}+p^{s_3}+\ldots+p^{s_q}.$$

Ако $s_i\geqq 1$ за $i=2, 3, \ldots, q$, то p ще дели сумата $p^{s_2}+p^{s_3}+\ldots+p^{s_q}$ и числото k. Тогава от последното равенство следва, че p дели единицата, което е невъзможно. Следователно поне едно от числата $s_2, s_3, \ldots, s_q$ е равно на нула. Можем да считаме, че $s_2=0$, т. е. $\zeta_2=\{Q\}$ е едноелементна орбита ($Q\in O(P)$). За всеки елемент $f\in P$ имаме равенството $fQf^{-1}=Q$ и затова $PQ=QP$. Съгасно твърдение 4 произведението PQ е подгрупа на G. Освен това Q е нормален делител в PQ. Наистина ако $g\in PQ$, то $g=fh$ ($f\in P$, $h\in Q$) и $gQg^{-1}=fhQh^{-1}f^{-1}=fQf^{-1}=Q$. Понеже P и Q се съдържат в PQ, $P\neq Q$ и $|P|=|Q|=p^t$, то $Q\neq PQ$. Затова фактор-групата PQ/Q е неединична група. Нека $\eta: PQ\to PQ/Q$ е естественият хомоморфизъм на PQ върху нейната фактор-група PQ/Q. Ако $g\in PQ$, то $g=fh$ ($f\in P$, $h\in Q$) и затова

$$gQ=fhQ=fQ=\eta(f).$$

Следователно хомоморфизмът η изобразява подгрупата P върху PQ/Q. Тъй като P е p-група, а неединичен хомоморфен образ на p-група е също p-група, фактор-групата PQ/Q е p-група. По първата част на теоремата във фактор-групата PQ/Q има подгрупа от ред p. Пълният първообраз A при η на тази подгрупа е подгрупа в PQ (и в G) от ред $p|Q|=p^{t+1}$, която съдържа Q. Тъй като P и Q са спрегнати в G, то $P=gQg^{-1}$ за някой елемент

$g \in G$. Да разгледаме подгрупата $B = gAg^{-1}$ на G. Тя е спрегната с подгрупата A и затова $|B| = |A| = p^{t+1}$. Освен това от включването $Q \subset A$ следва включването $P = gQg^{-1} \subset gAg^{-1} = B$, т. е. P се съдържа в подгрупата B, която е от ред p^{t+1}. Теоремата е доказана.

Следствие 12. *Ако p е просто число и p^r $(r \geqq 1)$ е най-високата степен на p, която дели реда n на крайната група G, то всяка силовска p-подгрупа на G има ред, равен на p^r.*

Теорема 13 (втора теорема на Силов). *Всеки две силовски p-подгрупи на една крайна група са спрегнати.*

Доказателство. Нека G е крайна група от ред $n = p^r l$, където $r \geqq 1$ и $(p, l) = 1$, а P и Q са две силовски p-подгрупи на G. По следствие 12 ще бъдат изпълнени равенствата $|P| = |Q| = p^r$. Да означим с M множеството от всички силовски p-подгрупи на G и да разгледаме действието спрягане на G в M, т. е. ако $g \in G$ и $S \in M$, то $g \circ S = gSg^{-1}$. Целта ни е да покажем, че в M има само една орбита относно това действие на G, а именно цялото множество M.

Нека $O(P) = \{P_1 = P, P_2, \ldots, P_k\}$ е орбитата, определена от P, и $H = S_G(P)$ е стабилизаторът (нормализаторът) на P в G. Тъй като $P \subseteq H$ и $|P| = p^r$, то $|H| = p^r l_1$. Но $n = |G| = p^r l$ и редът на H дели n. Затова индексът k на H в G е равен на $\frac{l}{l_1}$ и е взаимно прост с числото p. Да разгледаме действието спрягане на p-групата Q в множеството $O(P)$. Множеството $O(P)$ относно това действие се разбива на непресичащи се орбити $\zeta_1, \zeta_2, \ldots, \zeta_q$, съответно с по $c_1, c_2, \ldots, c_q$ на брой елемента. Понеже числата c_i делят реда $|Q| = p^r$ на Q и p е просто число, то $c_i = p^{\lambda_i}$ $(\lambda_i \geqq 0, i = 1, 2, \ldots, q)$. Освен това

$$k = p^{\lambda_1} + p^{\lambda_2} + \ldots + p^{\lambda_q}.$$

Тъй като k не се дели на p, поне едно от числото λ_i е равно на нула. Можем да считаме, че $\lambda_1 = 0$ и $\zeta_1 = \{U\}$ $(U \in O(P))$ е едноелементна орбита относно действието на Q. Тогава $UQ = QU$, тъй като $fUf^{-1} = U$ за всяко $f \in Q$. Както в доказателството на предната теорема се вижда, че фактор-групата UQ/Q е p-група и тъй като Q е p-група, то UQ е p-подгрупа на G. Понеже U и Q се съдържат в UQ и са силовски p-подгрупи, то $Q = UQ = U \in O(P)$ и Q се оказва спрегната със силовската p-подгрупа P. Теоремата е доказана.

Следствие 13. *Всеки две силовски p-подгрупи на една крайна група са изоморфни.*

Действително ако P и Q са две силовски p-подгрупи на крайната група G, то $Q = gPg^{-1}$ за някой елемент $g \in G$. Лесно се проверява, че изображението $\varphi: P \to Q$, определено с равенството $\varphi(f) = gfg^{-1}$ $(f \in P)$, е изоморфизъм на P върху Q.

Теорема 14 (трета теорема на Силов). *Ако редът n на крайната група G се дели на простото число p, то броят на*

силовските p-подгрупи на G дели n и е равен на $1+kp$, *където* $k \geqq 0$.

Доказателство. Нека M е множеството от всички силовски p-подгрупи на G и $m=|M|$, а Q е една силовска p-подгрупа на G. Разглеждаме действието спрягане на Q в M. Множеството M се разбива на непресичащи се орбити относно това действие. Самата подгрупа Q като елемент на M образува една едноелементна орбита $\{Q\}$. Ще покажем, че всяка друга орбита е съставена от повече от един елемент. Да допуснем, че $\{P\}$ е друга едноелементна орбита. Тогава, както в доказателството на предишната теорема, се получава, че $PQ=QP$ е p-подгрупа на G и затова тя ще съвпада със силовските p-подгрупи P и Q, т. е. $P=Q$, което е противоречие. Нека $\zeta_1=\{Q\}, \zeta_2, \ldots, \zeta_q$ са различните орбити в M относно действието на Q. Тогава $|\zeta_i|=p^{\lambda_i}$ ($\lambda_i \geqq 1$, $i=2, 3, \ldots, q$), тъй като $|\zeta_i| \geqq 2$ и $|\zeta_i|$ делят реда $|Q|=p^l$ на силовската p-подгрупа Q. Понеже

$$m=1+p^{\lambda_2}+p^{\lambda_3}+\ldots+p^{\lambda_q}$$

и $\lambda_i \geqq 1$ ($i=2, 3, \ldots, q$), то $m=1+kp$ ($k \in Z$).

Да разгледаме действието спрягане на цялата група G в множеството M от нейните силовски p-подгрупи. По предишната теорема в M ще има само една орбита относно това действие, а именно цялото множество M. Затова $m=|M|$ дели реда на групата G (виж твърдение 19). Теоремата е доказана.

ГЛАВА V

ПРЪСТЕНИ И ПОЛЕТА

§ 1. Определение на пръстен. Примери

Определение 1. Непразното множество A се нарича *пръстен*, ако в него са определени две бинарни алгебрични операции, които условно наричаме събиране и умножение, така че спрямо събирането A е абелева група, а за умножението е изпълнен асоциативният закон и двете операции са свързани с двата дистрибутивни закона

$$a(b+c)=ab+ac,\ (b+c)a=ba+ca \quad (a, b, c \in A).$$

Пръстенът A се нарича *комутативен*, ако за операцията умножение в A е в сила комутативният закон, т. е. $ab=ba$ за всяко $a, b \in A$, и *некомутативен* — в противния случай.

Примери на пръстени

1. Множествата $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ съответно на целите, рационалните, реалните и комплексните числа с обикновените операции събиране и умножение на числа.

2. Множеството $\{0\}$, което се състои от един нулев елемент, с операции, определени по следния начин: $0+0=0$, $0 \cdot 0=0$.

3. Множеството $n\mathbf{Z}$ на всички цели числа, които се делят на цялото положително число n.

4. Множеството $\mathbf{Z}(i)$ от целите гаусови числа, т. е. множеството на всички комплексни числа $a+bi$, където a и b са цели числа.

5. Множествата $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$ и $\mathbf{C}[x]$ съответно на всички полиноми с цели, рационални, реални и комплексни коефициенти.

6. Двойките цели числа (a, b) образуват пръстен, който означаваме със $\mathbf{Z} \oplus \mathbf{Z}$, ако операциите събиране и умножение се определят покомпонентно с равенствата

$$(a, b)+(c, d)=(a+c, b+d);\ (a, b)(c, d)=(ac, bd).$$

7. Множеството $F[0, 1]$ на всички реални функции, дефинирани в интервала $[0, 1]$ с обикновеното събиране и умножение на функции:

$$(f+g)(x)=f(x)+g(x),\ (fg)(x)=f(x)g(x).$$

8. Множеството $M(n, \mathbf{C})$ на всички квадратни матрици от ред n с комплексни елементи относно обикновените операции събиране и умножение на матрици. Този пръстен се нарича *пълен матричен пръстен* над пръстена C на комплексните числа.

Комутативни пръстени са **всички пръстени от примерите** 1)—7.

Пълният матричен пръстен $M(n, C)$ при $n \geqq 2$ е некомутативен. Наистина нека E_{ij} е матрицата от $M(n, C)$, в която елементът от нейния i-ти ред и j-ти стълб е 1, а всички останали елементи са нули. Тогава матриците E_{11} и E_{12} от $M(n, C)$ не комутират, защото

$$E_{11}E_{12}=E_{12},\quad E_{12}E_{11}=0 \text{ и } E_{12}\neq 0.$$

Асоциативните закони ни дават възможност да дефинираме сума и произведение на произволен краен брой елементи a_1, a_2, ..., a_n на пръстена A независимо от поставянето на скобите, които ще записваме съкратено така:

$$a_1+a_2+\ldots+a_n=\sum_{i=1}^{n} a_i,\quad a_1a_2\ldots a_n=\prod_{i=1}^{n} a_i.$$

Като се използува комутативният закон на събирането (съответно на умножението) в пръстена A, с индукция се доказва че сумата (произведението) на произволен брой елементи на пръстена не зависи от реда на събираемите (множителите).

Сумата на n еднакви събираеми a ще наричаме *n-кратно* на a и ще го означаваме чрез na. Произведението на n еднакви множителя a се нарича *n-та степен* на елемента a и се означава чрез a^n.

От определението на сума и произведение на произволен брой елементи следва, че за произволни естествени числа m и n са изпълнени следните равенства:

(1) $$(m+n)a=ma+na,$$

(2) $$(mn)a=m(na),$$

(3) $$n(a+b)=na+nb,$$

(4) $$a^m a^n=a^{m+n},$$

(5) $$(a^m)^n=a^{mn},$$

(6) $$(ab)^n=a^n b^n, \text{ ако } ab=ba,$$

(7) $$n(ab)=(na)b=a(nb),$$

(8) $$(ma)(nb)=(mn)ab.$$

Например равенство (7) се доказва по следния начин:

$$n(ab)=ab+ab+\ldots+ab=(a+a+\ldots+a)b=(na)b.$$

Пръстенът A съгласно определението по отношение на събирането е абелева група. Тази група ще наричаме *адитивна група на пръстена A*. Следователно изпълнени са следните твърдения:

1) *във всеки пръстен A съществува единствен нулев елемент* 0;

2) *за всеки елемент a от A съществува единствен противоположен елемент* $-a$;

3) *сумата* $a+(-b)$, *където* a *и* b *са произволни елементи от* A, *ще означаваме с* $a-b$ *и ще наричаме разлика на елементите* a *и* b, *т. е.*

$$a-b=a+(-b).$$

Разликата $a-b$ е единственото решение на уравнението $x+b=b+x=a$.

Лесно се проверява, че противоположният елемент на сумата на произволен брой събираеми е равен на сумата от противоположните елементи на събираемите, т. е.

$$-\left(\sum_{i=1}^{n} a_i\right)=\sum_{i=1}^{n}(-a_i)\ .$$

За n равни събираеми получаваме равенството $-na=n(-a)$. По определение ще считаме, че $(-n)\,a=-na=n\,(-a)$, т. е. по този начин в пръстена A се въвеждат отрицателни кратни на елемента a. За числото 0 полагаме $0a=0$ (отляво 0 е числото нула, а отдясно на равенството — нулевият елемент на пръстена). Така кратните na на елемента a са определени за всяко цяло число n. Знаем, че в адитивната група на пръстена формулите (1) и (2) са верни за произволни цели числа m и n.

Задача. Докажете, че формулата (3) е вярна за произволно цяло число n.

Във формулировката на дистрибутивните закони участвува само сумата на две събираеми. Но лесно се доказва, че са верни равенствата

$$\left(\sum_{i=1}^{m} a_i\right)b=\sum_{i=1}^{m} a_i b,\quad b\left(\sum_{i=1}^{m} a_i\right)=\sum_{i=1}^{m} b a_i.$$

а така също и равенството

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{i=1}^{n} b_i\right)=\sum_{i=1}^{m}\sum_{j=1}^{n} a_i\, b_j.$$

Ще отбележим още следните свойства на пръстените:

1. *Във всеки пръстен произведението на произволен елемент с нулевия елемент е равно на нулевия елемент.*

Действително ако x е произволен (спомагателен) елемент от пръстена, то $ax=a\,(x+0)=ax+a0$ и понеже спрямо събирането A е абелева група, то $a\,0=0$. По аналогичен начин се доказва, че $0\,a=0$.

2. *Във всеки пръстен за произволни негови елементи* a *и* b *са изпълнени равенствата*

$$(-a)\,b=-(ab),\ a\,(-b)=-(ab).$$

Наистина

$$0=0\ b=[a+(-a)]\ b=ab+(-a)\ b,$$

т. е. $(-a)\ b=-(ab)$. Второто равенство се доказва аналогично. Обикновено вместо $-(ab)$ ще пишем $-ab$.

Като следствие получаваме известното правило за умножение на отрицателни числа („минус по минус дава плюс“):

$$(-a)(-b)=ab\ \ (a,\ b\in A),$$

тъй като

$$(-a)(-b)=-[a(-b)]=-[-(ab)]=ab.$$

3. *Във всеки пръстен са изпълнени дистрибутивните закони и за разлика, т. е.*

$$(a-b)\ c=ac-bc,\ \ c\ (a-b)=ca-cb.$$

Действително

$$(a-b)\ c=[a+(-b)]\ c=ac+(-b)\ c=ac+(-bc)=ac-bc.$$

По същия начин се доказва и второто равенство.

Лесно се доказва, че в произволен пръстен за разликата са в сила следните свойства:

а) $a-b=c-d$ тогава и само тогава, когато $a+d=b+c$;

б) $(a-b)+(c-d)=(a+c)-(b+d)$;

в) $(a-b)-(c-d)=(a+d)-(b+c)$;

г) $(a-b)(c-d)=(ac+bd)-(ad+bc)$.

Освен това равенствата (1), (2), (7) и (8) са в сила за произволни $m,\ n\in Z$.

§ 2. Делители на нулата и обратими елементи в пръстен

Определение 2. Елементите a и b на пръстена A, за които $a\neq 0$, $b\neq 0$, но $ab=0$, се наричат *делители на нулата*. По-точно елементът a се нарича *ляв делител на нулата*, а елементът b — *десен делител на нулата*.

Примери

1. Всички пръстени, посочени в примерите 1—5 от § 1, са пръстени без делители на нулата.

2. В пръстени $Z\oplus Z$ (§ 1, пример 6) има делители на нулата. Например $(1,\ 0).(0,\ 1)=(0,\ 0)$, но елементите $(1,\ 0)$ и $(0,\ 1)$ са ненулеви в $Z\oplus Z$. Въобще всички делители на нулата в пръстена $Z\oplus Z$ са елементите от вида $(a,\ 0)$ и $(0,\ b)$, където $a\neq 0$ и $b\neq 0$.

3. В пръстена $F[0,\ 1]$ (§ 1, пример 7) има делители на нулата.

Нека $f=f(x)$ е различна от нула реална функция, определена в интервала $[0,\ 1]$ и която приема стойност нула поне за едно x_0 $(0\leqq x_0\leqq 1)$. Да разгледаме функцията g, дефинирана по следния начин:

$$g(x)=\begin{cases}1, \text{ ако } f(x)=0 \text{ и } 0\leqq x\leqq 1;\\ 0, \text{ ако } f(x)\neq 0 \text{ и } 0\leqq x\leqq 1.\end{cases}$$

Очевидно функцията g не е равна на нула, но $fg=0$, т. е. f и g са делители на нулата в пръстена $F[0, 1]$.

Твърдение 1. *Ако елементът a на комутативния пръстен A е делител на нулата, то всяко произведение ac ($c \in A$) е или нула, или делител на нулата.*

Доказателство. Да допуснем, че $ac \neq 0$. Тъй като a е делител на нулата в A, в A съществува такъв ненулев елемент b, че $ba=0$. Тогава $b(ac)=(ba)c=0c=0$, т. е. елементът ac е делител на нулата.

Твърдение 2. *Във всеки пръстен A без делители на нулата са в сила законите за съкращаване на ненулеви елементи, т. е. от $ab=ac$ или $ba=ca$ и $a \neq 0$ следва, че $b=c$.*

Действително от $ab=ac$ следва, че $a(b-c)=0$ и тъй като $a \neq 0$, то $b-c=0$.

Ако в пръстена A съществува единичен елемент e, т. е. такъв елемент e, че $ae=ea=a$ за всяко $a \in A$, то ще казваме, че пръстенът A е *пръстен с единица*.

Както в теорията на групите, се доказва, че единичният елемент (ако съществува) е единствен.

За произволни естествени числа s и t е в сила формулата

$$(st)e=(se)(te). \tag{1}$$

Наистина $(st)e=s(te)=s(ete)=(se)(te)$, където първото и последното равенство следват съответно от формулите (2) и (7) на § 1.

Единичният елемент на пръстена ще означаваме по-нататък с 1, като от текста ще бъде ясно кога става дума за числото единица и кога за единичния елемент на пръстена. В примерите 1, 2, 4—7 пръстените са пръстени с единица. В пръстена от пример 2 единицата съвпада с нулевия елемент.

Задача. Ако в пръстена A с единица е в сила равенството $1=0$, то A се състои само от нулевия елемент.

Ако $n>1$ е цяло число, то пръстенът nZ (§ 1, пример 3) е пръстен без единица.

Определение 3. Ако A е пръстен с единица 1, то елементът a от A се нарича обратим или делител на единицата, ако в A съществува такъв елемент b, че $ab=ba=1$.

Ако a е обратим елемент, както в теорията на групите се доказва, че елементът b със свойството $ab=ba=1$ е единствен. Този единствен елемент ще наричаме *обратен* на елемента a и ще го означаваме с a^{-1}.

Примери

1. В пръстена Z на целите числа обратими елементи са само 1 и -1. В пръстените Q, R и C обратими елементи са всички числа, различни от нула.

2. В пръстена от пример 2 на § 1 имаме равенството $0=1$ и този единствен елемент е обратим.

3. Ако $n \neq 1$, то nZ е пръстен без единица и за обратими елементи в този пръстен не можем да говорим.

4. В пръстена $\mathbf{Z}(i)$ обратимите елементи са ± 1 и $\pm i$.

5. В пръстена $\mathbf{Z}[x]$ обратими елементи са 1 и -1. В $\mathbf{Q}[x]$, $\mathbf{R}[x]$ и $\mathbf{C}[x]$ обратими елементи са ненулевите полиноми от степен нула.

6. В $\mathbf{Z} \oplus \mathbf{Z}$ обратими елементи са само $(1, 1)$, $(-1, 1)$, $(1, -1)$ и $(-1, -1)$.

7. В пръстена $F[0, 1]$ обратими елементи са само функциите, които за всяко x $(0 \leqq x \leqq 1)$ приемат стойности, различни от нула.

8. В пръстена $M(n, \mathbf{C})$ обратими елементи са само неособените матрици.

Твърдение 3. *Ако A е пръстен с единица, а a и b са два обратими елемента в A, то елементите a^{-1} и ab са също обратими в A.*

Доказателство. Тъй като $aa^{-1} = a^{-1}a = 1$ и $(ab)(b^{-1}a^{-1}) = 1$, то a^{-1} и ab са обратими и $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$.

Следствие 1. *Ако A^* е подмножеството от всички обратими елементи на пръстен A с единица, то A^* е група спрямо операцията умножение.*

Групата A^* ще наричаме *мултипликативна група на пръстена A.*

Задача. Докажете, че обратим елемент не може да бъде делител на нулата.

Определение 4. Ако комутативният пръстен A с единица е без делители на нулата и единицата не съвпада с нулевия елемент на A, то пръстенът A се нарича *област на цялостност.*

Пръстените $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}(i)$, $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$, $\mathbf{C}[x]$ са области на цялостност.

§ 3. Подпръстени и идеали

Определение 5. Непразното подмножество M на пръстена A се нарича негов *подпръстен*, ако M е пръстен относно операциите, спрямо които A е пръстен.

Например $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ и всеки пръстен е подпръстен на всеки от следващите след него пръстени; $n\mathbf{Z}$ е подпръстен на $\mathbf{Z}$; $\mathbf{Z}(i)$ е подпръстен на $\mathbf{C}$ и т. н. Във всеки пръстен подмножеството $\{0\}$, съставено само от нулевия елемент, е подпръстен. Всеки пръстен A е подпръстен на себе си. Последните два подпръстена се наричат тривиални (несобствени), а всички останали подпръстени на A се наричат нетривиални (собствени).

При проверката дали дадено подмножество M на пръстена A е подпръстен е удобно да се използува следното

Твърдение 4. *Непразното подмножество M на пръстена A е негов подпръстен тогава и само тогава, когато разликата и произведението на всеки два елемента от M се съдържат в M.*

Действително ако M е подпръстен на A, то очевидно разликата и произведението на всеки два елемента от M са също еле-

менти на M. Обратно, ако непразното подмножество M на пръстена A заедно с всеки два свои елемента съдържа тяхната разлика и произведение, то M е адитивна абелева група (вж. твърдение 2, глава IV), а останалите аксиоми за пръстен автоматично се пренасят от пръстена A за неговото подмножество M.

Например подмножеството от всички цели положителни числа не е подпръстен на $\mathbf{Z}$. То съдържа заедно с всеки два елемента тяхната сума и произведение, но тяхната разлика — невинаги.

Нека M е подмножество на пръстена $\mathbf{Q}$, съставено от всички цели числа и числата от вида $n+\frac{1}{2}$, където n е цяло число. Очевидно M заедно с всеки два свои елемента съдържа и тяхната сума и разлика (т. е. M е подгрупа на адитивната група на пръстена $\mathbf{Q}$). Но M не е подпръстен в $\mathbf{Q}$, тъй като $\frac{1}{2}\in M$, но $\frac{1}{4}=\frac{1}{2}\cdot\frac{1}{2}$ не се съдържа в M, т. е. M не съдържа произведението на всеки два свои елемента.

Определение 6. Подпръстенът I на пръстена A се нарича *ляв* (*десен*) *идеал* на A, ако за всеки елемент a от I и за всеки елемент r от A произведението $ra(ar)$ е елемент от I, т. е. подпръстенът I издържа умножението отляво (отдясно) с елементи от пръстена A. Ако I е едновременно и ляв, и десен идеал на A, то I се нарича *двустранен идеал* или просто *идеал* на пръстена A.

Примери.

1. Подпръстенът $n\mathbf{Z}$ на $\mathbf{Z}$ е идеал на $\mathbf{Z}$.

2. Подмножествата $I_1=\{(a,\ 0)\mid a\in\mathbf{Z}\}$ и $I_2=\{(0,\ b)\mid b\in\mathbf{Z}\}$ са идеали на пръстена $\mathbf{Z}\oplus\mathbf{Z}$.

3. Нека x_0, $0\leqq x_0\leqq 1$, е фиксирано число. Подмножеството

$$F_{x_0}[0,\ 1]=\{f\ \ f\in F[0,\ 1],\ \ f(x_0)=0\}$$

е идеал на $F[0,\ 1]$.

Трябва да отбележим, че не всеки подпръстен е идеал. Така например Z не е идеал в $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$; $\mathbf{Q}$ не е идеал в $\mathbf{R}$ и $\mathbf{C}$; $\mathbf{R}$ и $Z(i)$ не са идеали в $\mathbf{C}$ и т. н.

Във всеки пръстен A нулевият подпръстен $\{0\}$ и целият пръстен A са идеали в A.

Идеалът I на пръстена A се нарича нетривиален (собствен, истински) идеал, ако $I\neq A$, $\{0\}$, и тривиален, ако $I=A$ или $I=\{0\}$.

Задача. Ако I е идеал на A, който съдържа поне един обратим елемент, то $I=A$.

Определение 7. *Сума* $I_1+I_2+\ldots+I_n$ на идеалите I_1, $I_2,\ldots,I_n$ на пръстена A наричаме подмножеството на A, което се състои от всевъзможните суми от вида $x_1+x_2+\ldots+x_n$, където $x_i\in I_i$ $(i=1,\ 2,\ \ldots,\ n)$.

Теорема 1. *Сумата на краен брой идеали и сечението на произволен брой идеали на пръстена A са идеали на A.*

Доказателство. Теоремата ще докажем за два идеала.

Нека I и J са два идеала на A, $r \in A$, а z_1 и z_2 са два произволни елемента от $I+J$. Тогава $z_i = x_i + y_i$, където $x_i \in I$ и $y_i \in J$ $(i=1, 2)$. Тъй като I и J са идеали на A, то $x_1 r$, $r x_1$, $x_1 - x_2 \in I$ и $y_1 r$, $r y_1$, $y_1 - y_2 \in I$. Следователно елементите

$$rz_1 = rx_1 + ry_1,\ z_1 r = x_1 r + y_1 r,\ z_1 - z_2 = (x_1 - x_2) + (y_1 - y_2)$$

се съдържат в $I+J$, т. е. $I+J$ е идеал на A. Ако t_1 и t_2 са произволни елементи от сечението $I \cap J$, то $t_1 r$, $r t_1$ и $t_1 - t_2$ също принадлежат на сечението, тъй като I и J са идеали. Затова $I \cap J$ е идеал на A. Доказателството в общия случай се извършва по аналогичен начин.

Някои от идеалите на даден комутативен пръстен представляват особен интерес. Ще разгледаме три отделни типа идеали.

Нека a е произволен елемент на комутативния пръстен A с единица 1. Да означим с (a) множеството от всички елементи на A от вида ar, където r е произволен елемент на A, т. е.

$$(a) = \{ar \mid r \in A\}.$$

Очавидно елементът a се съдържа в (a). Не е трудно да се види, че подмножеството (a) е идеал на пръстена A.

Определение 8. Идеалът (a) ще наричаме *главен идеал* на A, породен от елемента a.

Пример. Ако $n \geqq 1$ е цяло число, то $n\mathbf{Z}$ е главен идеал на $\mathbf{Z}$, породен от n, т. е. $n\mathbf{Z} = (n)$.

Теорема 2. *Всеки подпръстен на пръстена* $\mathbf{Z}$ *на целите числа е главен идеал на* $\mathbf{Z}$.

Доказателство. Адитивната група на пръстена $\mathbf{Z}$ е безкрайна циклична и всяка нейна подгрупа е също циклична. Нека $H \neq \{0\}$ е произволна подгрупа на адитивната група на $\mathbf{Z}$. Тогава H се поражда от най-малкото цяло положително число n, което се съдържа в H и се състои от всички цели числа, които се делят на n. Следователно $H = n\mathbf{Z} = (n)$. Така доказахме по-силен резултат от твърдението на теоремата, а именно всяка подгрупа на адитивната група на пръстена $\mathbf{Z}$ е главен идеал в $\mathbf{Z}$.

Определение 9. Идеалът I на комутативния пръстен A с единица се нарича *прост*, ако са изпълнени следните условия

(*i*) $I \neq A$;

(*ii*) ако $ab \in I$, то поне един от елементите a и b се съдържа в I.

Примери

1. Идеалите $I_1 = \{(a, 0) \mid a \in \mathbf{Z}\}$ и $I_2 = \{(0, b) b \mid \in \mathbf{Z}\}$ са прости идеали на пръстена $\mathbf{Z} \oplus \mathbf{Z}$.

2. Идеалът $F_{x_0}[0, 1]$ $(0 \leqq x_0 \leqq 1)$ е прост идеал на пръстена $F[0, 1]$.

3. Ако p е просто число, то главният идеал $p\mathbf{Z} = (p)$ е прост идеал в пръстена $\mathbf{Z}$.

Определение 10. Идеалът I на пръстена A с единица ще наричаме *максимален*, ако са изпълнени условията

(*i*) $I \neq A$;
(*ii*) ако J е идеал на A и $I \subset J \subseteq A$, то $J = A$.

Примери

1. Ако p е просто число, то главният идеал $p\mathbf{Z}$ е максимален идеал на $\mathbf{Z}$.

2. Ако x_0, $0 \leqq x_0 \leqq 1$, е произволно число, идеалът $F_{x_0}[0, 1]$ е максимален идеал в пръстена $F[0, 1]$.

Теорема 3. *Всеки максимален идеал на комутативен пръстен с единица е прост идеал.*

Доказателство. Нека A е произволен комутативен пръстен с единица, I е максимален идеал на A и произведението ab е елемент от I. Да допуснем, че a не се съдържа в I. Да означим с K главния идеал (a) и да разгледаме идеала $J = I + K$. Идеалът J съдържа идеала (a), но $I \neq J$, тъй като $a \in K$ (т. е. $a \in J$) и a не се съдържа в идеала I. Тъй като I е максимален и $I \subset J \subseteq A$, то $J = A$. Тогава $1 \in J$, т. е. $1 = c + ra$, където $c \in I$ и $ra \in K$. Като умножим двете страни на последното равенство с b, получаваме

$$b = cb + rab.$$

Дясната страна на това равенство е сума на два елемента от I и затова е елемент от I. Следователно елементът b се съдържа в идеала I. С това доказахме, че максималният идеал I е прост идеал на A.

Задача. Докажете, че простите идеали $I_1 = \{(a, 0) \mid a \in \mathbf{Z}\}$ и $I_2 = \{0, b) \mid b \in \mathbf{Z}\}$ не са максимални в пръстена $\mathbf{Z} \oplus \mathbf{Z}$.

Следователно твърдението, обратно на твърдението на теорема 3, не е вярно, т. е. че всеки прост идеал е максимален.

Задача. Всеки ненулев прост идеал на пръстена $\mathbf{Z}$ на целите числа е максимален.

§ 4. Фактор-пръстени

Нека B е произволна подгрупа на адитивната група на пръстена A. В такъв случай можем да образуваме адитивната фактор-група A/B. Можем ли да пренесем операцията умножение от пръстена A във фактор-групата A/B, така че A/B да се превърне в пръстен? В общия случай отговорът е отрицателен. При решението на този въпрос се проявява важното значение на понятието идеал, а именно, ако I е идеал в A, то в адитивната фактор-група A/I може да бъде пренесена и операцията умножение от A. Наистина да положим

$$(a + I)(b + I) = ab + I,$$

където $a + I$, $b + I$ са произволни съседни класове от A/I.

Така определеното умножение в A/I е коректно, т. е. не зависи от конкретните представители a и b на съседните класове. И наистина ако $a_1 + I = a + I$ и $b_1 + I = b + I$, то $a_1 = a + c_1$ и $b_1 = b + d_1$,

където $c_1, d_1 \in I$. По определение $(a_1+I)(b_1+I)=a_1b_1+I$. Трябва да докажем, че

$$ab+I=a_1b_1+I.$$

Но $a_1b_1=(a+c_1)(b+d_1)=ab+ad_1+c_1b+c_1d_1$. Тъй като елементът $ad_1+c_1b+c_1d_1$ се съдържа в I, то от горното равенство следва, че елементите a_1b_1 и ab са представители на един и същ съседен клас на A по I, т. е. $ab+I=a_1b_1+I$. С това коректността на дефиницията на умножението в A/I е доказана.

Ще докажем, че A/I е пръстен относно операциите събиране и умножение на съседни класове, който наричаме *фактор-пръстен* на пръстена A по неговия идеал I. Наистина A/I е фактор-група на адитивната група на пръстена A, т. е. абелева група спрямо събирането. Да проверим останалите аксиоми за пръстен.

Асоциативността на умножението следва от равенствата

$$(a+I)[(b+I)(c+I)]=(a+I)(bc+I)=a(bc)+I=$$
$$=(ab)c+I=(ab+I)(c+I)=[(a+I)(b+I)](c+I).$$

По подобен начин се проверяват и дистрибутивните закони.

Например десният дистрибутивен закон се установява по следния начин:

$$[(a+I)+(b+I)](c+I)=[(a+b)+I](c+I)=(a+b)c+I=$$
$$=(ac+bc)+I=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I)$$

където са използувани съответните закони, които са изпълнени в пръстена A.

Ако A е пръстен с единица 1, а I е произволен идеал в A, то фактор-пръстенът A/I е пръстен с единица $1+I$. Действително

$$(a+I)(1+I)=a\,.\,1+I=a+I=1\,.\,a+I=(1+I)(a+I).$$

Пример. Нека n е произволно цяло положително число. Вече знаем, че nZ е главен идеал в пръстена Z, т. е. $nZ=(n)$. Фактор-пръстенът $Z/(n)$ съдържа n елемента. Това са съседните класове

$$0+(n)=(n),\ 1+(n),\ \ldots,\ n-1+(n).$$

Този фактор-пръстен на Z ще бележим със Z_n и ще наричаме *пръстен на класовете остатъци по модул n* или просто *пръстен на остатъците по модул n*.

Задача. Пръстенът Z_n е пръстен без делители на нулата тогава и само тогава, когато $n=1$ или n е просто число.

Задача. Идеалът I на ненулевия комутативен пръстен A с единица е прост тогава и само тогава, когато фактор-пръстенът A/I е област на цялостност.

Задача. Идеалът I на комутативния пръстен A с единица е максимален тогава и само тогава, когато всеки ненулев елемент на фактор-пръстена A/I е обратим.

§ 5. Хомоморфизми. Теорема за хомоморфизмите

Определение 11. Нека A и B са пръстени. Изображението $\varphi: A \to B$ се нарича *хомоморфизъм* на пръстена A в пръстена B, ако са изпълнени следните условия:

(i) φ е изображение на множеството A в множеството B;

(ii) за всеки два елемента $a_1, a_2 \in A$ са изпълнени равенствата

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2), \quad \varphi(a_1 a_2) = \varphi(a_1)\,\varphi(a_2).$$

Другояче казано, φ е хомоморфизъм на адитивната група на пръстена A в адитивната група на пръстена B, който изобразява произведението на елементи от A в произведението на образите им в B.

Ще казваме, че хомоморфизмът $\varphi: A \to B$ е хомоморфизъм на A върху B, ако всеки елемент от B има първообраз при φ от A. Ако съществува поне един хомоморфизъм на пръстена A върху пръстена B, то B ще наричаме *хомоморфен образ* на пръстена A.

Определение 12. Ще казваме, че хомоморфизмът φ на пръстена A върху пръстена B е *изоморфизъм* или *пръстенов изоморфизъм*, ако φ е взаимно еднозначно изображение на A върху B.

Ако съществува поне един изоморфизъм на пръстена A върху пръстена B, то пръстените A и B ще наричаме *изоморфни* и тогава ще пишем $A \cong B$.

Задача. Да се докаже, че отношението „изоморфни“ е релация на еквивалентност.

Примери

1. Нека m е произволно цяло число, а $f(x)$ е произволен полином от пръстена $\mathbf{Z}[x]$. Тогава $f(m)$ е цяло число. Да определим изображението φ_m на $\mathbf{Z}[x]$ в $\mathbf{Z}$ с равенството

$$\varphi_m[f(x)] = f(m).$$

Тогава лесно се проверява, че φ_m е хомоморфизъм на пръстена $\mathbf{Z}[x]$ върху пръстена $\mathbf{Z}$.

По подобен начин можем да определим хомоморфизми на пръстените $\mathbf{Q}[x]$, $\mathbf{R}[x]$ и $\mathbf{C}[x]$ съответно върху пръстените $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$.

2. Изображението φ_1 на пръстена $\mathbf{Z} \oplus \mathbf{Z}$ в $\mathbf{Z}$, определено с равенството

$$\varphi_1[(a, b)] = a,$$

е хомоморфизъм $\mathbf{Z} \oplus \mathbf{Z}$ върху пръстена $\mathbf{Z}$.

3. Ако x_0 е фиксирано число от интервала $[0, 1]$, а φ_{x_0} е изображение на пръстена $F[0, 1]$ в $\mathbf{R}$, определено с равенството $\varphi_{x_0}(f) = f(x_0)$, то φ_{x_0} е хомоморфизъм на пръстена $F[0, 1]$ върху пръстена $\mathbf{R}$ на реалните числа.

4. Нека A е произволен пръстен, I — идеал на A, а A/I е съответният фактор-пръстен. Изображението $\eta: A \to A/I$, определено с равенството

$$\eta(a) = a + I$$

за всяко $a \in A$, е хомоморфизъм на пръстена A върху негов фактор-пръстен A/I и се нарича *естествен хомоморфизъм* на A върху A/I.

По този начин, като съпоставим на всяко цяло число m класа $m+(n)$, получаваме естествения хомомсрфизъм на пръстена Z на целите числа върху пръстена Z_n от остатъците по модул n.

Определение 13. Ако φ е произволен хомоморфизъм на пръстена A в пръстена B, то подмножеството на A, съставено от всички елементи, които φ изобразява в нулата на пръстена B, се нарича *ядро* на хомоморфизма φ и се бележи с $\ker\varphi$, т. е

$$\ker\varphi=\{a \mid a \in A,\ \varphi(a)=0\}.$$

Задача. Да се докаже, че ядрото на хомоморфизма φ е идеал на пръстена A.

Задача. Докажете, че ядрата на всевъзможните хомоморфизми на даден пръстен и само те са неговите идеали.

Ако $\varphi: A \to B$ е хомоморфизъм на пръстена A в пръстена B, то подмножеството $\operatorname{Im}\varphi=\{\varphi(a) \mid a \in A\}=\varphi(A)$ на B се нарича *образ* на A при φ.

Задача. Докажете, че образът $\varphi(A)=\operatorname{Im}\varphi$ на пръстена A при φ е подпръстен на B.

По този начин съпоставихме на всеки пръстен A две серии от пръстени:

1) всички фактор-пръстени на A;

2) всички хомоморфни образи на A.

При това видяхме, че всеки фактор-пръстен на пръстена A е негов хомоморфен образ при съответния естествен хомоморфизъм. Но до каква степен хомоморфните образи на един комутативен пръстен могат да се различават от неговите фактор-пръстени? На този въпрос пълен отговор дава следната

Теорема 4 (теорема за хомоморфизмите). *Ако $\varphi: A \to B$ е хомоморфизъм на пръстена A върху пръстена B и I е ядрото на φ, то фактор-пръстенът A/I е изоморфен на пръстена B. При това съществува такъв изоморфизъм σ на A/I върху B, че произведението $\sigma\eta$ на изоморфизма σ с естествения хомоморфизъм η на пръстена A върху фактор-пръстена A/I съвпада с хомоморфизма φ.*

Доказателство. Разглеждаме изображенията $\eta: A \to A/I$ и $\sigma: A/I \to B$, където $\sigma(a+I)=\varphi(a)$ за всяко $a+I$ от A/I. Тъй като A, A/I и B са адитивни абелеви групи, то от теоремата за хомоморфизмите на групи следва, че σ е изоморфизъм между адитивните групи A/I и B, при което $\sigma\eta=\varphi$. Остава да се покаже, че σ изобразява произведение на елементи от A/I в произведението на съответните им образи в B. Този факт следва от равенствата

$$\sigma[(a+I)(b+I)]=\sigma(ab+I)=\varphi(ab)=\varphi(a)\,\varphi(b)=\sigma(a+I)\,\sigma(b+I)$$

за произволни a и b от A. Теоремата е доказана.

Следствие 2. *Ако φ е хомоморфизъм на пръстена A в пръс-*

тена B и $\operatorname{Im}\varphi$ *е образът на A при φ, то фактор-пръстенът $A/\ker\varphi$ е изоморфен на подпръстена* $\operatorname{Im}\varphi$ *на пръстена B.*

Пример. Знаем, че идеали на пръстена Z на целите числа са само главните идеали $nZ=(n)$, където $n\geqq 0$. Следователно фактор-пръстени на Z са само пръстените от остатъците $Z_0=Z/(0)=Z$ и Z_n, $n\geqq 1$. По теоремата за хомоморфизмите всеки хомоморфен образ на Z е изоморфен или на Z, или на някой от пръстените Z_n $(n\geqq 1)$.

Задача. Да се докаже, че пръстените Z_n и Z_m са неизоморфни при $n\neq m$.

§ 6. Директни суми на пръстени и идеали

Нека $A_1, A_2, \ldots, A_n$ са n (не обезателно различни) пръстени и A е множеството от всички наредени n-торки от вида $(a_1, a_2, \ldots, a_n)$, където $a_i \in A_i$ $(i=1, 2, \ldots, n)$. Две n-торки са равни тогава и само тогава, когато съвпадат съответните им компоненти. За всеки два елемента $a=(a_1, a_2, \ldots, a_n)$ и $b=(b_1, b_2, \ldots, b_n)$ от множеството A дефинираме сума

$$a+b=(a_1+b_1, a_2+b_2, \ldots, a_n+b_n) \tag{1}$$

и произведение

$$ab=(a_1b_1, a_2b_2, \ldots, a_nb_n). \tag{2}$$

Не е трудно да се провери, че по отношение на така въведените операции множеството A е пръстен.

Действително от определението (1) и (2) на сума и произведение в A следва, че операциите събиране и умножение в A са асоциативни; събирането е комутативно; нулев елемент в A е наредената n-торка $o=(o_1, o_2, \ldots, o_n)$, където с o_i сме означили нулевия елемент на пръстена A_i $(i=1, 2, \ldots, n)$; противоположен елемент на елемента $a=(a_1, a_2, \ldots, a_n)$ е наредената n-торка $-a=(-a_1, -a_2, \ldots, -a_n)$. Осен това за всеки три елемента a, b, c от A непосредствено се проверяват равенствата

$$(a+b)c=ac+bc, \quad c(a+b)=ca+cb,$$

т. е. двете операции в A са свързани с дистрибутивните закони.

Така полученият пръстен A се нарича *директна сума* на пръстените $A_1, A_2, \ldots, A_n$ и се означава с

$$A=A_1\oplus A_2\oplus \ldots \oplus A_n=\sum_{i=1}^{n}\oplus A_i .$$

Не е трудно да се види, че директната сума $A_1\oplus A_2\oplus \ldots \oplus A_n$ е пръстен с единица тогава и само тогава, когато всеки от пръстените A_i има единица $1_i \in A_i$ $(i=1, 2, \ldots, n)$. В този случай единичният елемент на A е наредената n-торка $(1_1, 1_2, \ldots, 1_n)$.

Също лесно се вижда, че директната сума $A_1\oplus A_2\oplus \ldots \oplus A_n$

е комутативен пръстен тогава и само тогава, когато директните събираеми $A_1, \ldots, A_n$ са комутативни пръстени.

Посочената конструкция показва как с помощта на няколко, в общия случай съвършено различни пръстени може да бъде построен нов пръстен — тяхната директна сума.

Нека $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ е директна сума на пръстените $A_1, A_2, \ldots, A_n$. Да означим с φ_i изображението от A_i в A, което се определя с равенството

$$\varphi_i(a_i) = (o_1, o_2, \ldots, o_{i-1}, a_i, o_{i+1}, \ldots, o_n)$$

за всяко a_i от A_i $(i = 1, 2, \ldots, n)$. Да означим с $\overline{A}_i$ образа на A_i в A при изображението φ_i. Очевидно е, че φ_i е взаимно еднозначно изображение на A_i върху $\overline{A}_i$. Нека a_i и a_i' са два произволни елемента от A_i. Тогава

$$\varphi_i(a_i + a_i') = (o_1, \ldots, o_{i-1}, a_i + a_i', o_{i+1}, \ldots, o_n) =$$

$$= (o_1, \ldots, a_i, \ldots, o_n) + (o_1, \ldots, a_i', \ldots, o_n) = \varphi(a_i) + \varphi(a_i'),$$

$$\varphi_i(a_i\, a_i') = (o_1, \ldots, o_{i-1}, a_i\, a_i', o_{i+1}, \ldots, o_n) =$$

$$= (o_1, \ldots, a_i, \ldots, o_n)(o_1, \ldots, a_i', \ldots, o_n) = \varphi(a_i)\, \varphi(a_i').$$

Следователно $\overline{A}_i$ е подпръстен на A и φ_i е изоморфизъм на пръстена A_i върху подпръстена $\overline{A}_i$ $(i = 1, 2, \ldots, n)$.

Подпръстените $\overline{A}_i$ на A са идеали в A. Наистина ако $a \in A$ и $b = (o_1, \ldots, b_i, \ldots, o_n)$ е произволен елемент от $\overline{A}_i$, то

$$ab = (o_1, \ldots, a_i\, b_i, \ldots, o_n) \in \overline{A}_i,$$

където a_i е i-тата компонента на a.

Ако $c = (c_1, c_2, \ldots, c_n)$ е произволен елемент от A, то

$$c = (c_1, o_2, \ldots, o_n) + (o_1, c_2, \ldots, o_n) + \ldots + (o_1, o_2, \ldots, c_n) =$$

$$= \varphi_1(c_1) + \varphi_2(c_2) + \ldots + \varphi_n(c_n) = \overline{c}_1 + \overline{c}_2 + \ldots + \overline{c}_n,$$

т. е. всеки елемент от A се представя като сума на елементи съответно взети по един от идеалите $\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_n$. Не е трудно да се забележи, че това представяне на елементите от A е еднозначно определено и следователно пръстенът A е директна сума на своите идеали $\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_n$ в смисъл на следното

Определение 14. Ще казваме, че пръстенът B е директна сума на своите идеали $I_1, I_2, \ldots, I_n$, и записваме $B = I_1 \oplus I_2 \oplus \ldots \oplus I_n$, ако всеки елемент b от B се представя еднозначно във вида

$$b = b_1 + b_2 + \ldots + b_n,$$

където $b_i \in I_i$ $(i = 1, 2, \ldots, n)$.

В приложенията е удобно да се използува следната

Теорема 5. *Пръстенът B е директна сума на своите идеали $I_1, I_2, I_3, \ldots, I_n$ тогава и само тогава, когато са изпълнени условията*

(*i*). *Пръстенът B съвпада със сумата $I_1 + I_2 + \ldots + I_n$ на идеалите $I_1, I_2, \ldots, I_n$.*

(*ii*). *Сечението на всеки идеал* I_k *със сумата* $\sum_{i\neq k} I_i$ *на останалите идеали е равно на нулевия идеал, т. е.*

$$I_k \cap \left(\sum_{i\neq k} I_i\right) = (0),\ k = 1, 2, \ldots, n.$$

Доказателство. Нека B е директна сума на идеалите си $I_1, I_2, \ldots, I_n$, т. е. всеки елемент $b \in B$ по единствен начин се записва като сума

$$b = b_1 + b_2 + \ldots + b_n\ (b_k \in I_k).$$

Това означава най-напред, че пръстенът B е сума на своите идели $I_1, I_2, \ldots, I_n$, т. е. че условието (*i*) е изпълнено. Ако допуснем, че някой ненулев елемент x принадлежи на сечението

$$I_k \cap \left(\sum_{i\neq k} I_i\right)\ (1 \leqq k \leqq n), \tag{3}$$

то x ще има две различни представяния:

$$x = 0 + \ldots + 0 + x + 0 + \ldots + 0\ (x \in I_k)$$

и

$$x = x_1 + \ldots + x_{k-1} + 0 + x_{k+1} + \ldots + x_n\ (x_i \in I_i),$$

което е противоречие. Следователно изпълнено е и условието (*ii*).

Обратно, нека за пръстена B и идеалите му $I_1, I_2, \ldots, I_n$ са изпълнени условията (*i*) и (*ii*) Трябва да покажем, че представянето на всеки елемент от B като сума на елементи, съответно взети по един от $I_1, I_2, \ldots, I_n$, е единствено. Нека елементът b от B има две различни представяния

$$b = b_1 + b_2 + \ldots + b_n = c_1 + c_2 + \ldots + c_n,$$

където $b_i, c_i \in I_i$ $(i = 1, 2, \ldots, n)$. Това означава, че за някое $k\ (1 \leqq k \leqq n)$ ще имаме $b_k \neq c_k$. Тогава ненулевият елемент

$$b_k - c_k = (c_1 - b_1) + \ldots + (c_{k-1} - b_{k-1}) + (c_{k+1} - b_{k+1}) + \ldots + (c_n - b_n)$$

ще принадлежи на сечението (3), а това е невъзможно. Теоремата е доказана.

Пример. Идеалите I_1 и I_2 на пръстена $\mathbf{Z} \oplus \mathbf{Z}$, където

$$I_1 = \{(a, 0) \mid a \in \mathbf{Z}\},\ I_2 = \{(0, b) \mid b \in \mathbf{Z}\},$$

имат нулево сечение $J_1 \cap J_2 = \{(0, 0)\}$ и затова тяхната сума $I_1 + I_2$ е директна. При това $I_1 \oplus I_2 = \mathbf{Z} \oplus \mathbf{Z}$.

Задача. Ако I и J са два ненулеви идеала в пръстена $\mathbf{Z}$, то тяхната сума $I + J$ не е директна.

Задача. Ако I и J са два ненулеви идеала в пръстена $\mathbf{Z}(i)$, то тяхната сума $I + J$ не е директна.

Задача. Ако в комутативния пръстен A няма делители на нулата, то сумата на всеки два ненулеви идеала не е директна.

Следствие 3. *Нека B е директна сума на своите идеали $I_1, I_2, \ldots, I_n$, а b и c са два произволни елемента от B. Ако $b = b_1 + b_2 + \ldots + b_n$ и $c = c_1 + c_2 + \ldots + c_n$, където $b_i, c_i \in I_i$ $(i = 1, 2, \ldots, n)$, то*

$$bc = b_1c_1 + b_2c_2 + \ldots + b_nc_n.$$

Доказателство. В сила е равенството

$$bc = \left(\sum_{i=1}^{n} b_i\right)\left(\sum_{k=1}^{n} c_k\right) = \sum_{i=1}^{n}\sum_{k=1}^{n} b_i\, c_k\,.$$

Ще покажем, че $b_i\, c_k = 0$ при $i \neq k$. Наистина, тъй като I_i и I_k са идеали, то

$$b_i\, c_k \in I_i \cap I_k \subseteq I_k \cap \left(\sum_{j \neq k} I_j\right) = (0),$$

т. е. $b_i\, c_k = 0$ при $i \neq k$. Затова

$$bc = b_1c_1 + b_2c_2 + \ldots + b_nc_n.$$

Видяхме, че ако $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ е директна сума на пръстените $A_1, A_2, \ldots, A_n$, то A е директна сума на своите идеали $\overline{A_1}, \overline{A_2}, \ldots, \overline{A_n}$, които са изоморфни съответно на пръстените $A_1, A_2, \ldots, A_n$. Очевидно е, че понятието директна сума на идеали не зависи от номерацията на идеалите, а конструкцията на директна сума на пръстени е свързана с конкретната номерация на пръстените. Обаче с точност до изоморфизъм директната сума на пръстени също не зависи от реда, в който са взети пръстените. Този факт се получава непосредствено от следното

Твърдение 5. *Пръстенът B е изоморфен на директната сума $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ на пръстените $A_1, A_2, \ldots, A_n$ тогава и само тогава, когато B е директна сума на свои идеали $I_1, I_2, \ldots, I_n$, които са изоморфни съответно на пръстените $A_1, A_2, \ldots, A_n$.*

Доказателство. Нека φ е изоморфизъм на A върху B. Знаем, че A е директна сума на своите идеали $\overline{A_i}$ и $A_i \cong \overline{A_i}$ $(i = 1, 2, \ldots, n)$. Нека $I_i = \varphi(\overline{A_i})$. Тогава I_i е идеал в B, изоморфен на $\overline{A_i}$, и затова $A_i \cong I_i$. Тъй като $A = \overline{A_1} + \overline{A_2} + \ldots + \overline{A_n}$, то $B = \varphi(A) = \varphi\overline{(A_1)} + \ldots + \varphi\overline{(A_n)} = I_1 + \ldots + I_n$. Да допуснем, че $b \in I_k \cap \left(\sum_{i \neq k} I_i\right)$. Тогава $b = \varphi(a_k) = \varphi(a_1) + \ldots + \varphi(a_{k-1}) + \varphi(a_{k+1}) + \ldots + \varphi(a_n)$, където $a_i \in \overline{A_i}$ $(i = 1, 2, \ldots, n)$. Тъй като $\varphi(a_k) = \varphi(a_1 + \ldots + a_{k-1} + a_{k+1} + \ldots + a_n)$ и φ е изоморфизъм, то $a_k = a_1 + \ldots + a_{k-1} + a_{k+1} + \ldots$

$+a_n \in \overline{A_k} \cap \left(\sum_{i \neq k} \overline{A_i}\right)$, т. е. $a_k = 0$ и затова $b = \varphi(a_k) = \varphi(0) = 0$. Полу чихме, че $I_k \cap \left(\sum_{i \neq k} I_i\right) = (0)$ за $k = 1, 2, \ldots, n$. По теорема 5 пръстенът B е директна сума на своите идеали $I_1, I_2, \ldots, I_n$.

Обратно, нека $B = I_1 \oplus I_2 \oplus \ldots \oplus I_n$ и $A_i \cong I_i$ $(i = 1, 2, \ldots, n)$. Нека $\varphi_i : A_i \to I_i$ е изоморфизъм на A_i върху I_i. Всеки елемент a от A има вида $a = (a_1, a_2, \ldots, a_n)$, $a_i \in A_i$. Да означим с φ изображението от A в B, което се определя с равенството

$$\varphi(a) = \varphi_1(a_1) + \varphi_2(a_2) + \ldots + \varphi_n(a_n).$$

Не е трудно да се забележи, че φ е изоморфизъм на A върху пръстена B. Твърдението е доказано.

Следствие 4. *Нека $A_1, A_2, \ldots, A_n$ са произволни пръстени. Ако $i_1, i_2, \ldots, i_n$ е произволна пермутация на числата 1, 2, ..., n, то директните суми $A_1 \oplus A_2 \oplus \ldots \oplus A_n$ и $A_{i_1} \oplus A_{i_2} \oplus \ldots \oplus A_{i_n}$ са изоморфни.* С други думи, *директната сума на пръстени с точност до изоморфизъм не зависи от реда на номериране на пръстените.*

Доказаните резултати показват, че понятията директна сума на пръстени и директна сума на идеали по същество не се разли чават. В първия случай става дума за определен тип конструира не на пръстен от отнапред дадени пръстени, а във втория слу чай — за даден пръстен, който се оказва, че може да бъде получен (с точност до изоморфизъм) чрез конструкция. Ето защо запис ваме $B = I_1 \oplus I_2 \oplus \ldots \oplus I_n$, когато пръстенът B е директна сума на своите идеали $I_1, I_2, \ldots, I_n$. Ако A е директна сума на пръстените $A_1, A_2, \ldots, A_n$, то ще отъждествяваме идеалите $\overline{A_1}, \overline{A_2}, \ldots, \overline{A_n}$ съ ответно с пръстените $A_1, A_2, \ldots, A_n$.

§ 7. Китайска теорема за остатъците

Още в древността китайските математици са умеели да нами рат цели числа x, които при делението на дадени две по две взаимно прости числа $n_1, n_2, \ldots, n_k$ да дават съответно отнапред дадени остатъци $c_1, c_2, \ldots, c_k$. По друг начин казано, те са умеели да намират цели числа x, за които разликата $x - c_i$ се съдържа в главния идеал (n_i) на пръстена Z за всяко $i = 1, 2, \ldots, k$. Сле дващата теорема е обобщение на тази задача за произволен пръс тен с единица.

Теорема 6 (китайска теорема за остатъците). *Нека A е произволен пръстен с единица и $I_1, I_2, \ldots, I_n$ са такива идеали на пръстена A, че $A = I_k + I_l$ при $k \neq l$. Тогава за всеки избор на елементите $c_1, c_2, \ldots, c_n$ от пръстена A съществува такъв елемент x от A, че разликата $x - c_i$ принадлежи на идеала I_i, за всяко $i = 1, 2, \ldots, n$.*

Доказателство. Нека $n=2$. Тъй като $A=I_1+I_2$, единицата 1 на A се записва във вида

$$1=a_1+a_2 \ (a_1 \in I_1, \ a_2 \in I_2).$$

Тогава елементът $x=c_2a_1+c_1a_2$ от A притежава необходимите свойства. Наистина

$$x-c_1=c_2a_1+c_1(a_2-1)=c_2a_1-c_1a_1 \in I_1,$$

а така също

$$x-c_2=c_2(a_1-1)+c_1a_2=-c_2a_2+c_1a_2 \in I_2.$$

Следователно при $n=2$ теоремата е вярна.

Нека $n>2$. Тъй като

$$A=I_1+I_i \ (i=2, 3, \ldots, n),$$

то $1=a_i+b_i$, при което $a_2, a_3, \ldots, a_n$ са елементи от I_1, а $b_2, b_3, \ldots, b_n$ са съответно от $I_2, I_3, \ldots, I_n$. Тогава

$$1=(a_2+b_2)(a_3+b_3)\ldots(a_n+b_n)=b_2b_3\ldots b_n+a,$$

където a е сума от произведения на елементи, поне един от които е обезателно някое $a_i \in I_1 \ (2 \leqq i \leqq n)$. Следователно елементът a принадлежи на идеала I_1, а произведението $b_2b_3\ldots b_n$ се съдържа в сечението $\bigcap_{i=2}^{n} I_i$. Затова единицата $1=b_2b_3\ldots b_n+a$ на A се съдържа в идеала $I_1+\bigcap_{i=2}^{n} I_i$. Оттук следва, че A съвпада с този идеал, т. е.

$$A=I_1+\bigcap_{i=2}^{n} I_i.$$

Съгласно доказаното при $n=2$, приложено за идеалите I_1 и $\bigcap_{i=2}^{n} I_i$ и елементите 1 и 0, в пръстена A съществува такъв елемент x_1, че разликите x_1-1 и $x_1-0=x_1$ принадлежат съответно на идеалите I_1 и $\bigcap_{i=2}^{n} I_i$, т. е. елементът x_1 се съдържа в идеалите $I_2, I_3, \ldots, I_n$, а разликата x_1-1 е елемент от идеала I_1. По същия начин се намира елемент x_i, който се съдържа в идеалите $I_1, I_2, \ldots, I_{i-1}, I_{i+1}, \ldots, I_n$, а разликата x_i-1 е елемент от $I_i \ (i=2, 3, \ldots, n)$. Тогава елементът

$$x=c_1x_1+c_2x_2+\ldots+c_nx_n$$

от пръстена A притежава необходимите свойства.

Действително разликата

$$x-c_i=c_1x_1+\ldots+c_{i-1}x_{i-1}+c_i(x_i-1)+c_{i+1}x_{i+1}+\ldots+c_nx_n$$

се съдържа в идеала I_i, тъй като елементите $x_1, x_2, \ldots, x_{i-1}$ $x_{i+1}, \ldots, x_n$ са от I_i. Теоремата е доказана.

Два идеала I и J на даден пръстен A се наричат взаимно прости, ако $I+J=A$. Например ако n и m са две взаимно прости цели числа, то не е трудно да се види, че сумата на главните идеали (n) и (m) на пръстена Z съвпада със Z, т. е. идеалите (n) и (m) са взаимно прости.

Следствие 5. *Нека A е произволен пръстен с единица, а $I_1, I_2, \ldots, I_n$ са два по два взаимно прости идеала в A. Тогава факторпръстенът $A/\left(\bigcap_{i=1}^{n} I_i\right)$ е изоморфен на директната сума $A/I_1 \oplus A/I_2 \oplus \ldots \oplus A/I_n$ на факторпръстените A/I_1, A/I_2, $\ldots$, A/I_n.*

Доказателство. Нека $\varphi_i: A \to A/I_i$ е естественият хоморфизъм на пръстена A върху неговия фактор-пръстен A/I_i. Дефинираме изображението φ на пръстена A в пръстена $S=A/I_1 \oplus A/I_2 \oplus \ldots \oplus A/I_n$ с равенството

$$\varphi(a)=(\varphi_1(a), \varphi_2(a), \ldots, \varphi_n(a))$$

за всяко $a \in A$.

За да установим верността на твърдението, достатъчно е да покажем, че φ е хоморфизъм на A върху S с ядро $\ker \varphi=\bigcap_{i=1}^{n} I_i$, тъй като в такъв случай тс ще следва непосредствено от теоремата за хоморфизмите.

Нека $s=(c_1+I_1, c_2+I_2, \ldots, c_n+I_n)$ е произволен елемент от пръстена S, където $c_i \in A$ $(i=1, 2, \ldots, n)$. Съгласно предната теорема съществува такъв елемент x от A, за който разликата $x-c_i$ принадлежи на I_i за всяко $i=1, 2, \ldots, n$. Това означава, че $x+I_i = c_i+I_i$, т. е.

$$\varphi_i(x)=x+I_i=c_i+I_i=\varphi_i(c_i) \quad (i=1, 2, \ldots, n).$$

Тогава

$$\varphi(x)=(\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x))=(c_1+I_1, c_2+I_2, \ldots, c_n+I_n)=s.$$

Следователно φ е изображение на A върху пръстена S. От друга страна,

$$\varphi(a+b)=(\varphi_1(a+b), \varphi_2(a+b), \ldots, \varphi_n(a+b))=$$

$$=(\varphi_1(a)+\varphi_1(b), \varphi_2(a)+\varphi_2(b), \ldots, \varphi_n(a)+\varphi_n(b))=$$

$$=(\varphi_1(a), \varphi_2(a), \ldots, \varphi_n(a))+(\varphi_1(b), \varphi_2(b), \ldots \varphi_n(b))=$$

$$=\varphi(a)+\varphi(b).$$

По същия начин се проверява, че

$$\varphi(ab)=\varphi(a)\varphi(b)$$

и следователно φ е хоморфизъм на пръстена A върху пръстена S.

За да намерим ядрото $\ker \varphi$, ще отбележим, че нулата 0 на пръстена S е $(I_1, I_2, \ldots, I_n)$. Елементът x от пръстена A принадлежи на ядрото $\ker \varphi$ тогава и само тогава, когато $\varphi(x)=(x+I_1, x+I_2, \ldots, x+I_n)=(I_1, I_2, \ldots, I_n)=0$, т. е. точно тогава, когато $x \in I_i$ $(i=1, 2, \ldots, n)$, което е еквивалентно с условието $x \in \bigcap_{i=1}^{n} I_i$. Следователно $\ker \varphi = \bigcap_{i=1}^{n} I_i$. От теоремата за хомоморфизмите получаваме, че

$$A/\left(\bigcap_{i=1}^{n} I_i\right) \cong S,$$

с което следствието е доказано.

Следствие 6. *Нека A е произволен пръстен с единица и $I_1, I_2, \ldots, I_n$ са два по два взаимно прости идеала на A. Ако сечението $\bigcap_{i=1}^{n} I_i$ съвпада с нулевия идеал (0) на A, то пръстенът A е изоморфен на директната сума $A/I_1 \oplus A/I_2 \oplus \ldots \oplus A/I_n$ на фактор-пръстените $A/I_1, A/I_2, \ldots, A/I_n$.*

Действително фактор-пръстенът на A по неговия нулев идеал е изоморфен на A и остава да се приложи предишното твърдение.

§ 8. Полета. Характеристика на поле. Линейна алгебра над произволно поле

Важен клас от комутативни пръстени с единица е класът който ще разгледаме в настоящия параграф.

Определение 15. Комутативният пръстен P с единица ще наричаме поле, ако единицата не съвпада с нулевия елемент на P и всеки ненулев елемент на P е обратим, т. е. P е поле, ако мултипликативната му група P^* съвпада с подмножеството $P \setminus \{0\}$ от ненулевите елементи на P.

Примери

1. Пръстените $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ са полета.

2. Множеството $\mathbf{Q}(i)$ от всички комплексни числа $a+bi$ с произволни рационални a и b е поле. Това поле се нарича поле на гаусовите числа.

3. Множеството $\mathbf{Q}(\sqrt{2})$ на реалните числа от вида $a+b\sqrt{2}$ с произволни рационални a и b е поле.

4. Множеството от два елемента, които ще означим с 0 и 1, е поле при следното дефиниране на операциите събиране и умножение:

$$0+0=1+1=0;\ 1+0=0+1=1;$$
$$0 \cdot 0=0 \cdot 1=1 \cdot 0=0;\ 1 \cdot 1=1.$$

5. Множеството от всички матрици от вида

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad (a, b \in \mathbf{R})$$

е поле по отношение на обикновените операции събиране и умножение на матрици.

Задача. Докажете, че полето C на комплексните числа е изоморфно на полето от пример 5.

Задача. Да се докаже, че следните пръстени не са полета: пръстенът $\mathbf{Z}$, пръстенът, който се състои от един-единствен нулев елемент, пръстените $\mathbf{Z}(i)$, $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$, $\mathbf{C}[x]$, $\mathbf{Z} \oplus \mathbf{Z}$, $F[0, 1]$.

Твърдение 6. *Полетата не съдържат делители на нулата и следователно в тях е в сила законът за съкращаване на ненулеви елементи.*

Наистина, ако $a \neq 0$ и $ab = 0$, като умножим двете страни на това равенство с a^{-1}, ще получим $b = 0$. Втората част на твърдението следва от предложение 4.

Теорема 7. *Всеки краен комутативен пръстен без делители на нулата, който съдържа поне два елемента, е поле.*

Доказателство. Нека A е комутативен пръстен без делители на нулата с n елемента и $n > 1$. Да вземем произволен не нулев елемент a от A и да разгледаме подмножеството Aa от всички елементи на A от вида ba $(b \in A)$, т. е.

$$Aa = \{ba \mid b \in A\}.$$

Тъй като A не съдържа делители на нулата, то всички елементи на подмножеството Aa са различни, тъй като от $x_1 a = x_2 a$ $(x_1, x_2 \in A)$ следва, че $x_1 = x_2$. Затова A и Aa съдържат по равен брой елементи. Оттук следва, че $A = Aa$. Понеже $a \in A = Aa$, то A съдържа такъв елемент e, че $a = ea$. Ако b е произволен елемент от A, то $ba = bea$ и съгласно твърдение 6 заключаваме, че $b = be$, т. е. e е единичен елемент на A. Но e се съдържа и в подмножеството Aa. Затова съществува такъв елемент $c \in A$, че $e = ca$. С това показахме, че A е пръстен с единица и всеки негов ненулев елемент е обратим, т. е. A е поле. Теоремата е доказана.

В произволно поле P може да въведем частно $\frac{b}{a}$ при $a \neq 0$. По определение полагаме $\frac{b}{a} = ba^{-1}$. Лесно се доказва, че в полето P се запазват всички правила за оперирane с дроби:

1) $\frac{a}{b} = \frac{c}{d}$ тогава и само тогава, когато $ad = bc$;

2) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$;

3) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$;

4) $\frac{-a}{b} = -\frac{a}{b} = \frac{a}{-b}$.

Нека P е произволно поле, а e е неговият единичен елемент.

Ако всички цели кратни на единицата на полето P са различни елементи на полето P, т. е. $me \neq ne$ при $m \neq n$ ($m, n \in Z$), казваме, че полето P има *характеристика нула*. Ако обаче съществуват такива цели числа m и n, че $m > n$, но в P е в сила равенството $me = ne$, то $(m-n)e = 0$ и следователно в P съществува такова положително кратно на единицата, което е равно на нула. В този случай P се нарича *поле с крайна характеристика* p, ако p е най-малкото естествено число, за което $pe = 0$.

Примери

1. Всички числови полета са полета с характеристика нула. Такива полета са например $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$ и т. н.

2. Всички крайни полета са очевидно с крайна характеристика. Например полето от по-горе разгледания пример 4 има характеристика 2. Не е трудно да се провери, че фактор-пръстените Z_2, Z_3 и Z_5 (виж примера от § 4), т. е. класовете остатъци по модул 2, 3 и 5, са полета съответно с характеристики 2, 3 и 5. Изобщо, ако p е просто число, по-нататък ще докажем, че *фактор-пръстенът* Z_p *е поле с характеристика* p.

Съществуват и безкрайни полета, които имат крайна характеристика.

Твърдение 7. *Ако полето* P *има крайна характеристика* p, *числото* p *е просто.*

Доказателство. Да допуснем, че числото p е съставно. Тогава $p = st$ ($1 < s < p$, $1 < t < p$) и $0 = pe = (st)e = (se).(te)$, където последното равенство следва от формула (1) и § 2. Понеже в полето няма делители на нулата, то $se = 0$ или $te = 0$, което противоречи на определението на характеристиката.

Твърдение 8. *Ако характеристиката на полето* P *е равна на* p, *за всеки елемент* a *от това поле е в сила равенството* $pa = 0$. *Ако обаче* P *е поле с характеристика* 0 *и* $a \in P$, $a \neq 0$, *а* n *е цяло число, от* $n \neq 0$ *и* $a \neq 0$ *следва* $na \neq 0$.

Доказателство. В първия случай, като приложим формула (7) на § 1, получаваме, че

$$pa = p(ea) = (pe)a = 0 \,.\, a = 0.$$

Ако P има характеристика 0, от равенствата

$$na = n(ea) = (ne)a = 0 = 0 \,.\, a \quad (a \neq 0)$$

следва, че $ne = 0$, което е възможно само при $n = 0$.

Полетата са пръстени, които по свойствата си са най-близки до числовите пръстени $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$. Това особено силно се изразява в линейната алгебра — много от теоремите на тази област на алгебрата остават верни и за случая, когато основното поле е произволно. При това доказателствата в този случай почти дословно повтарят тези в случая, когато основното поле е полето R на реалните числа. Накратко ще споменем някои от твърденията, които остават в сила за произволното поле P (виж. [14]):

1) метода на Гаус за решаване на системи линейни уравнения;

2) теорията на детерминантите;

3) правилото на Крамер;

4) теорията на n-мерните векторни пространства (линейна зависимост на вектори, ранг на система вектори и т. н.);

5) теоремата за ранга на матрица и общата теория за системите линейни уравнения;

6) резултатите за алгебрата на матриците;

7) определението на линейно пространство, теорията на линейните пространства и техните линейни преобразувания.

Трябва да отбележим само, че известното доказателство на твърдението, че една детерминанта е равна на нула, ако два нейни реда са равни, не е приложимо, когато характеристиката на основното поле P е равна на две, въпреки че твърдението е вярно и в този случай. Освен това всяка неопределена система линейни уравнения над полето P има краен брой решения, ако P е крайно, и безкрайно много решения — в противоположния случай.

§ 9. Полиноми на една променлива над комутативен пръстен

Понятието полином с числови коефициенти на една променлива лесно и естествено се обобщава с въвеждането на полиноми на една променлива с коефициенти от произволен пръстен A. По-нататък за простота на изложението ще предполагаме, че A е комутативен пръстен с единица 1.

Да допуснем, че A е подпръстен на комутативния пръстен B и единицата на A е единица и на пръстена B. Тъй като сечение на подпръстени на B е подпръстен на B (докажете това!), то за всяко подмножество Y на B има най-малък подпръстен на B, който съдържа подмножество Y. Този подпръстен е сечението на всички подпръстени на B, които съдържат Y, и за него се казва, че е подпръстенът на B, породен от подмножеството Y. В частния случай, когато Y се състои от елементите на подпръстена A и един фиксиран елемент b от B, минималният подпръстен, породен от A и b, се означава с $A[b]$. По този начин $A[b]$ е минималният подпръстен на B, който съдържа A и елемента b. Ако $a_0, a_1, \ldots, a_n$ $(n \geqq 0)$ са елементи от A, ясно е, че елементът $a_0+a_1b+a_2b^2+\ldots+a_nb^n$ се съдържа в $A[b]$. Подмножеството от всички елементи на B, които могат да се запишат по този начин, съдържа A и елемента $b=0+1\,.\,b$. Тъй като сума, разлика и произведение на елементи от това подмножество се записват също във вида $a_0+a_1b+\ldots+a_nb^n$ за подходящи $a_0, a_1, \ldots, a_n$ от A и $n \geqq 0$, това подмножество е подпръстен на B, който съдържа A и b и който се съдържа в $A[b]$. Но $A[b]$ е минималният подпръстен на B със свойството да съдържа A и b и затова $A[b]$ съвпада с подмножеството от елементите на B от разглеждания вид, т. е.

$$A[b]=\{a_0+a_1b+\ldots+a_nb^n \mid a_i \in A,\ n=0,\ 1,\ 2,\ \ldots\}.$$

Ясно е, че нулевият елемент 0 на B за всяко неотрицателно цяло число n се записва във вида $0=0+0.b+\ldots+0.b^n$. Ако това е единственият начин за записване на нулевия елемент като елемент на $A[b]$, то за b казваме, че е *трансцендентен елемент* над пръстена A. Когато b е трансцендентен над пръстена A, пръстенът $A[b]$ се нарича пръстен на полиномите на елемента b над A, а неговите елементи — полиноми на b с коефициенти от A. В този случай всеки полином $f\in A[b]$ на b се записва във вида $f=a_0+a_1b+\ldots+a_nb^n$ $(n\geqq 0,\ a_i\in A)$ и този запис е еднозначен в следния смисъл: ако $f=\bar{a}_0+\bar{a}_1b+\ldots+\bar{a}_mb^m$ $(\bar{a}_i\in A)$ е друг запис на f като полином на b, то в сила са следните две условия:

1) ако $a_i\neq 0$, то $m\geqq i$ и $a_i=\bar{a}_i$;

2) ако $\bar{a}_j\neq 0$, то $n\geqq j$ и $a_j=\bar{a}_j$.

Наистина при $n\geqq m$ от равенството $a_0+a_1b+\ldots+a_nb^n=\bar{a}_0+\bar{a}_1b+\ldots+\bar{a}_mb^m$ следва $0=(a_0-\bar{a}_0)+(a_1-\bar{a}_1)b+\ldots+(a_m-\bar{a}_m)b^m+a_{m+1}b^m+\ldots+a_nb^n$. Понеже b по предположение е трансцендентен над A, от последното равенство следват равенствата $a_0-\bar{a}_0=0,\ a_1-\bar{a}_1=0,\ \ldots,\ a_m-\bar{a}_m=0,\ a_{m+1}=a_{m+2}=\ldots=a_n=0$, т. е. условие 1) е в сила. По същия начин се вижда, че условие 2) е в сила, когато $n\leqq m$.

Не е трудно да се види, че пръстенът на полиномите над A на един трансцендентен над A елемент b с точност до изоморфизъм не зависи от конкретния елемент b. Действително ако A е подпръстен и на комутативния подпръстен D, единицата на A е единица и на D, а $d\in D$ е трансцендентен елемент над A, то съществува такъв изоморфизъм $\varphi: A[b]\to A[d]$ на $A[b]$ върху $A[d]$, че $\varphi(a)=a$ за всяко $a\in A$ и $\varphi(b)=d$. За всеки елемент $f=a_0+a_1b+\ldots+a_nb^n$ от $A[b]$ изоморфизмът φ се определя с равенството $\varphi(f)=a_0+a_1d+\ldots+a_nd^n$. Проверката, че φ е коректно определено изображение и е изоморфизъм на пръстена $A[b]$ върху пръстена $A[d]$, е проста и се извършва непосредствено.

Посочената независимост на пръстена на полиномите над A от конкретния трансцендентен елемент ни дава възможност с x да означим кой да е трансценденген елемент над A, а с $A[x]$ — пръстена на полиномите на x над A. Често за x се казва, че е променлива, като се подразбира, че x може да бъде произволен трансцендентен елемент над пръстена A. За $A[x]$ се казва, че е пръстен на полиномите на една променлива x над A.

Ако

$$f(x)=a_0+a_1x+\ldots+a_nx^n\ (a_i\in A) \tag{1}$$

е полином на x на A, то елементите $a_0,\ a_1,\ \ldots,\ a_n$ се наричат *коефициенти* на $f(x)$. Ако a_k е последният ненулев коефициент на $f(x)$, то a_k се нарича *старши коефициент*, a_kx^k — *старши член* на $f(x)$, а k — *степен* на $f(x)$.

Под степен на нулевия полином разбираме символа $-\infty$, а под старши коефициент и старши член — елемента 0.

Ако

(2) $$g(x)=b_0+b_1x+\ldots+b_mx^m \quad (b_i\in A)$$
е също полином на x над A, то $f(x)g(x)=c_0+c_1x+\ldots+c_{n+m}x^{n+m}$, където

$$c_k=\sum_{i+j=k} a_ib_j \quad (k=0, 1, \ldots, n+m).$$

Тъй като полиномът не се изменя при прибавяне на събираеми от вида $0x^t$, можем да считаме, че

$$f(x)=\sum_{i=0}^{r} a_i x^i, \quad g(x)=\sum_{i=0}^{r} b_i x^i,$$

където $r=\max\{m, n\}$, $a_i=0$ при $i>n$ и $b_j=0$ при $j>m$. Тогава за сумата $f(x)+g(x)$ имаме

$$f(x)+g(x)=\sum_{i=0}^{r}(a_i+b_i)x^i.$$

Често вместо записа (1) на полинома $f(x)$ се използува и записът с обратна номерация на коефициентите, т. е.

(1′) $$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n.$$

Няма да приведем доказателствата на следните три важни твърдения, тъй като те са напълно аналогични на доказателствата на съответните твърдения за полиноми с числови коефициенти.

Теорема 8. *Нека A е област на цялостност. Ако $f(x)$ и $g(x)$ са два полинома на x с коефициенти от A, то*

$$\deg[f(x)+g(x)]\leqq\max\{\deg f(x), \deg g(x)\},$$

$$\deg[f(x)g(x)]=\deg f(x)+\deg g(x),$$

Следствие 7. *Ако A е област на цялостност, то пръстенът $A[x]$ е също област на цялостност.*

Теорема 9. *Нека P е произволно поле, а $f(x)$ и $g(x)$ са полиноми с коефициенти от P, при което $g(x)$ е ненулев полином. Тогава съществуват такива единствени полиноми $q(x)$ и $r(x)$ с коефициенти от P, че*

$$f(x)=q(x)g(x)+r(x), \quad \deg r(x)<\deg g(x).$$

В определението на пръстена на полиномите над комутативния пръстен A се изисква съществуване на трансцендентен елемент над A. Да се занимаем сега с въпроса за съществуване на такъв елемент. За всеки комутативен пръстен A с единица ще покажем конструктивно, че съществува пръстенът $A[x]$ на полиномите над A на една променлива x, т. е. ще покажем, че съществува трансцендентен елемент над A.

Да означим с G множеството от всички редици $(a_0, a_1, a_2, \ldots)$,

от елементи на A, в които само краен брой компоненти a_i са различни от нулевия елемент на A. Ако $f=(a_0, a_1, a_2, \ldots)$ и $g=(b_0, b_1, b_2, \ldots)$ са два елемента от G, то по определение полагаме

$$f+g=(a_0+b_0, a_1+b_1, a_2+b_2, \ldots),$$

$$fg=(c_0, c_1, c_2, \ldots),$$

където

$$c_k=\sum_{i+j=k} a_i\, b_j \quad (k=0, 1, 2, \ldots).$$

Тъй като краен брой от компонентите на f и g са различни от нула, само краен брой и от компонентите на $f+g$ и fg са различни от нула, т. е. $f+g$ и fg са елементи на G. С непосредствена проверка се установява, че спрямо въведените операции събиране и умножение G е комутативен пръстен. Нулев елемент 0 на този пръстен е редицата $(0, 0, 0, \ldots)$ с нулеви компоненти, а единичен елемент с редицата $(1, 0, 0, \ldots)$. Изображението $\sigma: A\to G$, определено с равенството $\sigma(a)=(a, 0, 0, \ldots)$ за всяко $a\in A$, е хомоморфизъм на пръстена A в пръстена G, който изобразява различни елементи на A в различни елементи на G. Следователно A е изоморфен на подпръстена на G, съставен от всички редици, компонентите на които с номер, по-голям или равен на 1, са нулеви. Затова можем да отъждествим всеки елемент a на A с неговия образ $(a, 0, 0, \ldots)$ при σ и да считаме, че A е подпръстен на G. Очевидно единицата $1=(1, 0, 0, \ldots)$ на A е единица и на G. Ако $a\in A$, а $f=(a_0, a_1, a_2, \ldots)$ е произволен елемент на G, то от определението на произведение на елементи на G следва, че $af=(a, 0, 0, \ldots)(a_0, a_1, a_2, \ldots)=(aa_0, aa_1\ aa_2, \ldots)$, т. е. елементът a от A умножава елемента f от G, като с a се умножава всяка компонента на f. Да означим с x елемента $(0, 1, 0, \ldots)$. За всяко естествено число n имаме $x^n=(0, 0, \ldots, 0, 1, 0, \ldots)$, където всички компоненти са нулеви освен тази с номер n, която е равна на единица. Полагаме $x^0=(1, 0, 0, \ldots)=1$. Елементът x от G е трансцендентен над A. Наистина ако $a_0+a_1x+\ldots+a_nx^n=0$, където $a_i\in A$, то лявата страна на това равенство е редицата $(a_0, a_1, \ldots, a_n, 0, \ldots)$ и тя е равна на нулевия елемент $0=(0, 0, \ldots)$ на G тогава и само тогава, когато $a_0=a_1=\ldots=a_n=0$. Следователно подпръстенът $A[x]$ на G е пръстенът на полиномите на елемента x над пръстена A. Освен това не е трудно да се види, че $G=A[x]$. С това доказателството за съществуването на пръстена на полиномите на една променлива над комутативния пръстен A е завършено.

Формално алгебричното въвеждане на полиномите над произволен комутативен пръстен A с единица, което изложихме, тук по необходимост се налага поради невъзможността да използуване тяхното теоретико-функционално въвеждане. За числови пръс-

тени двата начина са еквивалентни, но за произволни комутативни пръстени такава еквивалентност не съществува. Действително нека $f(x)=x^2+1$ и $g(x)=x+1$ са полиноми над полето Z_2. Полиномите $f(x)$ и $g(x)$ са различни от формално алгебрично гледище, тъй като съответните им коефициенти не са равни. Но $f(x)$ и $g(x)$ съвпадат като функции, определени в Z_2, защото $f(0)=g(0)=1$ и $f(1)=g(1)=0$. За безкрайни полета обаче бихме могли да въведем полиномите и теоретико-функционално, т. е. да ги дефинираме като функции от специален вид и да ги отъждествяваме като функции (без да използуваме коефициентите). Това твърдение се съдържа в следната

Теорема 10. *Полиномите $f(x)$ и $g(x)$ с коефициенти от безкрайното поле P са равни тогава и само тогава, когато $f(x)$ и $g(x)$ съвпадат като функции, дефинирани в P.*

Доказателство. Нека

$$f(x)=\sum_{i=0}^{n} a_i\, x^i, \quad g(x)=\sum_{i=0}^{n} b_i\, x^i.$$

Ясно е, че ако полиномите $f(x)$ и $g(x)$ имат еднакви коефициенти, те съвпадат и като функции.

Обратно, нека полиномите $f(x)$ и $g(x)$ са равни като функции, т. е. $f(\alpha)=g(\alpha)$ за всяко $\alpha \in P$. Тъй като P е безкрайно поле, можем да подберем в него $n+1$ различни елемента $\alpha_0, \alpha_1, \ldots, \alpha_n$ $(\alpha_i \neq \alpha_j,\ i \neq j)$. Разглеждаме системата

$$\begin{cases} x_0+\alpha_0 x_1+\alpha_0^2 x_2+\ldots+\alpha_0^n x_n=f(\alpha_0)=g(\alpha_0) \\ x_0+\alpha_1 x_1+\alpha_1^2 x_2+\ldots+\alpha_1^n x_n=f(\alpha_1)=g(\alpha_1) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_0+\alpha_n x_1+\alpha_n^2 x_2+\ldots+\alpha_n^n x_n=f(\alpha_n)=g(\alpha_n) \end{cases}$$

от $n+1$ линейни уравнения с $n+1$ неизвестни $x_0, x_1, \ldots, x_n$. Тази система има едно-единствено решение, понеже за детерминантата ѝ като детерминанта на Вандермонд имаме

$$\begin{vmatrix} 1 & \alpha_0 & \alpha_0^2 & \ldots & \alpha_0^n \\ 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^n \end{vmatrix} = \prod_{i>j} (\alpha_i-\alpha_j) \neq 0.$$

Но $(a_0, a_1, \ldots, a_n)$ и $(b_0, b_1, \ldots, b_n)$ са решения на горната система и затова те съвпадат, т. е. $a_0=b_0$, $a_1=b_1$, $\ldots$, $a_n=b_n$. Следователно двата полинома $f(x)$ и $g(x)$ съвпадат. Теоремата е доказана.

§ 10. Поле от частни

Нека P е произволно поле. Тъй като P е комутативен пръстен без делители на нулата, всеки негов подпръстен е комутативен и е без делители на нулата. Интересно е да отговорим на следния въпрос: ако A е комутативен пръстен без делители на нулата, съществува ли поле P, в което A да бъде подпръстен или A да бъде изоморфен на някой подпръстен на полето P?. Ще покажем, че този въпрос има положителен отговор.

Нека A е ненулев комутативеи пръстен без делители на нулата и

$$A_1=\{(a, b)\,|\,a,\quad b\in A,\ b\neq 0\}$$

е множеството от всички наредени двойки (a, b) с елементи a и b от пръстена A, където $b\neq 0$. По-нататък, без да отбелязваме винаги, ще разглеждаме само такива наредени двойки (a, b), за които $a, b\in A$ и $b\neq 0$. Ще казваме, че две наредени двойки (a, b) и (c, d) са *сравними* помежду си, което ще записваме $(a, b)\equiv(c, d)$ тогава и само тогава, когато $ad=bc$. Веднага се проверява, че релацията „$\equiv$“ е релация на еквивалентност, т. е.

1) $(a, b)\equiv(a, b)$;
2) ако $(a, b)\equiv(c, d)$, то $(c, d)\equiv(a, b)$;
3) ако $(a, b)\equiv(c, d)$ и $(c, d)\equiv(e, f)$, то $(a, b)\equiv(e, f)$.

За да докажем например свойство 3), достатъчно е да забележим, че първите две релации в 3) са еквивалентни съответно на равенствата $ad=bc$ и $cf=de$. Като умножим първото равенство с елемента f, а второто — с елемента b, ще получим $(ad)f=(bc)f=b(cf)=b(de)$, т. е. $(ad)f=b(de)$. Тъй като A не съдържа делители на нулата и $d\neq 0$, то $af=be$ и затова $(a, b)\equiv(e, f)$.

Известно е, че всяка релация на еквивалентност, която действува в дадено множество, разлага това множество на непресичащи се класове от еквивалентни помежду си елементи. Нека P е множеството на всички класове, на които се разбива множеството A_1 през релацията „$\equiv$“. Да означим с $[a, b]$ класа от всички наредени двойки от A_1, които са сравними с наредената двойка (a, b), т. е.

$$[a, b]=\{(x, y)\,|\,(x, y)\equiv(a, b)\}.$$

Както обикновено, наредената двойка (a, b) ще наричаме представител на класа $[a, b]$. Ще докажем, че в P могат да бъдат определени операции събиране и умножение, така че спрямо тях то да бъде поле. За целта да положим

$$[a, b]+[c, d]=[ad+bc, bd], \tag{1}$$

$$[a, b]\,.\,[c, d]=[ac, bd]. \tag{2}$$

Класовете в десните части на (1) и (2) съществуват, понеже $bd\neq 0$. Най-напред трябва да установим, че операциите събиране и умножение са дефинирани коректно чрез формулите (1), т. е. те не зависят от избора на представителите на отделните класове

Действително нека $[a, b]=[a_1, b_1]$ и $[c, d]=[c_1, d_1]$, т. е. $(a, b)\equiv(a_1, b_1)$ и $(c, d)\equiv(c_1, d_1)$. Необходимо е да докажем, че

$$[ad+bc,\ bd]=[a_1d_1+b_1c_1,\ b_1d_1], \tag{1}$$

$$[ac,\ bd]=[a_1c_1,\ b_1d_1]. \tag{2}$$

От $(a, b)\equiv(a_1, b_1)$ и $(c, d)\equiv(c_1, d_1)$ следват равенствата

$$ab_1=a_1b,\ cd_1=c_1d. \tag{3}$$

Тогава равенството (1) е изпълнено, защото са сравними съответните им представители, т. е.

$$(ad+bc)b_1d_1=(a_1d_1+b_1c_1)bd.$$

Наистина

$$(ad+bc)\,b_1d_1=(ab_1)\,dd_1+(bb_1)\,cd_1=$$
$$=(a_1b)dd_1+(bb_1)c_1d=(a_1d_1+b_1c_1)bd.$$

където при второто равенство са използувани равенствата (3).

Аналогично равенството (2) е изпълнено, защото

$$acb_1d_1=(ab_1)cd_1=(a_1b)c_1d=(bd)a_1c_1,$$

т. е. сравними са наредените двойки (ac, bd) и (a_1c_1, b_1d_1).

Твърдение 9. *Множеството P е поле относно определените чрез* (1) *и* (2) *операции събиране и умножение.*

Доказателство. Лесно се проверява, че събирането и умножението в P са комутативни и асоциативни. Освен това в сила е дистрибутивният закон

$$([a, b]+[c, d])[e, f]=[a, b][e, f]+[c, d][e, f],\quad b, d, f\neq 0.$$

Действително

$$([a, b]+[c, d])[e, f]=[ad+bc,\ bd][e, f]=$$
$$=[ade+bce,\ \ bdf],\ bdf\neq 0.$$

За дясната страна получаваме същия резултат:

$$[a, b][e, f]+[c, d][e, f]=[ae,\ bf]+[ce,\ df]=$$
$$=[aedf+bfcc,\ bfdf]=[ade+bce,\ bdf],$$

където в последното равенство сме използували факта, че двата класа имат еквивалентни представители.

Нулев елемент в $P(+)$ е класът $0=[0, b]$, а класът $[-a, b]$ е противоположен на $[a, b]$, т. е. $[-a, b]=-[a, b]$. Лесно се проверява, че класът $e=[a, a]$ е единичен елемент относно умножението, а обратен на $[a, b]$ при $a\neq 0$ е класът $[b, a]$, защото

$$[a, b][b, a]=[ab,\ ab]=e.$$

Твърдението е доказано.

Задача. Докажете, че $[a, -b]=-[a, b]$.

Твърдение 10. *Полето P съдържа подпръстен, който е изоморфен на пръстена A.*

Доказателство. Нека c е фиксиран ненулев елемент на A. Разглеждаме изображението $\varphi: A \to P$, което на всеки елемент a от A съпоставя класа $[ac, c]$ от P, т. е. $\varphi(a) = [ac, c]$. Не е трудно да се провери, че изображението φ е съгласувано с операциите в A и P. Действително

$$\varphi(a+b) = [(a+b)c, c] = [ac, c] + [bc, c] = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = [abc, c] = [ac, c][bc, c] = \varphi(a)\varphi(b).$$

Следователно φ е хомоморфизъм на пръстена A в полето P и затова образът $\operatorname{Im}\varphi = \varphi(A)$ на пръстена A ще бъде подпръстен на P. Но φ е и взаимно еднозначно изображение. Наистина ако $\varphi(a) = \varphi(b)$, то $[ac, c] = [bc, c]$. Последното равенство показва, че наредените двойки (ac, c) и (bc, c) са сравними, т. е. $ac^2 = bc^2$, откъдето следва, че $a = b$.

По такъв начин се убедихме, че φ е изоморфизъм между пръстена A и подпръстена $\varphi(A)$ на полето P. Твърдението е доказано.

Определение 16. Полето P се нарича *поле от частни* на пръстена A.

Като обединим резултатите от предишните две твърдения, получаваме

Теорема 11. *За всеки комутативен пръстен A без делители на нулата съществува такова поле P, което съдържа подпръстен, изоморфен на пръстена A.*

Наистина ако A е нулев пръстен. то нулевият подпръстен на всяко поле е изоморфен на A. Ако A е ненулев пръстен, то полето от частни P на пръстена A съдържа подпръстен, изоморфен на A.

Лесно се вижда, че изоморфизмът φ от доказателството на твърдение 10 не зависи от избора на ненулевия елемент $c \in A$. Ако отъждествим всеки елемент a от A със съответния му елемент $\varphi(a) = [ac, c]$ от P, т. е. ако положим $a \equiv [ac, c]$, то A може да се разглежда като подпръстен на полето P и в такъв случай сте казва, че пръстенът A е *вложен в полето* P. Тогава

$$[a, b] = [ac, c][c, bc] = [ac, c][bc, c]^{-1} = ab^{-1},$$

т. е. всеки елемент $[a, b]$ от полето P се записва във вида ab^{-1}, където $a, b \in A$ и $b \neq 0$. Например пръстенът Z на целите числа се влага в полето Q на рационалните числа и Q е поле от частни на пръстена Z. В този случай вместо класовете $[a, b]$, $a, b \in Z$ $(b \neq 0)$. се употребяват символите $\frac{a}{b}$, наречени рационални числа (дроби). Не е трудно да се съобрази, че формулите (1) и (2) съответствуват точно на правилата за събиране и умножаване на дроби. Рационалното число $\frac{a}{b}$ също представлява клас от наредени двойки, защото $\frac{a}{b} = \frac{ac}{bc}$ за всяко цяло число $c \neq 0$. По същия начин полето $Q(i)$ на гаусовите числа е поле от частни на пръстена $Z(i)$ на целите гаусови числа.

ГЛАВА VI

ОБЛАСТИ НА ГЛАВНИ ИДЕАЛИ

§ 1. Елементарни свойства на делимостта

Нека A е комутативен пръстен с единица. Ще казваме, че елементът b от A *дели* елемента a от A, ако $a=bc$, където c е също елемент от A. Ще казваме също „*a се дели* на b“ или „*b е делител* на a“, което кратко ще записваме със символа b/a и ще четем „b дели a“.

Задача. Нека A е комутативен пръстен с единица и $a, b \in A$. Докажете, че a/b тогава и само тогава, когато $(a) \supseteq (b)$.

Определение 1. Ще казваме, че елементът $a \in A$ *е асоциран* на елемента $b \in A$ (пишем $a \sim b$), ако $a=b\varepsilon$, където ε е обратим елемент в пръстена A.

Твърдение 1. *Релацията „асоцираност“ е релация на еквивалентност.*

Доказателство. Всеки елемент a може да се запише във вида $a=a.1$, т. е. $a \sim a$. Ако $a \sim b$, то $a=b\varepsilon$, където ε е обратим елемент. Но ε^{-1} е също обратим и $b=a\varepsilon^{-1}$, т. е. $b \sim a$. Ако $a \sim b$ и $b \sim c$, то $a=b\varepsilon_1$ и $b=c\varepsilon_2$, където ε_1 и ε_2 са обратими елементи. Тогава $a=c(\varepsilon_1\varepsilon_2)$ и тъй като елементът $\varepsilon_1\varepsilon_2$ е обратим, то $a \sim c$.

Теорема 1. *Елементите a и b от областта A на цялостност са асоциирани тогава и само тогава, когато a/b и b/a.*

Доказателство. Ако $a \sim b$, то и $b \sim a$, а от определението за асоциираност непосредствено следва, че a/b и b/a.

Обратно, нека a/b, b/a и $b=ad$, $a=bc$, където $c, d \in A$. Тогава $a=bc=adc$ и следователно $a(1-dc)=0$. Ако $a=0$, то $b=0$ и затова $a \sim b$. При $a \neq 0$ от равенството $a(1-dc)=0$ следва, че $1=dc$, понеже пръстенът A е без делители на нулата. Това показва, че елементите d и c са обратими и $a \sim b$. Теоремата е доказана.

Следствие 1. *Ако A е област на цялостност, то главните идеали (a) и (b) съвпадат тогава и само тогава, когато $a \sim b$.*

Действително равенството $(a)=(b)$ е изпълнено точно тогава, когато $(a) \subseteq (b)$ и $(b) \subseteq (a)$. Но тези условия са еквивалентни на условията $a \in (b)$ и $b \in (a)$, т. е. на условията b/a и a/b. Следователно равенството $(a)=(b)$ е равносилно на a/b, b/a и твърдението следва от теоремата.

Ще отбележим някои елементарни свойства на делимостта.

1) *Ако a/b и b/c, то a/c.*

Наистина от $b=ad_1$, $c=bd_2$ следва $c=ad_1d_2$, т. е. a/c.

По подобен начин се доказват и следните свойства:

2) *Ако* c/a *и* c/b, *то* $c/(a \pm b)$;

3) *Ако* b/a, *то* b/ac *за всяко* $c \in A$;

4) *Ако* ε *е обратим елемент, то* ε/a, *където* a *е произволен елемент на* A;

5) *ако* b/a *и* ε *е обратим елемент, то* $b \varepsilon/a$.

Нека a и b са два елемента на комутативния пръстен A с единица. Те имат поне един общ делител, например единицата. Ако сред общите делители на двата елемента a и b има такъв, който се дели на всички останали, този общ делител се нарича *най-голям общ делител* на елементите a и b (НОД). Най-големият общ делител невинаги съществува. Това зависи от свойствата на пръстена A и от конкретните негови елементи a и b.

Да допуснем, че елементите a и b притежават НОД. Единствен ли е този НОД? Ако d_1 и d_2 са два НОД на a и b, от определението на НОД следва, че d/d_2 и d_2/d_1. Ако пръстенът A е област на цялостност, то оттук и теорема 1, заключаваме, че $d_1 \sim d_2$.

Обратно, нека d е НОД на елементите a и b и $d_1 \sim d$, т. е. $d_1 = d\varepsilon$, където ε е обратим елемент на A. Тогава от d/a и d/b по свойство 5) следва, че d_1/a и d_1/b. Ако $c \in A$ е произволен общ делител на a и b, то c/d и по свойство 1) ще имаме c/d_1. Следователно d_1 е също НОД на a и b. Така получихме следното твърдение:

Твърдение 2. *Ако* A *е област на цялостност и* a, b *са два елемента от* A, *за които съществува НОД, то множеството от НОД на елементите* a *и* b *е пълен клас от асоциирани елементи, т. е. съвпада с множеството от всички асоциирани елементи на произволен НОД на* a *и* b.

По аналогичен начин се въвежда и понятието *най-голям общ делител* на няколко елемента $a_1, a_2, \ldots, a_n$, който се означава с НОД $(a_1, a_2, \ldots, a_n)$.

§ 2. Евклидови пръстени

Нека $Z(i)$ е пръстенът от комплексните числа от вида $a+bi$, където a и b са цели. Вече знаем, че този пръстен е област на цялостност. Ще покажем, че в този пръстен е възможно „деление с непълно частно и остатък".

Под *норма* на цялото гаусово число $z=a+bi$ $(a, b \in Z)$ ще разбираме квадрата на модула му и ще я означаваме с $N(z)$ т. е.

$$N_1(z)=|z|^2=a^2+b^2.$$

Очевидно нормата е цяло неотрицателно число, което само тогава е равно на нула, когато числото z е равно на нула. От свойствата на модулите на комплексните числа непосредствено следва равенството

$$N(zt)=N(z)\,N(t),$$

:където $z,\ t \in \mathbf{Z}(i)$.

Теорема 2. *Нека t е произволно ненулево цяло гаусово число. За всяко z от $\mathbf{Z}(i)$ съществуват поне две цели гаусови числа q и r, за които са изпълнени условията*

$$z = qt + r,\quad N(r) < N(t).$$

Доказателство. Да разгледаме комплексното число $\frac{z}{t} = a + bi$, където a и b са рационални числа. Затворените интервали $\left[a - \frac{1}{2}, a + \frac{1}{2}\right]$, $\left[b - \frac{1}{2}, b + \frac{1}{2}\right]$ имат дължина единица и затова съдържат поне по едно цяло рационално число. Нека c и d са две такива числа от $\mathbf{Z}$, че

$$a - \frac{1}{2} \leqq c \leqq a + \frac{1}{2},\ b - \frac{1}{2} \leqq d \leqq b + \frac{1}{2},$$

т. е.

$$|a - c| \leqq \frac{1}{2},\ |b - d| \leqq \frac{1}{2}.$$

Полагаме $q = c + di$, $r = z - qt$. Ясно е, че q и r принадлежат на $\mathbf{Z}(i)$ и $z = qt + r$. Освен това $\frac{r}{t} = \frac{z}{t} - q = (a - c) + (b - d)i$. Тогава $\frac{N(r)}{N(t)} = \frac{|r|^2}{|t|^2} = (a - c)^2 + (b - d)^2 \leqq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$, т. е. $N(r) < N(t)$. Теоремата е доказана.

Тук трябва да отбележим, че в общия случай целите гаусови числа q и r от доказаната теорема не са еднозначно определени. Например ако $z = 2 + 3i$ и $t = 1 + i$, то $z = (2 + i)t + 1 = 3t - 1$ и $1 = N(1) = N(-1) < N(t) = 2$. Затова тук q и r не се наричат *непълно частно и остатък* за разлика от случая с пръстените $\mathbf{Z}$ и $P[x]$, където P е поле. Това различие обаче не се отразява съществено върху основните свойства на пръстена $\mathbf{Z}(i)$. Пръстените $\mathbf{Z}$, $\mathbf{Z}(i)$ и $P[x]$ (P е поле) са едни от най-важните примери за така наречените *евклидови пръстени*.

Определение 2. Областта на цялостност A се нарича *евклидов пръстен*, ако на всеки ненулев елемент a от A е съпоставено цяло неотрицателно число $N(a)$ (норма на a) и е изпълнено следното условие: за всеки два елемента $a,\ b \in A$, където $b \neq 0$, в A съществуват такива два елемента q и r (не обезателно еднозначно определени), че

$$a = bq + r$$

и ако $r \neq 0$, то $N(r) < N(b)$.

Примери

1. Пръстенът $\mathbf{Z}$ на целите числа е евклидов — под норма на цялото число m се разбира неговата абсолютна стойност $|m|$.

2. Пръстенът $\mathbf{Z}(i)$ на целите гаусови числа е евклидов (теорема 5).

3. Пръстенът $P[x]$ на полиномите на една променлива над

полето P е евклидов, като под норма на полинома $f(x)$ се разбира неговата степен $\deg f(x)$.

4. Всяко поле P е евклидов пръстен, където нормата в P може да бъде произволна, например $N(a)=0$ за всяко $a \in P$.

Едно от най-важните свойства на евклидовите пръстени се дава от следната

Теорема 3. *Всеки два елемента a и b от евклидовия пръстен A притежават най-голям общ делител.*

Доказателство. Ако $b=0$, то НОД на a и b е равен на a.

Нека $b \neq 0$. Тогава съществуват q_1, $r_1 \in A$ такива, че $a=bq_1+r_1$, и ако $r_1 \neq 0$, то $N(r_1)<N(b)$. Когато $r_1 \neq 0$, съществуват q_2, $r_2 \in A$ такива, че $b=r_1 q_2+r_2$, и ако $r_2 \neq 0$, то $N(r_2)<N(r_1)$. Когато $r_2 \neq 0$, съществуват q_3, $r_3 \in A$ такива, че $r_1=r_2 q_3+r_3$, и ако $r_3 \neq 0$, то $N(r_3)<N(r_2)$ и т. н. Понеже в посочения процес на деление $N(b)>N(r_1)>N(r_2)>\ldots$ при $r_1 \neq 0$, $r_2 \neq 0$, ... и нормата на всеки ненулев елемент от A е цяло неотрицателно число, след краен брой стъпки ще получим $r_{n+1}=0$, т. е. $r_{n-1}=q_{n+1} r_n$. По този начин се получава следната система от равенства и неравенства:

$$
\begin{aligned}
&a=bq_1+r_1, \quad N(r_1)<N(b),\\
&b=r_1 q_2+r_2, \quad N(r_2)<N(r_1),\\
&r_1=r_2 q_3+r_3, \quad N(r_3)<N(r_2),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_k=r_{k+1} q_{k+2}+r_{k+2}, \quad N(r_{k+2})<N(r_{k+1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{n-2}=r_{n-1} q_n+r_n, \quad N(r_n)<N(r_{n-1}),\\
&r_{n-1}=r_n q_{n+1}.
\end{aligned}
$$

Ще покажем, че последният ненулев „остатък“ r_n е НОД на елементите a и b. Наистина, като проследим предните равенства от последното към първото, получаваме r_n/r_{n-1}, r_n/r_{n-2}, ..., r_n/r_1, r_n/b, r_n/a, т. е. r_n е общ делител на a и b. Обратно, ако d/a и d/b, то като проследим равенствата от първото към последното, получаваме d/r_1, d/r_2, ..., d/r_n. Затова r_n е НОД на a и b. Теоремата е доказана.

Описаният процес на последователно деление се нарича *алгоритъм на Евклид* за намиране на НОД на два елемента в евклидов пръстен.

§ 3. Области на главни идеали

Пръстенът Z на целите числа е област на цялостност, в която всеки идеал е главен. Нашата цел е да покажем до края на тази глава, че в пръстен с последните две свойства са в сила всички основни факти от теорията за делимост на целите числа.

Определение 3. Комутативният пръстен A с единица се нарича *пръстен на главни идеали*, ако всеки идеал в A е главен, т. е. ако всеки идеал в A се поражда от един свой елемент. Ако един пръстен на главни идеали е област на цялостност, той се нарича *област на главни идеали*.

Примери:

1. Пръстенът Z на целите числа е област на главни идеали.
2. Хомоморфните образи Z_n $(n \geqq 1)$ на Z са пръстени на главни идеали. При това пръстенът Z_n на остатъците по модул n $(n > 1)$ е област на главни идеали тогава и само тогава, когато n е просто число.
2. Всяко поле е област на главни идеали.

Задача. Докажете, че фактор-пръстен на пръстен на главни идеали е също пръстен на главни идеали.

Твърдение 3. *Всеки евклидов пръстен е област на главни идеали.*

Доказателство. Нека A е евклидов пръстен. Тогава A е област на цялостност и трябва да покажем само, че в A всеки идеал е главен. Нека I е произволен идеал на A. Ако I е нулевият идеал, то I е главен и се поражда от нулевия елемент на A, т. е. $I = (0)$.

Нека $I \neq 0$. Нормите на ненулевите елементи от I образуват подмножество на множеството от всички неотрицателни цели числа. Затова в I има поне един ненулев елемент a с най-малка норма $N(a)$. Да разгледаме главния идеал (a), породен от a. Тъй като всеки елемент x от (a) има вида $x = ra$ $(r \in A$ и $a \in I)$, в сила е включването $(a) \subseteq I$. Нека $y \in I$. Понеже A е евклидов пръстен, съществуват такива q, $r \in A$, че $y = aq + r$, и ако $r \neq 0$, то $N(r) < N(a)$. Елементът $r = y - aq$ се съдържа в идеала I. Ако допуснем, че $r \neq 0$, то r се оказва ненулев елемент в I, който има по-малка норма от нормата на a, което е невъзможно. Следователно $r = 0$ и $y = qa \in (a)$. Така получихме и включването $I \subseteq (a)$. Двете включвания показват, че I съвпада с главния идеал, породен от a. Твърдението е доказано.

Нека A е комутативен пръстен с единица, а $a_1, a_2, \ldots, a_n$ са елементи от A. С $(a_1, a_2, \ldots, a_n)$ ще означаваме сумата $(a_1) + \ldots + (a_n)$ на главните идеали, породени от $a_1, a_2, \ldots, a_n$. Очевидно, идеалът $(a_1, a_2, \ldots, a_n)$ се състои от всички елементи на A от вида $r_1a_1 + r_2a_2 + \ldots + r_na_n$, където $r_1, r_2, \ldots, r_n \in A$. За този идеал се казва, че е *крайно породен*, а $a_1, a_2, \ldots, a_n$ се наричат пораждащи или образуващи елементи на идеала $(a_1, a_2, \ldots, a_n)$.

Теорема 4. *Ако A е комутативен пръстен с единица, то следните две условия са еквивалентни:*

1) *всеки идеал на A е крайно породен;*
2) *за всяка верига от идеали на A от вида*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots \tag{1}$$

съществува такова естествено число m, че $I_m = I_{m+1} = I_{m+2} = \ldots$.

Доказателство. Нека в A е изпълнено условие 1), а (1) е произволна верига от идеали на A. Да означим с I теоретико-множественото обединение $\bigcup_{i=1}^{\infty} I_i$ на идеалите I_1, I_2, ... Ще покажем, че подмножеството I е идеал на A. Нека a и b са от I, а $r \in A$. Тогава $a \in I_k$ и $b \in I_l$ за някои k и l. Тъй като I_k е идеал, то $ra \in I_k \subseteq I$, т. е. I издържа умножението с произволни елементи от A. Ако $s = \max\{k, l\}$, то $a, b \in I_s$ и затова $a - b \in I_s \subseteq I$, което показва, че I е подгрупа на адитивната група на пръстена A. Следователно I е идеал на A.

Тъй като всеки идеал на A е крайно породен, съществуват такива елементи $a_1, a_2, \ldots, a_n \in A$, че $I = (a_1, a_2, \ldots, a_n)$. Всеки елемент a_i се съдържа в някой идеал I_{k_i} $(i = 1, 2, \ldots, n)$. Нека $m = \max\{k_1, k_2, \ldots, k_n\}$. Тогава $a_1, a_2, \ldots, a_n$ се съдържат в I_m, понеже $I_{k_i} \subseteq I_m$ $(i = 1, 2, \ldots, n)$. Всеки елемент x от I се записва във вида $x = r_1a_1 + r_2a_2 + \ldots + r_na_n$, от което следва, че всеки елемент от I се съдържа в I_m, т. е. $I \subseteq I_m$. Обратното включване е изпълнено по самото определение на I. Така получихме равенството $I_m = I = \bigcup_{i=1}^{\infty} I_i$. От това равенство и от включванията $I_m \subseteq I_{m+1} \subseteq \ldots \subseteq I$ следват равенствата $I = I_m = I_{m+1} = \ldots$, т. е. в пръстена A е изпълнено условие 2) на теоремата.

Обратно, нека за пръстена A е изпълнено условие 2) и I е произволен идеал на A. Да допуснем, че I не е крайно породен идеал. Тогава всяко крайно подмножество от елементи на I ще поражда идеал на A, който строго се съдържа в I. Избираме произволен елемент a_1 от I. Идеалът $I_1 = (a_1)$ се съдържа в I, но не съвпада с I. Нека a_2 е елемент от I, който не се съдържа в I_1. Тогава идеалът $I_2 = (a_1, a_2)$ строго съдържа I_1, тъй като $a_2 \in I_2$ и a_2 не се съдържа в I_1. Понеже I_2 е крайно породен и $I_2 \subseteq I$, то $I_2 \neq I$. Да допуснем, че вече сме избрали елементите a_1, a_2, ..., a_n от I и $I_n = (a_1, a_2, \ldots, a_n)$. Тогава I_n се съдържа в I, но не съвпада с I, тъй като I не е крайно породен. Избираме елемент a_{n+1} от I така, че той да не се съдържа в I_n и полагаме $I_{n+1} = (a_1, a_2, \ldots, a_{n+1})$. Така получаваме веригата от идеали $I_1 \subset I_2 \subset \ldots \subset I_n \subset I_{n+1} \subset \ldots$, в която няма равенство на никое място. Съществуването на такава верига от идеали в A противоречи на факта, че A удовлетворява условие 2). Следователно идеалът I е крайно породен и затова пръстенът A удовлетворява условие 1). Теоремата е доказана.

Определение 4. Всеки комутативен пръстен A с единица, в който е изпълнено едно от условията на предишната теорема, се нарича *нътеров пръстен*. Ако при това A е област на цялостност, то A се нарича *нътерова област*.

Следствие 2. *Всеки пръстен на главни идеали е нътеров пръстен.*

Наистина всеки идеал в пръстен на главни идеали се пораж-да от един елемент, т. е. всеки идеал в такъв пръстен е крайно породен.

За резултатите, които ще изложим в следващия параграф, е важно следното

Следствие 3. *Нека A е област на главни идеали. Тогава в A не съществува безкрайна редица от елементи $a_1, a_2, \ldots, a_n, \ldots$, за която са изпълнени следните две условия:*

1) a_{i+1}/a_i $(i=1, 2, \ldots, n, \ldots)$;

2) *a_i не е асоциран с a_{i+1}* $(i=1, 2, \ldots, n, \ldots)$.

Доказателство. Да допуснем, че в A има редица $a_1, a_2, \ldots, a_n, \ldots$ от елементи със свойствата 1) и 2). Да означим с I_n главния идеал, породен от елемента a_n $(n=1, 2, \ldots)$. Тъй като a_{i+1}/a_i, ще бъде вярно включването $I_i \subseteq I_{i+1}$ $(i \geqq 1)$. Така се получава веригата $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ от идеали в A. По предишното следствие пръстенът A е ньотеров и затова съществува такова естествено число m, че $I_m = I_{m+1} = \ldots$. От съвпадението $I_m = (a_m) = (a_{m+1}) = I_{m+1}$ следва (следствие 1), че a_m и a_{m+1} са асоциирани, което противоречи на свойството 2) на редицата $a_1, a_2, \ldots$. Полученото противоречие показва, че в областта A на главни идеали не съществува редица със свойствата 1) и 2). Следствието е доказано.

В следващото изложение с НОД $(a_1, a_2, \ldots, a_n)$ ще означаваме най-голям общ делител на елементите $a_1, a_2, \ldots, a_n$.

Твърдение 4. *Ако $a_1, a_2, \ldots, a_n$ са елементи от комутативния пръстен A с единица, то*

$$(a_1)+(a_2)+\ldots+(a_n)=(d) \tag{2}$$

тогава и само тогава, когато $d=$НОД $(a_1, a_2, \ldots, a_n)$ *и*

$$d=a_1u_1+a_2u_2+\ldots+a_nu_n,\ u_i \in A,\ i=1, 2, \ldots, n. \tag{3}$$

Доказателство. Нека е изпълнено равенството (2). Тогава от (2) и $d \in (d)$ непосредствено следва условието (3). Понеже $(a_i) \subseteq (d)$, то d/a_i за $i=1, 2, \ldots, n$, т. е. d е общ делител на елементите $a_1, a_2, \ldots, a_n$. Ако d_1 е друг техен общ делител, то от (3) следва, че d_1/d. Следователно $d=$НОД $(a_1, a_2, \ldots, a_n)$.

Обратно нека $d=$НОД $(a_1, a_2, \ldots, a_n)$ и е изпълнено условието (3). От d/a_i следва, че $(a_i) \subseteq (d)$, т. е. $(a_1)+(a_2)+\ldots+(a_n) \subseteq (d)$, а от (3) получаваме, че $(d) \subseteq (a_1)+(a_2)+\ldots+(a_n)$. Следователно равенството (2) е изпълнено.

Следствие 4. *Ако A е област на главни идеали, то всеки n елемента $a_1, a_2, \ldots, a_n$ от A има най-голям общ делител d, за който е изпълнено условието* (3).

Следващата теорема показва, че обратното твърдение на следствие 4 е вярно за ньотерови области даже когато условието (3) е поставено само при $n=2$.

Теорема 5. *Следните две твърдения са еквивалентни:*

1) *A е област на главни идеали;*

2) *A* е *ньотерова област, в която всеки два елемента a и b имат най-голям общ делител d и $d=au+bv$ за някои $u, v \in A$.*

Доказателство. 1)⇒2). Според следствие 2 пръстенът A е ньотерова област. Тъй като $(a)+(b)=(d)$ за някой елемент $d \in A$, то условието 2) следва от твърдение 4.

2) ⇒1). Достатъчно е ла докажем, че всеки идеал I на пръстена A е главен. Тъй като A е ньотеров пръстен, то I е крайнопороден идеал, т. е.

$$I=(a_1, a_2, \ldots, a_n)=(a_1)+(a_2)+\ldots+(a_n).$$

Ако $n=1$, то I е главен идеал. Да предположим индуктивно, че $n>1$ и всеки идеал, който се поражда най-много от $n-1$ елемента, е главен идеал на A. Тъй като по условие съществува елемент $d=\text{НОД}(a_1, a_2)$ и $d=a_1u+a_2v$ $(u, v \in A)$, то от твърдение 4 следва, че $(a_1)+(a_2)=(d)$. Следователно $I=(d)+(a_3)+\ldots+(a_n)$ се поражда от $n-1$ елемента и според индуктивното предположение I е главен идеал. Теоремата е доказана.

Накрая ще отбележим без доказателство следните факти.

1. Съществуват области на цялостност, в които всеки два елемента имат НОД и които не са области на главни идеали. В тях най-големият общ делител d на два елемента a и b в общия случай не се представя във вида $d=au+bv$. Примери на такива пръстени са пръстените $P[x_1, \ldots, x_n]$ $(n \geqq 2)$ от полиномите на повече от една променлива над произволно поле P.

2. Съществуват области на цялостност, които не са ньотерови пръстени. Такъв пръстен е например пръстенът $P[x_1, x_2, \ldots]$ от полиномите на безбройно много променливи $x_1, x_2, \ldots$ над произволно поле P. В тази област на цялостност идеалът, породен от променливите $x_1, x_2, \ldots, x_n, \ldots$, не е крайно породен идеал.

§ 4. Аритметика в области на главни идеали

Нека A е произволна област на главни идеали, $a \in A$, $a \neq 0$ и $a=bc$. Ще казваме, че разлагането $a=bc$ на елемента a е истинско разлагане, ако b и c не са делители на единицата, т. е. ако b и c са необратими елементи. За a ще казваме също, че a допуска истинско разлагане или a е разложим елемент.

Ако в разлагането $a=bc$ елементът b е необратим, то и a е необратим, т. е. не може да се говори за истинско разлагане на обратим елемент.

Определение 5. Необратимите ненулеви елементи на областта A на главни идеали, които нямат истинско разлагане, се наричат *прости*.

Лема 1. *Ако елементът p е прост, то прости ще бъдат и всички елементи, които са асоциирани с него.*

Доказателство. Нека $q \sim p$. Тогава $q=\varepsilon p$, където ε е

обратим елемент. Да допуснем, че q не е прост. Възможни са следните два случая: 1) q е обратим; 2) q е необратим.

1. Нека елементът $q=\varepsilon p$ е обратим. Тогава $p=\varepsilon^{-1}q$ като произведение на два обратими елемента е също обратим, което е противоречие с простотата на p.

2. Ако q е необратим, то той допуска истинско разлагане $q=ab$, където a и b са необратими. Тогава $p=(\varepsilon^{-1}a)b$ е истинско разлагане на p, което противоречи на факта, че p е прост елемент.

Примери

1. В пръстена Z на целите числа прости елементи са всички прости числа и техните противоположни.

2. Никое поле не съдържа прости елементи, тъй като ненулевите му елементи са обратими.

3. В пръстена $P[x]$ на всички полиноми над полето P прости елементи са неразложимите полиноми.

4. В пръстена $Z(i)$ на целите гаусови числа прости елементи (виж [19], стр. 126) са:

(*i*) всички прости числа от вида $4x+3$ ($x\in Z$) и асоциираните им;

(*ii*) числото $1+i$ и асоциираните му;

(*iii*) числата от вида $a+bi$, $a-bi$ и асоциираните им, където a^2+b^2 е просто число от вида $4\lambda+1$ ($\lambda\in Z$) и a е четно число.

Лема 2. *Всеки необратим ненулев елемент на областта A на главни идеали се дели на някой прост елемент.*

Доказателство. Нека $a\in A$, $a\neq 0$ и a е необратим елемент.

1. Ако a е прост елемент, лемата е вярна, понеже $a\mid a$.

2. Ако a не е прост, той допуска истинско разлагане $a=a_1b_1$. Ако a_1 е прост, твърдението е доказано. Ако елементът a_1 не е прост, той допуска истинско разлагане $a_1=a_2b_2$. Ако a_2 не е прост елемент, то $a_2=a_3b_3$ и т. н. Този процес не може да продължава неограничено. Действително в редицата

$$a_0=a,\ a_1,\ a_2,\ \ldots$$

е изпълнено условието a_{i+1}/a_i за всяко $i=0, 1, 2, \ldots$ При това $a_i=a_{i+1}b_{i+1}$, където b_{i+1} не е обратим елемент ($i=0, 1, 2, \ldots$), т. е. a_i не е асоцииран с a_{i+1}. Според следствие 3 в A такава безкрайна редица не съществува, т. е. за някое цяло положително число n елементът a_n ще се окаже прост. Лемата е доказана.

Теорема 6. *Всеки необратим ненулев елемент на областта A на главни идеали се разлага в произведение на краен брой прости елементи.*

Доказателство. Нека a е необратим елемент на областта A на главни идеали и $a\neq 0$. По лема 2 съществува прост елемент p_1, който дели a, т. е. $a=p_1a_1$. Ако a_1 е необратим, съществува прост елемент p_2, който дели a_1, т. е. $a_1=p_2a_2$ и т. н. Така получаваме $a_i=p_{i+1}a_{i+1}$, $i=1, 2, \ldots$ Този процес не може да бъде безкраен. Това се показва по същия начин както в доказателството на предишната лема. Следователно за някое цяло по-

ложително число n ще имаме $a_{n-1}=p_n\varepsilon_n$, където ε_n е обратим елемент. По лема 1 елементът $a_{n-1}=p_n'$ ще бъде прост. Следователно $a=p_1 p_2 \ldots p_{n-1} p_n'$ е произведение на прости елементи.

Лема 3. *Ако простият елемент p дели произведението $a_1a_2 \ldots a_n$, то p дели поне един от множителите $a_1, a_2, \ldots, a_n$.*

Доказателство. Ще проведем доказателството с индукция спрямо броя n на множителите.

Ако $n=1$, твърдението е очевидно.

Нека $n=2$, т. е. p/a_1a_2. Да допуснем, че p не дели a_1. Простият елемент p се дели само на обратимите елементи и на своите асоциирани. Общ делител на a_1 и p не може да бъде елемент, асоцииран с p, тъй като тогава a_1 ще се дели на p. Следователно общи делители на a_1 и p са само обратимите елементи и един от НОД на a_1 и p е единицата. Тогава съгласно твърдение 4 $1=a_1u+pv$ за някои елементи u и v от A. Умножаваме двете страни на това равенство с a_2 и получаваме

$$a_2=(a_1\ a_2)\,u+p\,(a_2v).$$

Всяко от събираемите на дясната страна на това равенство се дели на p и затова p/a_2.

Да допуснем, че лемата е вярна за произволни $n-1$ на брой множителя. По условие $p/(a_1a_2 \ldots a_{n-1})a_n$. Следователно или p/a_n и лемата е вярна, или $p/a_1a_2 \ldots a_{n-1}$. Ако е в сила вторият случай, то по индуктивното предположение от $p/a_1a_2 \ldots a_{n-1}$ следва, че p дели поне един от множителите $a_1, a_2, \ldots, a_{n-1}$. Лемата е доказана.

Теорема 7 (за единственост на разлагането). *Нека A е област на главни идеали и a е необратим ненулев елемент на A. Ако $a=p_1p_2 \ldots p_n=q_1q_2 \ldots q_m$, където p_i и q_j са прости ($i=1, 2, \ldots, n$; $j=1, 2, \ldots, m$), то $n=m$ и при подходяща смяна на номерацията на елементите q_j ще имаме $p_i\sim q_i$ за всяко $i=1, 2, \ldots, n$.* С други думи, *всеки необратим ненулев елемент a от областта A на главни идеали се разлага по единствен начин с точност до асоциираност в произведение на прости множители.*

Доказателство. Доказателството ще проведем с индукция спрямо броя n на множителите в първото разлагане.

Ако $n=1$, то $a=p_1$ е прост елемент и затова той не допуска истинско разлагане. Следователно $m=n=1$ и $p_1\sim q_1$ (даже $p_1=q_1$).

Да допуснем, че теоремата е вярна за всички елементи, които имат поне едно разлагане на $n-1$ на брой прости множителя. Тъй като p_1/a и $a=q_1q_2 \ldots q_m$, то по лема 3 p_1 ще дели поне един от простите множители q_j. Като се смени евентуално номерацията на елементите q_j, можем да считаме, че p_1/q_1. Но тогава $p_1\sim q_1$ (p_1 и q_1 са прости елементи), т. е. $p_1=q_1\varepsilon_1$, където ε_1 е обратим елемент. Така получаваме

$$a=q_1\varepsilon_1p_2 \ldots p_n=q_1q_2 \ldots q_m.$$

Тъй като в A няма делители на нулата, от последното равенство получаваме

$$(\varepsilon_1 p_2) p_3 \ldots p_n = q_2 q_3 \ldots q_m.$$

Елементът $(\varepsilon_1 p_2) p_3 \ldots p_n$ има разлагане на $n-1$ на брой прости множителя $\varepsilon_1 p_2, p_3, \ldots, p_n$. По предположението на индукцията $n-1=m-1$ и след подходяща смяна на номерацията на q_j ще имаме $\varepsilon_1 p_2 \sim q_2$ и $p_i \sim q_i$ за $i=3, \ldots, n$. От това, че ε_1 е обратим елемент и $\varepsilon_1 p_2 \sim q_2$, непосредствено следва, че $p_2 \sim q_2$. Получихме, че $n=m$ и $p_i \sim q_j$ за $i=1, 2, \ldots, n$. С това доказателството е завършено.

Твърдение 5. *Нека A е област на главни идеали. Ако p е произволен прост елемент от A, който не дели елемента b от A, но p^k/ab при $k \geqq 1$, то p^k/a.*

Доказателство. Ако $k=1$, твърдението е частен случай на лема 3. Нека $k>1$. Да допуснем, че за $k-1$ теоремата е вярна. Тогава от p^k/ab и p не дели b следва, че p/a, т. е. $a=pa_1$. Нека $ab=p^k d$. Заместваме a в последното равенство с неговото равно и получаваме

$$p(a_1 b - p^{k-1} d) = 0.$$

Тъй като A няма делители на нулата, то $a_1 b = p^{k-1} d$, т. е. $p^{k-1}/a_1 b$. Тогава по индуктивното предположение p^{k-1}/a_1 и $a_1 = p^{k-1} a_2$. Заместваме a_1 в равенството $a=pa_1$ и получаваме: $a=p^k a_2$, т. е. p^k/a.

Теорема 8. *Нека a и b са необратими елементи на областта A на главни идеали и $a=p_1 p_2 \ldots p_n$, $b=q_1 q_2 \ldots q_m$ са разлаганията им на прости множители. Ако никой прост елемент от разлагането на a не е асоциран с елемент от разлагането на b, то НОД $(a, b)=1$.*

Доказателство. Ако $d=$НОД(a, b) и допуснем, че d е необратим, то по теорема 6 ще имаме разлагането $d=r_1 r_2 \ldots r_k$, където r_i са прости елементи. Тогава

$$a = a_1 d = (p_1' p_2' \ldots p_{n-k}') r_1 r_2 \ldots r_k,$$
$$b = b_1 d = (q_1' q_2' \ldots q_{m-k}') r_1 r_2 \ldots r_k$$

са нови разлагания на a и b на прости множители. Съгласно теорема 7 за единственост на разлагането ще бъде изпълнено условието $r_1 \sim p_i$ за някое i и $r_1 \sim q_j$ за някое j. Следователно $p_i \sim q_j$, което противоречи на условието на теоремата. Теоремата е доказана.

Ако a е необратим ненулев елемент на областта A на главни идеали, то видяхме, че a се разлага на прости множители и броят на тези прости множители е постоянно число, което зависи само от елемента a.

По определение под $\delta(a)$ ще разбираме броя на простите множители в кое да е разлагане на елемента a в произведение на прости множители. Тази функция разпространяваме и върху всич-

ки останали елементи на пръстена, като полагаме $\delta(a)=0$, ако a е обратим, и $\delta(0)=\infty$, където за посочения символ ∞ считаме, че са изпълнени условията:

(*i*) $n<\infty$,

(*ii*) $n+\infty=\infty$ за всяко число n;

(*iii*) $\infty+\infty=\infty$.

Задача. Докажете, че $\delta(ab)=\delta(a)+\delta(b)$ за всеки два елемента a и b от A.

Твърдение 6. *Ако* b/a, *то* $\delta(a)\geqq\delta(b)$.

Наистина ако $a=ba_1$, то от твърдението на последната задача $\delta(a)=\delta(b)+\delta(a_1)\geqq\delta(b)$.

Следствие 4. *Ако* $a\sim b$, *то* $\delta(a)=\delta(b)$.

Задача. Докажете, че във всяка област на главни идеали са верни следните твърдения:

(*i*) ако НОД$(a, b)=1$ и НОД$(a, c)=1$, то НОД$(a, bc)=1$;

(*ii*) ако a/c, b/c и НОД$(a, b)=1$, то ab/c.

Обобщете тези твърдения за повече множители.

(*iii*) ако a/bc и НОД$(a, b)=1$, то a/c.

Задача. Нека A е област на главни идеали. Докажете, че идеалът I на пръстена A е прост тогава и само тогава, когато е нулевият идеал или е главен идеал, породен от някой прост елемент на пръстена A.

Задача. Нека A е област на главни идеали, а p е един негов прост елемент. Докажете, че главният идеал (p) е максимален идеал в A.

Задача. Нека A е област на главни идеали и p е прост елемент в A. Докажете, че факторпръстенът $A/(p)$ е поле.

ГЛАВА VII

ЕЛЕМЕНТИ ОТ ТЕОРИЯ НА ЧИСЛАТА

Теорията на числата е един от най-старите и бурно развиващи се раздели на математиката, възникнал в древна Гърция няколко века преди новата ера. Нейните първи по-значителни постижения са свързани с имената на древногръцките математици Питагор, Ератостен, Диофант и др. В по-ново време големи заслуги за развитието ѝ имат Ферма, Ойлер, Лагранж, Гаус, Чебишев, съветските математици Виноградов, Гелфонд, Шнирелман и още много други.

Теория на числата е наука за числовите системи с техните връзки и закони, в която особено внимание се отделя на естествените числа, тъй като те са градивната основа за построяване на другите числови системи: цели, рационални, реални и комплексни числа.

Проблемите и задачите, които са възникнали в теория на числата, могат да се разделят на четири основни групи: решаване на диофантови (неопределени) уравнения, разпределение на простите числа в естествения ред или в други числови редици, решаване на някои адитивни проблеми (отнасящи се до разлагането на цели числа в сума от определен вид събираеми) и диофантови приближения. В последния раздел се разглеждат приближения на реални числа с рационални, решават се в цели числа различни видове неравенства, изучава се структурата на някои видове ирационални числа и др.

От гледна точка на методите, които се използуват за решаване на изброените задачи, в теория на числата са се развили следните основни направления: елементарна, аналитична, алгебрична и геометрична теория на числата. В тази глава ще изложим някои основни резултати от елементарната теория на числата

§ 1. Числови функции

Нека функцията $f(n)$ е дефинирана върху множеството N от естествените числа и приема стойностите си в множеството $\mathbf{Z}$ на целите числа. В теорията на числата е прието функцията $f(n)$ да се нарича *числова*, ако поне за едно естествено число n стойността $f(n)$ е различна от 0.

Определение 1. Числовата функция $f(n)$ се нарича *мултипликативна*, ако за всеки две взаимно прости естествени числа a и b е изпълнено равенството $f(ab)=f(a)f(b)$.

Нека $n_1, n_2, \ldots, n_k$ е произволна система от естествени числа, които са две по две взаимно прости. По индукция лесно се

доказва, че ако $f(n)$ е мултипликативна числова функция, то

$$f(n_1\ n_2\ \ldots\ n_k)=f(n_1)f(n_2)\ \ldots\ f(n_k).$$

Освен това за всяка мултипликативна числова функция $f(n)$ е изпълнено равенството $f(1)=1$. Наистина ако m е едно естествено число, за което $f(m)\neq 0$, то $f(m)=f(m\ .\ 1)=f(m)f(1)$ и следователно $f(1)=1$.

Нека $f(n)$ и $g(n)$ са две мултипликативни числови функции. Тогава тяхното произведение $h=fg$ е също мултипликативна числова функция. Наистина $h(1)=f(1)g(1)=1\neq 0$ и затова $h(n)$ е числова функция. Нека $m,\ n\in N$ и $(m,\ n)=1$. Тъй като f и g са мултипликативни, то

$$h(m\,n)=f(m\,n)\,g(m\,n)=f(m)f(n)\,g(m)g(n)=$$

$$=[f(m)\,g(m)][f(n)\,g(n)]=h(m)\,h(n),$$

т. е. h е мултипликативна числова функция.

От последното твърдение непосредствено следва, че произведението на произволен краен брой мултипликативни функции е мултипликативна функция.

Определение 2. Ако $f(n)$ е произволна числова функция, то функция

$$F(n)=\sum_{d|n} f(d),$$

където сумирането е разпространено върху всички положителни делители на n, се нарича *функция сума* на $f(n)$.

Функцията сума на $f(n)$ е числова функция. Наистина ако m е най-малкото естествено число, за което $f(m)\neq 0$, то

$$F(m)=\sum_{d|m} f(d)=f(m)\neq 0.$$

По-важно е следното

Твърдение 1. *Функцията сума на една мултипликативна числова функция е също мултипликативна.*

Доказателство. Нека $f(n)$ е произволна мултипликативна числова функция и $F(n)$ е нейната функция сума. Ако a и b са взаимно прости естествени числа, то $f(ab)=f(a)f(b)$. Нека d е произволен делител на ab и $a'=(a,\ d)$ е НОД на числата a и d, при което $a=a'a_1$, $d=a'b'$ и $ab=dq$ $(a_1,\ b',\ q\in Z)$. Тогава от равенството $ab=dq$ получаваме, че $a_1b=b'q$, където a_1 и b' са взаимно прости. Оттук следва, че $b'|b$. Освен това числата a' и b' са също взаимно прости, тъй като те са делители съответно на взаимно простите числа a и b. По този начин установихме, че всеки положителен делител d на ab се представя във вида $d=a'b'$, където $a'|a$, $b'|b$ и $(a',\ b')=1$. Следователно ако $a_1,\ a_2,\ \ldots,\ a_r$ са всички положителни делители на a, а $b_1,\ b_2,\ \ldots,\ b_s$ са всички положителни делители на b, то всички положителни делители на

ab са числата $c_{ij}=a_ib_j$ ($i=1,\ 2,\ldots,\ r;\ j=1,\ 2,\ldots,\ s$). Освен това всяко едно от числата $a_1,\ldots,a_r$ е взаимно просто с всяко едно от числата $b_1,\ldots,b_s$. Тогава

$$F(ab)=\sum_{i=1}^{r}\sum_{j=1}^{s}f(c_{ij})=\sum_{i=1}^{r}\sum_{j=1}^{s}f(a_i)\,f(b_j)=$$

$$=\left[\sum_{i=1}^{r}f(a_i)\right]\left[\sum_{j=1}^{s}f(b_j)\right]=F(a)\,F(b).$$

Твърдението е доказано.

От теорема 7 на глава VI следва, че всяко естествено число n по единствен начин се разлага като произведение $n=p_1p_2\ldots p_s$ на прости множители $p_1,\ p_2,\ldots,\ p_s$. Ако някои от тези прости числа се повтарят, след евентуална преномерация на множителите n може да се запише във вида $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, където $p_1,\ p_2,\ldots,\ p_k$ са различни прости числа, а $\alpha_1,\ \alpha_2,\ldots,\alpha_k$ са положителни цели числа. Това еднозначно представяне се нарича *каноничен вид* на естественото число n.

Теорема 1. *Ако $f(n)$ е мултипликативна числова функция и*

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$$

е каноничният вид на естественото число n, то

$$F(n)=\prod_{i=1}^{k}[1+f(p_i)+f(p_i^2)+\ldots+f(p_i^{\alpha_i})].$$

Доказателство. Тъй като съгласно твърдение 3 $F(n)$ е мултипликативна числова функция, а числата $p_1^{\alpha_1},\ p_2^{\alpha_2},\ldots,\ p_k^{\alpha_k}$ са две по две взаимно прости, то

$$F(n)=\prod_{i=1}^{k}F(p_i^{\alpha_i}).$$

Но числата $1=p_i^0,\ p_i,\ p_i^2,\ldots,\ p_i^{\alpha_i}$ са всичките положителни делители на числото $p_i^{\alpha_i}$ ($i=1,\ 2,\ldots,\ k$). Следователно

$$F(p_i^{\alpha_i})=\sum_{d\mid p_i^{\alpha_i}}f(d)=1+f(p_i)+f(p_i^2)+\ldots+f(p_i^{\alpha_i}).$$

Теоремата е доказана.

Теорема 2. *Нека $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$ е каноничният вид на естественото число n. Тогава сумата от всички положителни делители на числото n е*

(1) $$S(n)=\frac{(p_1^{\alpha_1+1}-1)(p_2^{\alpha_2+1}-1)\ldots(p_k^{\alpha_k+1}-1)}{(p_1-1)(p_2-1)\ldots(p_k-1)},$$

а техният брой е

(2) $$\tau(n)=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_n+1).$$

Освен това $S(n)$ и $\tau(n)$ са мултипликативни числови функции.

Доказателство. Разглеждаме числовата функция $f_s(n)=n^s$, където s е произволно цяло неотрицателно число. Очевидно $f_s(n)$ е мултипликативна числова функция. Тогава нейната функция сума съгласно предната теорема е

(3) $$F_s(n)=\sum_{d|n} d^s=\prod_{i=1}^{k}(1+p_i^s+p_i^{2s}+\ldots+p_i^{\alpha_i s})$$

и също е мултипликативна числова функция. При $s=1$ от (3) се вижда, че $F_1(n)$ е равно на сумата от всички положителни делители на n, т. е. $F_1(n)=S(n)$ и оттук получаваме формулата (1). Ако $s=0$, то $d^0=1$ и тогава равенствата (3) показват, че $F_0(n)=\tau(n)$, т. е. вярна е и формулата (2). Теоремата е доказана.

Определение 3. Естественото число n се нарича *съвършено*, ако сумата от всички положителни делители на n, които са по-малки от n, е равна на n, т. е. $S(n)=2n$.

Например числата 6 и 28 са съвършени, защото $6=1+2+3$, $28=1+2+4+7+14$. Следващите две съвършени числа са 496 и 8128. Досега не е известно съществуват ли нечетни съвършени числа. Доказано е, че ако такива числа съществуват, те са твърде големи и не могат да бъдат по-малки например от e^{5279}. Доказано е също така, че те могат да бъдат само от вида $p^{4k+1}l^2$, където $p=4m+1$ е просто число, $(p, l)=1$ и имат поне 2800 различни прости делителя. Не е известно също така краен ли е или безкраен броят на съвършените числа. Четните съвършени числа се характеризират със следната теорема.

Теорема 3. *Необходимото и достатъчно условие четното число n да бъде съвършено е то да бъде от вида $n=2^{\mu}(2^{\mu+1}-1)$, където $\mu\geqq 1$ и числото $2^{\mu+1}-1$ е просто.*

Доказателство. Нека отбележим, че достатъчността на условието е доказана още преди н. е. от Евклид, а необходимостта — почти две хилядолетия по-късно от Леонард Ойлер.

Достатъчност. Нека $n=2^{\mu}(2^{\mu+1}-1)$, $\mu\geqq 1$, и числото $p=2^{\mu+1}-1$ е просто. Тогава според теорема 2

$$S(n)=S(2^{\mu}p)=S(2^{\mu})\,S(p)=(2^{\mu+1}-1)(p+1)$$
$$=2^{\mu+1}(2^{\mu+1}-1)=2n,$$

т. е. числото n е съвършено.

Необходимост. Ако четното число n е съвършено и $n=2^{\mu}a$, където $\mu\geqq 1$, $(2, a)=1$, то

$$2n=S(n)=S(2^{\mu})\,S(a)=(2^{\mu+1}-1)\,S(a),$$

т. е. ще бъде изпълнено равенството

(1) $$2^{\mu+1}a=(2^{\mu+1}-1)S(a).$$

Понеже числото $p=2^{\mu+1}-1$ е нечетно и дели произведението $2^{\mu+1}a$, то p ще дели a. Нека $a=(2^{\mu+1}-1)t$, $t\in N$. Тогава равенството (1) приема вида

(2) $$2^{\mu+1}t=S(a).$$

Да допуснем, че $t>1$. Тогава числата t и $(2^{\mu+1}-1)t$ са различни делители на a и съгласно (2) тяхната сума е равна на $S(a)$. Но това е невъзможно, защото числото едно е положителен делител на a, различен от посочените два делителя. Следователно $t=1$, $a=2^{\mu+1}-1$ и $S(a)=2^{\mu+1}$. Последното равенство е възможно само когато a е просто число. С това доказателството е завършено.

Друг вид естествени числа с интересни свойства са така наречените *дружески числа*. Естествените числа a и b се наричат дружески, ако

$$S(a)-a=b,\ S(b)-b=a$$

и следователно

$$S(a)=S(b)=a+b.$$

Например числата 220 и 284 са дружески.

Определенията за дружески и съвършени числа се срещат още в трудовете на Евклид и Платон. Древните гърци са виждали в тях някаква съвършена хармония и са им придавали мистичен смисъл.

§ 2. Определение и основни свойства на сравненията

Определение 4. Нека n е фиксирано естествено число, т. е. $n\in N$. Ще казваме, че целите числа a и b са сравними по модул n и ще пишем $a\equiv b\pmod n$ тогава и само тогава, когато n дели разликата $a-b$.

Следващото твърдение показва, че на определението за сравнение по даден модул може да бъде дадена и друга форма.

Лема 1. *Целите числа a и b са сравними по модул n ($n\in N$) тогава и само тогава, когато при делението на n числата a и b дават един и същ остатък.*

Доказателство. Нека при делението на n числата a и b имат съответно остатъци r_1 и r_2 и непълни частни q_1 и q_2, т. е.

$$a=q_1n+r_1,\ b=q_2n+r_2\ (0\leqq r_1,\ r_2<n).$$

Тогава от равенството $r_1=r_2$ следва, че разликата $a-b=n(q_1-q_2)$ се дели на n и следователно $a\equiv b\pmod n$. Обратно, ако $a\equiv b\pmod n$, разликата

$$a-b=n(q_1-q_2)+r_1-r_2$$

се дели на n и затова n дели числото r_1-r_2. Тъй като $0\leqq|r_1-r_2|<n$, последното е възможно само тогава, когато $r_1=r_2$, с което лемата е доказана.

Ако (n) е главният идеал, породен от естественото число n, в пръстена $\mathbf{Z}$ на целите числа, както знаем, две цели числа a и b се съдържат в един и същ съседен клас на $\mathbf{Z}$ по идеала (n) тогава и само тогава, когато $a-b\in(n)$. Следователно сравнението $a\equiv b\pmod n$ е равносилно на съвпадението на съседните класове $a+(n)$ и $b+(n)$.

От всичко казано дотук се получава следното твърдение.

Твърдение 2. *За всеки две цели числа a, b и дадено естествено число n са еквивалентни следните пет твърдения:*

(i) $a+(n)=b+(n)$;

(ii) числото b се съдържа в съседния клас $a+(n)$;

(iii) числото n дели разликата $a-b$;

(iv) $a\equiv b\pmod n$;

(v) при делението на n числата a и b дават един и същ остатък.

Действително еквивалентността на твърденията *(i)* и *(ii)* следва от известния факт от теорията на пръстените, че всеки съседен клас еднозначно се определя от произволен свой елемент. Еквивалентността на *(i)* и *(iv)* вече отбелязахме, а еквивалентността на *(iii)* и *(iv)* следва от определението на сравнение по модул n. Накрая еквивалентността на *(iv)* и *(v)* е доказана в лема 1.

Да напомним, че със $\mathbf{Z}_n$ се означава фактор-пръстенът $\mathbf{Z}/(n)$ и елементите на този пръстен са съседните класове

$$C_0=0+(n),\ C_1=1+(n),\ \ldots,\ C_{n-1}=n-1+(n).$$

Лесно се вижда, че действията със сравнения по модул n които ще приведем по-долу, са всъщност операциите събиране и умножение на елементите на фактор-пръстена $\mathbf{Z}_n$. В сила са следните свойства:

1) *За всяко цяло число a имаме $a\equiv a\pmod n$.*

2) *Ако $a\equiv b\pmod n$, то $b\equiv a\pmod n$.*

3) *Ако $a\equiv b\pmod n$ и $b\equiv c\pmod n$, то $a\equiv c\pmod n$.*

4) *Ако $a\equiv b\pmod n$ и c е произволно цяло число, то $ac\equiv bc\pmod n$ и $ac\equiv bc\pmod{nc}$.*

Наистина $n/(a-b)$ и затова $n/(a-b)c$ и $nc/(a-b)c$, т. е. $ac\equiv bc\pmod n$ и $ac\equiv bc\pmod{nc}$.

Когато няма опасност от недоразумения по кой модул се разглеждат сравненията, писането на $\bmod n$ може да се изпусне.

5) *Ако $a\equiv b$ и $c\equiv d$, то $a+c\equiv b+d$, $a-c\equiv b-d$ и $ac\equiv bd$.*

Действително числата $a-b$ и $c-d$ по условие се делят на n. Тогава същото свойство притежават числата $(a+c)-(b+d)=(a-b)+(c-d)$ и $(a-c)-(b-d)=(a-b)+(d-c)$. Освен това според 4) от $a\equiv b$ следва $ac\equiv bc$ и от $c\equiv d$ следва $bc\equiv bd$. Като приложим свойство 3, получаваме $ac\equiv bd$.

Чрез неколкократно прилагане на предното свойство стигаме до извода, че е вярно следното твърдение:

6) *Ако* $S=\sum_{\alpha} A_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$ $(0 \leqq \alpha_i \in Z)$

е произволен израз на целите числа $x_1, x_2, \ldots, x_k$ *с цели коефициенти* A_α *и в израза за* S *заменим* $A_\alpha, x_1, x_2, \ldots, x_k$ *съответно със сравнимите им числа* $B_\alpha, y_1, y_2, \ldots, y_k$ *по модул* n, *новополученото число е също сравнимо с* S *по модул* n.

Наистина от сравненията

$$A_\alpha \equiv B_\alpha,\ x_1 \equiv y_1,\ x_2 \equiv y_2,\ \ldots,\ x_k \equiv y_k \pmod n$$

следват сравненията

$$A_\alpha \equiv B_\alpha,\ x_1^{\alpha_1} \equiv y_1^{\alpha_1},\ x_2^{\alpha_2} \equiv y_2^{\alpha_2},\ \ldots,\ x_k^{\alpha_k} \equiv y_k^{\alpha_k} \pmod n.$$

Чрез почленно умножаване получаваме сравнението

$$A_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} \equiv B_\alpha y_1^{\alpha_1} y_2^{\alpha_2} \ldots y_k^{\alpha_k} \pmod n.$$

Като сумираме по α, ще получим

$$\sum_{\alpha} A_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} \equiv \sum_{\alpha} B_\alpha y_1^{\alpha_1} y_2^{\alpha_2} \ldots y_k^{\alpha_k} \pmod n.$$

Частен случай на свойството 6) е свойството

7) *Ако* $f(x)$ *с произволен полином с цели коефициенти и* $a \equiv b \pmod n$, *то* $f(a) \equiv f(b) \pmod n$.

8) *Ако* $ca \equiv cb \pmod n$, *то* $a \equiv b \left(\mathrm{mod}\ \frac{n}{d}\right)$, където $d=(c, n)$ *е най-големият общ делител на числата* c *и* n.

Наистина нека $d=(c, n)$, $c=c_1 d$ и $n=n_1 d$. Тогава $(c_1, n_1)=1$ и даденото сравнение може да се запише във вида

$$c_1 d\, a \equiv c_1 d\, b \pmod{n_1 d},$$

което показва, че числото

$$\frac{c_1 d\, a - c_1 d\, b}{n_1 d} = \frac{c_1 (a-b)}{n_1}$$

е цяло. Но от $(c_1, n_1)=1$ и $n_1 / c_1(a-b)$ следва, че $n_1/(a-b)$, т. е $a \equiv b \pmod{n_1}$, $n_1 = \frac{n}{d}$, с което твърдението е доказано.

В частност, когато $(c, n) = 1$, от $ca \equiv cb \pmod n$ следва $a \equiv b \pmod n$.

Ще отбележим, че не може да се съкращава общ множител в двете страни на сравнението, когато той не е взаимно прост с модула. Например сравнението $2.3 \equiv 2.5 \pmod 4$ е вярно, но 3 не е сравнимо с 5 по модул 4.

Като следствия от изброените свойства на сравненията по даден модул могат да бъдат посочени и някои други, като например: 1) всяко събираемо от едната страна на сравнението може да бъде прехвърлено от другата с обратен знак; 2) към коя да е страна на сравнението може да бъде прибавено число, кратно на модула; 3) всяко число може да бъде заменено със своя остатък по даден модул и т. н.

Накрая ще отбележим, че ако от всеки от съседните класове $C_0, C_1, \ldots, C_{n-1}$ на $\mathbf{Z}$ по идеала (n) изберем по едно число, получената система от цели числа се нарича *пълна система от остатъци* по модул n. Следователно системата от цели числа $\alpha_1, \alpha_2, \ldots, \alpha_m$ ще образува една пълна система от остатъци по модул n точно тогава, когато техният брой m е равен на броя на съседните класове по идеала (n), т. е. $m=n$ и всеки две от числата $\alpha_1, \alpha_2, \ldots, \alpha_m$ принадлежат на различни съседни класове по (n), т. е. тези числа са две по две несравними по модул n.

Числата $0, 1, \ldots, n-1$ образуват една пълна система от остатъци по модул n.

Задача. Докажете, че ако $(a, n)=1$ и променливата x описва една произволна пълна система от остатъци по модул n, то $ax+b$ също описва пълна система от остатъци по модул n при всяко цяло число b.

§ 3. Обратими елементи във фактор-пръстен $\frac{\mathbf{Z}}{I}$ на пръстена на целите числа

Нека I е произволен ненулев идеал на пръстена $\mathbf{Z}$ на целите числа. Както вече знаем, I се поражда от някое положително цяло число n, т. е. $I=(n)$. Очевидно съседният клас $1+I=1+(n)$ е единичният елемент на фактор-пръстена $Z_n=\mathbf{Z}/I=\mathbf{Z}(n)$. В този параграф ще разгледаме мултипликативната група Z_n^* от обратимите елементи на пръстена Z_n.

Теорема 4. *Съседният клас $a+(n)$ принадлежи на мултипликативната група Z_n^* на фактор-пръстена Z_n тогава и само тогава, когато a и n са взаимно прости числа.*

Доказателство. Съседният клас $a+(n)$ принадлежи на Z_n^* тогава и само тогава, когато съществува такъв съседен клас $b+(n)$ от Z_n, че

$$[a+(n)][b+(n)]=ab+(n)=1+(n),$$

което е еквивалентно на равенството $ab+kn=1$ за някое $k\in\mathbf{Z}$. Но последното равенство всъщност означава, че числата a и n са взаимно прости.

По-рано, при разглеждането на примитивните n-ти корени от единицата, означихме с $\varphi(n)$ броя на целите положителни числа, които са по-малки от n и са взаимно прости с n. Числовата функция φ е известна като функция на Ойлер, а числото $\varphi(n)$ се нарича *индикатор* на числото n. По определение имаме $\varphi(1)=1$.

Елементите на фактор-пръстена Z_n са $C_0=0+(n), C_1=1+(n), \ldots, C_{n-1}=n-1+(n)$, а обратимите елементи сред тях според предната теорема са тези съседни класове C_i $(0<i<n)$, за които i е взаимно просто с n. Следователно вярно е следното твърдение.

Следствие 1. *Редът на мултипликативната група Z_n^* на*

фактор-пръстена $Z_n = Z/(n)$ *е равен на индикатора* $\varphi(n)$ *на числото* n.

Следствие 2. *Фактор-пръстенът* $Z_n = Z/(n)$ *е поле тогава и само тогава, когато* n *е просто число.*

Наистина Z_n е поле тогава и само тогава, когато всеки съседен клас C_i $(i = 1, 2, \ldots, n-1)$ от Z_n е обратим в Z_n. Но съгласно теорема 4 това е изпълнено тогава и само тогава, когато всичките числа $1, 2, \ldots, n-1$ са взаимно прости с n, което е еквивалентно на условието n да бъде просто число.

Ако p е просто число, очевидно Z_p е поле с характеристика p.

Задача. Ако n е съставно число, докажете, че факторпръстенът Z_n съдържа делители на нулата.

От теоремата на Лагранж за крайните групи следва, че редът на всеки елемент g на крайната група G дели реда $|G| = m$ на G и затова $g^m = 1 \in G$ за всяко $g \in G$. В частност за всеки съседен клас $a+(n)$ от Z_n^* ще бъде изпълнено равенството

$$[a+(n)]^{\varphi(n)} = 1+(n). \tag{1}$$

Следствие 3 (теорема на Ферма—Ойлер). *Ако* a *и* n *са взаимно прости числа, то*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Наистина ако a и n са взаимно прости, то съгласно теорема 4 съседният клас $a+(n)$ е елемент от Z_n^* и ще бъде изпълнено равенството (1). Но

$$[a+(n)]^{\varphi(n)} = a^{\varphi(n)}+(n)$$

и затова $a^{\varphi(n)} - 1$ ще се дели на n, т. е. изпълнено е сравнението (2).

Следствие 4 (теорема на Ферма). *Ако* p *е просто число и* p *не дели цялото число* a, *то*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Твърдението е частен случай на предишното следствие, защото $\varphi(p) = p-1$ и $(a, p) = 1$.

Теоремата на Ферма може да се изкаже и в следната форма.

Твърдение 3. *Ако* p *е просто число, то*

$$a^p \equiv a \pmod{p}$$

за всяко цяло число a.

Действително, ако p дели a, очевидно $a^p \equiv a \pmod{p}$. Ако пък p не дели a, по следствие 4 $a^{p-1} \equiv 1 \pmod{p}$ и чрез умножаване с a получаваме, че $a^p \equiv a \pmod{p}$.

Нека цялото число a е взаимно просто с модула n и b е произволно число от съседния клас $a+(n)$. Тогава класът $a+(n) = b+(n)$ е обратим елемент в Z_n и според теорема 4 числото b е също взаимно просто с модул n. Ако от всички класове, които са взаимно прости с дадения модул n, се вземе по едно число, получената система от числа се нарича *редуцирана*

система от остатъци по модул n. Ясно е, че една система от числа ще бъде редуцирана система от остатъци по модул n тогава и само тогава, когато техният брой е равен на $\varphi(n)$, тези числа са две по две несравними по модул n и всяко едно от тях е взаимно просто с n.

Ако цялото число a е взаимно просто с модула n и x описва една редуцирана система от остатъци по модул n, то ax също описва редуцирана система от остатъци по модул n. Наистина нека x пробягва редуцираната система от остатъци $\alpha_1, \alpha_2, \ldots, \alpha_m$, където $m=\varphi(n)$. Тогава числата

$$a\alpha_1, a\alpha_2, \ldots, a\alpha_m \tag{3}$$

са две по две различни и всяко едно от тях е взаимно просто с n, понеже $(a, n)=1$ и $(\alpha_i, n)=1$ $(i=1, 2, \ldots, m)$. Ако допуснем, че

$$a\alpha_i \equiv a\alpha_j \pmod{n},$$

където $i \neq j$, от $(a, n)=1$ ще следва, че $\alpha_i \equiv \alpha_j \pmod{n}$ при $i \neq j$, което не е вярно. Следователно системата от числа (3) е също редуцирана система от остатъци по модул n.

Като се използува тази бележка, теоремата на Ферма — Ойлер се получава от почленното умножаване на сравненията $ax \equiv r \pmod{n}$, където $(a, n)=1$, $0<r<n$ и x пробягва оние числа от редицата $1, 2, \ldots, n-1$, които са взаимно прости с n.

§ 4. Основни свойства на функцията на Ойлер

По-рано установихме, че броят на примитивните n-ти корени на единицата е равен на $\varphi(n)$. В предния параграф показахме, че редът на мултипликативната група Z_n^* на фактор-пръстена $Z_n = Z/(n)$ на пръстена на целите числа е също равен на $\varphi(n)$. В този параграф ще получим редица други основни свойства на функцията $\varphi(n)$.

Лема 2. *За всяко просто число p и за всяко естествено число α е изпълнено равенството*

$$\varphi(p^\alpha)=p^{\alpha-1}(p-1).$$

Действително числото $\varphi(p^\alpha)$ е равно на броя на числата от редицата $1, 2, \ldots, p^\alpha$, които са взаимно прости с p^α, а този брой е равен на разликата между общия брой p^α на числата от тази редица и броя на числата от същата редица, които се делят на простото число p. Но последните числа са $1 \cdot p, 2p, \ldots, p^{\alpha-1} \cdot p$. Следователно

$$\varphi(p^\alpha)=p^\alpha - p^{\alpha-1}=p^{\alpha-1}(p-1).$$

Твърдение 4. *Функцията $\varphi(n)$ на Ойлер е мултипликативна числова функция.*

Доказателство. Трябва да докажем, че ако m и n са

две произволни взаимно прости естествени числа, изпълнено е равенството

$$\varphi(m\,n)=\varphi(m)\,\varphi(n).$$

Нека $I=(m)$ и $J=(n)$ са главните идеали на пръстена $\mathbf{Z}$ на целите числа, породени съответно от m и n. Понеже $(m, n)=1$, то съществуват такива цели числа u и v, че

$$um+vn=1,$$

което показва, че единицата 1 се съдържа в сумата $I+J$. Оттук следва равенството $\mathbf{Z}=I+J$, т. е. идеалите I и J на $\mathbf{Z}$ са взаимно прости. По едно следствие от китайската теорема за остатъците фактор-пръстенът $\mathbf{Z}/(I\cap J)$ е изоморфен на директната сума

$$\mathbf{Z}/I\oplus\mathbf{Z}/J=\mathbf{Z}_m\oplus\mathbf{Z}_n.$$

Тъй като сечението $I\cap J=(m)\cap(n)$ се състои от числата които едновременно се делят на взаимно простите числа m и n то $I\cap J=(m\,n)$. Затова $\mathbf{Z}/(I\cap J)=\mathbf{Z}/(m\,n)=\mathbf{Z}_{mn}$. Така стигаме до извода, че

(1) $$\mathbf{Z}_{mn}\cong\mathbf{Z}_m\oplus\mathbf{Z}_n \text{ при } (m, n)=1.$$

От предишния параграф знаем, че броят на обратимите елементи във фактор-пръстена $\mathbf{Z}_{mn}=\mathbf{Z}/(m\,n)$ е равен на $\varphi(m\,n)$, а от (1) следва, че този брой ще бъде равен на броя на обратимите елементи в директната сума $\mathbf{Z}_m\oplus\mathbf{Z}_n$. Ще докажем, че обратимите елементи в $\mathbf{Z}_m\oplus\mathbf{Z}_n$ са $\varphi(m)\,\varphi(n)$ на брой.

Наистина един елемент

$$\alpha=(a, b),\ a\in\mathbf{Z}_m,\ b\in\mathbf{Z}_n$$

от директната сума $\mathbf{Z}_m\oplus\mathbf{Z}_n$ е обратим точно тогава, когато съществува такъв елемент

$$\beta=(x, y),\ x\in\mathbf{Z}_m,\ y\in\mathbf{Z}_n$$

от $\mathbf{Z}_m\oplus\mathbf{Z}_n$, за който е изпълнено равенството

$$\alpha\beta=(ax, by)=(1_m, 1_n),$$

където $1_m=1+(m)$ и $1_n=1+(n)$ са единичните елементи съответно на $\mathbf{Z}_m$ и $\mathbf{Z}_n$. Тези условия са еквивалентни на равенствата

$$ax=1_m,\ by=1_n,$$

т. е. на обратимостта на a и b съответно в $\mathbf{Z}_m$ и $\mathbf{Z}_n$. Следователно елементът $\alpha=(a, b)$ от $\mathbf{Z}_m\oplus\mathbf{Z}_n$ е обратим тогава и само тогава, когато $a\in\mathbf{Z}_m^*$ и $b\in\mathbf{Z}_n^*$. Тъй като a пробягва множество от $\varphi(m)$ елемента, а b — множество от $\varphi(n)$ елемента, то обратимите елементи $\alpha=(a, b)$ на $\mathbf{Z}_m\oplus\mathbf{Z}_n$ са $\varphi(m)\,\varphi(n)$ на брой. По този начин $\varphi(m\,n)=\varphi(m)\,\varphi(n)$, с което твърдението е доказано.

Сега вече сме в състояние да докажем следната важна теорема.

Теорема 5. *Ако естественото число n има канонично представяне* $n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$, *то*

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Доказателство. Тъй като функцията на Ойлер е мултипликативна числова функция и числата $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$ са две по две взаимно прости, то

$$\varphi(n)=\varphi(p_1^{a_1})\,\varphi(p_2^{a_2})\ldots\varphi(p_k^{a_k}).$$

Но съгласно лема 2 за всяко $i=1, 2, \ldots, k$ е изпълнено равенството

$$\varphi(p_i^{a_i})=p_i^{a_i}\left(1-\frac{1}{p_i}\right).$$

Следователно

$$\varphi(n)=p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a_2}\left(1-\frac{1}{p_2}\right)\ldots p_k^{a_k}\left(1-\frac{1}{p_k}\right)=$$

$$=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right),$$

с което теоремата е доказана.

Следствие 5. *За функцията сума на функцията* $\varphi(n)$ *на Ойлер е изпълнено равенството*

$$F(n)=\sum_{d/n}\varphi(d)=n$$

за всяко естествено число n.

Действително при $n=1$ имаме $F(1)=\varphi(1)=1$, а ако $n>1$ и $n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ е каноничният вид на числото n, то съгласно теорема 1 имаме

$$F(n)=\prod_{i=1}^{k}\left[1+\varphi(p_i)+\varphi(p_i^2)+\ldots+\varphi(p_i^{a_i})\right]=$$

$$=\prod_{i=1}^{k}\left[1+(p_i-1)+(p_i^2-p_i)+\ldots+(p_i^{a_i}-p_i^{a_i-1})\right]=$$

$$=\prod_{i=1}^{k}p_i^{a_i}=n.$$

Задача. Докажете, че

$$\varphi(4n)=2\varphi(2n),\ \varphi(2+4n)=\varphi(1+2n).$$

§ 5. Сравнения от първа степен с едно неизвестно

Нека $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ е полином с цели коефициенти, т. е. целочислен полином, а m е фиксирано естествено число. Когато x приема произволни целочислени значения, полиномът $f(x)$ приема само целочислени стойности. Често се налага да се реши следната задача: *да се намерят всички целочислени значения на x, за които $f(x)$ приема стойности, които се делят на числото m.* За разглеждането на тази задача е удобно да се въведе сравнение от вида

$$f(x)\equiv 0 \pmod m, \tag{1}$$

където задължително $f(x)$ е полином с цели коефициенти. Ако модулът m не дели старшия коефициент на полинома $f(x)$, то $n=\deg f(x)$ се нарича степен на сравнението (1). *Да се реши сравнението* (1) ще рече да се намерят всички цели числа, които, заместени вместо неизвестното x, го превръщат във вярно числово сравнение.

Нека цялото число x_1 е решение на сравнението (1), т. е. $f(x_1)\equiv 0 \pmod m$. Ако x_2 е произволно число, за което $x_2\equiv x_1 \pmod m$, според свойство 7 от § 2 ще имаме $f(x_2)\equiv f(x_1) \pmod m$. Следователно x_2 също удовлетворява сравнението (1). Затова е целесъобразно да считаме, че x_2 и x_1 ($x_2\equiv x_1 \pmod m$) са едно и също решение на сравнението (1), т. е. съседния клас $x_1+(m)$ на пръстена Z по идеала (m) с представител x_1 ще считаме само за едно решение на (1). Две решения y_1 и y_2 на (1) ще считаме за различни, ако съседните класове $y_1+(m)$ и $y_2+(m)$ са различни, т. е. $y_1\not\equiv y_2 \pmod m$.

Две сравнения при един и същи модул m се наричат *еквивалентни*, ако те притежават едни и същи решения.

Например ако $g(x)$ е такъв целочислен полином, че при всяко цяло число a стойността $g(a)$ се дели на m, то сравненията $f(x)\equiv 0 \pmod m$ и $f(x)+g(x)\equiv 0 \pmod m$ са еквивалентни. По същата причина, ако в сравнението $f(x)\equiv 0 \pmod m$ заменим всеки коефициент на $f(x)$ с неговия остатък по модул m, новополученото сравнение ще бъде еквивалентно на даденото.

Затова в определението на степен на едно сравнение искахме модулът m да не дели старшия коефициент на полинома.

Сега е очевидно вече, че всичките решения на едно сравнение по модул m могат да се намерят, като се провери кои от остатъците $0, 1, 2, \ldots, m-1$ го удовлетворяват. Обаче в общия случай тази проверка е свързана с много изчисления и се налага да потърсим други пътища и методи за решаване на сравнения.

Най-напред ще разгледаме общото сравнение от първа степен, което за удобство ще запишем във вида

$$ax\equiv b \pmod m,\ a,\ b\in \mathbf{Z}, \tag{2}$$

където m не дели a.

Теорема 6. *Нека d е най-големият общ делител на числата a и m. Тогава:*

1) *ако $d=1$, сравнението* (2) *има точно едно решение;*

2) *ако $d\neq 1$ и d дели числото b, сравнението* (2) *има точно d различни решения, които образуват един клас по модул $m_1=\frac{m}{d}$;*

3) *ако d не дели числото b, сравнението* (2) *няма решение.*

Доказателство. 1) Нека $(a, m)=1$, а x_1 и x_2 са две цели числа, за които

$$ax_1\equiv b \pmod m,$$
$$ax_2\equiv b \pmod m.$$

Тогава $ax_1\equiv ax_2 \pmod m$ и по свойство 8 от § 2 ще имаме $x_1\equiv x_2 \pmod m$, т. е. сравнението (2) при $(a, m)=1$ има не повече от едно решение. Но $1=au+mv$ за някои цели числа u и v. Като умножим с b двете страни на последното равенство, получаваме $aub+m(vb)=b$, т. е.

$$a(ub)\equiv b \pmod m.$$

Това показва, че числото ub удовлетворява сравнението $ax\equiv b \pmod m$ и затова $ub+(m)$ е негово решение. Следователно в този случай сравнението (2) има точно едно решение.

2) Нека $d=(a, m)>1$ и d/b. Тогава $a=a_1d$, $b=b_1d$, $m=m_1d$, където a_1, b_1, m_1 са цели числа и $(a_1, m_1)=1$. Както вече видяхме, сравнението

$$a_1y\equiv b_1 \pmod{m_1} \tag{3}$$

има единствено решение

$$y\equiv\alpha \pmod{m_1},$$

т. е. всяко число от $\alpha+(m_1)$ удовлетворява сравнение (3) и ако някое цяло число t удовлетворява (3), то $t\in\alpha+(m_1)$.

Нека v е число от $\alpha+(m_1)$. Тогава $a_1v\equiv b_1 \pmod{m_1}$ и според свойство 4 от § 2 ще следва, че $da_1v\equiv db_1 \pmod{m_1d}$, т. е. числото v удовлетворява сравнението (2) и затова съседният клас $v+(m)$ е едно решение на това сравнение. Числата $x_1=\alpha$, $x_2=\alpha+m_1, \ldots, x_d=\alpha+(d-1)m_1$, се съдържат в класа $\alpha+(m_1)$ и са несравними по модул m. Затова съседните класове

$$\bar{x}_1=\alpha+(m),\ \bar{x}_2=\alpha+m_1+(m), \ldots, \bar{x}_d=\alpha+(d-1)m_1+(m) \tag{4}$$

са d различни решения на сравнението (2). Ще покажем, че това са всичките решения на (2) и че обединението на съседните класове $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_d$ съвпада с класа $\alpha+(m_1)$.

Нека w е цяло число, за което $aw\equiv b \pmod m$, т. е. $da_1w\equiv db_1 \pmod{m_1d}$. Според свойство 8 на числовите сравнения $a_1w\equiv b_1 \pmod{m_1}$ и затова $w\in\alpha+(m_1)$. Следователно всяко решение на сравнението (2) се съдържа в $\alpha+(m_1)$. В частност класовете

$\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_d$ са подмножества на $\alpha+(m_1)$. Но ако $t \in \alpha+(m_1)$, то, $t=\alpha+sm_1$ за някое цяло число s. Разделяме s на d и нека

$$s=dq+r \quad (0 \leqq r<d).$$

Тогава $t=\alpha+rm_1+qm$ се съдържа в класа $\bar{x}_{r+1}=\alpha+rm_1+(m)$. Следователно класът $\alpha+(m_1)$ е обединение на класовете $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_d$ и тези класове са всичките решения на сравнението $ax \equiv b \pmod m$.

3) Нека числото $d=(a, m)$ да не дели числото b. Да допуснем, че съществува цяло число x_0, за което

$$ax_0 \equiv b \pmod m,$$

т. е. $ax_0=b+mk$ за някое цяло число k. Тъй като d/a и d/m, то d дели $b=ax_0-mk$, което е противоречие. Следователно, когато $d=(m, a)$ не дели b, сравнението $ax \equiv b \pmod m$ няма решение. Теоремата е доказана.

Когато модулът m е твърде голямо число, решаването на сравнение от вида

$$ax \equiv b \pmod m$$

чрез непосредствена проверка (т. е. пресмятането кои от остатъците 0, 1, 2, ..., $m-1$ го удовлетворяват) е твърде трудно. Затова е целесъобразно сравнението да бъде заменено с неопределеното уравнение

$$ax=b+my \tag{4}$$

с две неизвестни x и y. Ясно е, че ако (x_0, y_0) е едно целочислено решение на (4), то x_0 удовлетворява сравнението $ax \equiv b \pmod m$ и, обратно, ако x_0 удовлетворява това сравнение, то съществува такова цяло число y_0, че (x_0, y_0) е целочислено решение на (4). По този начин решаването на даденото сравнение се свежда до намирането на целочислените решения на уравнението (4), което може да бъде извършено например по метода на Ойлер. За илюстрация на този метод ще разгледаме един конкретен пример.

Пример. Да се реши сравнението

$$47x+17 \equiv 0 \pmod{28}.$$

Най-напред коефициентите в лявата част на сравнението заменяме с техните остатъци по модул 28 и получаваме сравнението

$$19x+17 \equiv 0 \pmod{28}, \tag{5}$$

което е еквивалентно на даденото. Понеже $1=(19, 28)$, сравнението (5) има точно едно решение. За да намерим това решение, разглеждаме неопределеното уравнение

$$19x+17=28y.$$

От това уравнение получаваме

$$x=\frac{28y-17}{19}=y+\frac{9y-17}{19}=y+z,$$

където $z=\frac{9y-17}{19}$.

Понеже x и y трябва да бъдат цели числа, то е необходимо y да приема такива цели стойности, за които е цяло и числото $z=\frac{9y-17}{19}$, т. е. y трябва да бъде от вида

$$y=\frac{19z+17}{9}=2z+1+\frac{z+9}{9}=2z+1+u,$$

където z е такова цяло число, за което числото $u=\frac{z+9}{9}$ е също цяло. Тъй като $z=9u-8$ е цяло число за всяко $u\in Z$, като приемем u за целочислен параметър, ще получим

$$y=2z+1+u=2(9u-8)+1+u=19u-15,$$
$$x=y+z=(19u-15)+(9u-8)=28u-23,$$

т. е. за всяко цяло число u двойката цели числа $x=28u-23$ и $y=19u-15$ е решение на неопределеното уравнение $19x+17=28y$. Затова всички цели числа от вида $x=28u-23$ ($u\in Z$) удовлетворяват сравнението (5). Следователно единственото решение на сравнението (5), което е еквивалентно на даденото в началото сравнение, е $x\equiv-23 \pmod{28}$, т. е. $x\equiv 5 \pmod{28}$.

В редица случаи решаването на дадено сравнение може да бъде значително опростено, ако се прояви известна наблюдателност. Например, ако трябва да решим сравнението

$$19x+14\equiv 0 \pmod{21},$$

можем да забележим, че числото $7=(14, 21)$ трябва да дели произведението $19x$. Но 7 и 19 са взаимно прости, поради което $x=7t$ за някое $t\in Z$. Тогава даденото сравнение добива вида $19t+2\equiv 0 \pmod 3$, а то е еквивалентно на сравнението $t+2\equiv 0 \pmod 3$. Последното сравнение има единствено решение $t\equiv 1 \pmod 3$. Оттук получаваме $t=1+3u$ и $x=7t=21u+7$, т. е. $x\equiv 7 \pmod{21}$ е единственото решение на даденото сравнение.

Задача. Докажете, че решението на сравнението $ax\equiv b \pmod m$, където $(a, m)=1$, е $x\equiv ba^{\varphi(m)-1} \pmod m$.

§ 6. Системи сравнения от първа степен с едно неизвестно

По-обща от разгледаната в предишния параграф задача е задачата за намиране на решенията на една система от сравнения

$$\text{(I)}\qquad \begin{cases} f_1(x)\equiv 0 \pmod{m_1} \\ f_2(x)\equiv 0 \pmod{m_2} \\ \cdots\cdots\cdots \\ f_k(x)\equiv 0 \pmod{m_k}, \end{cases}$$

където $f_1(x), f_2(x), \ldots, f_k(x)$ са полиноми с цели коефициенти, а $m_1, m_2, \ldots, m_k$ са естествени числа.

Нека цялото число a удовлетворява системата (1), т. е. $m_i/f_i(a)$ при $i=1, 2, \ldots, k$, а $m=[m_1, m_2, \ldots, m_k]$ е най-малкото общо кратно на числата $m_1, m_2, \ldots, m_k$. Ако b е такова цяло число, че

$$b \equiv a \pmod{m},$$

поради това, че m_i/m, ще имаме $b \equiv a \pmod{m_i}$ за всяко $i=1, 2, \ldots, k$. Но тогава, както видяхме в предишния параграф, ще бъде изпълнено сравнението

$$f_i(b) \equiv 0 \pmod{m_i}, \quad i=1, 2, \ldots, k,$$

т. е. всяко число от съседния клас $a+(m)$ ще удовлетворява системата (1). По-нататък ще считаме, че всички числа от $a+(m)$ образуват едно решение на дадената система и ще записваме това решение със сравнението

$$x \equiv a \pmod{[m_1, m_2, \ldots, m_k]}.$$

Нека $x \equiv c_i \pmod{m_i}$ е решение на i-тото сравнение от системата (1), където $i=1, 2, \ldots, k$. Тогава всяко решение на системата

$$(2) \quad \left| \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \ldots\ldots\ldots \\ x \equiv c_k \pmod{m_k} \end{array} \right.$$

ще бъде решение и на системата (1).

Системата (2) има най-много едно решение. Наистина ако a и b са две числа, които я удовлетворяват, то $m_i/(b-a)$, $i=1, 2, \ldots, k$, и затова $b \equiv a \pmod{[m_1, m_2, \ldots, m_k]}$, т. е. $b \in a+([m_1, \ldots, m_k])$ и решението е не повече от едно.

Обратно, всяко решение на системата (1) е решение на система от вида (2) и затова системата (1) има най-много $n_1 n_2 \ldots n_k$ различни решения, където n_i е броят на решенията на нейното i-то сравнение от (1) при $i=1, 2, \ldots, k$.

Да се реши система сравнения от вида (2), за която предполагаме $0 \leqq c_i < m_i$, $i=1, 2, 3, \ldots k$, е равносилно да се намерят всички цели числа x, които при делението на m_1 дават остатък c_1, при делението на m_2 дават остатък c_2 и т. н. Тази задача е решавана още в началото на нашата ера от китайския математик Сун Тзу, поради което е известна като „китайската задача за остатъците". Работата на Сун Тзу в Европа е станала известна едва през 1852 г. Независимо от китайските математици метод за решаване на такива задачи е бил даден и от индийския математик Браменгупта (588—660).

Теорема 7. *Ако числата $m_1, m_2, \ldots, m_k$ са две по две взаимно прости, системата* (2) *има решение и то е единствено.*

Доказателство. Единствеността на решението беше раз-

гледана по-горе. За да докажем съществуването на решение на системата (2), разглеждаме идеалите $I_j=(m_j)$, $j=1, 2, \ldots, k$. Тъй като по условие $(m_i, m_j)=1$, сумата I_i+I_j при $i\neq j$ съдържа числото 1 и следователно $Z=I_i+I_j$, т. е. идеалите $I_1, I_2, \ldots, I_k$ са два по два взаимно прости. Съгласно теорема 6 от глава V за числата $c_1, c_2, \ldots, c_k$ съществува такова цяло число x_0, че $x_0-c_i \in I_i$ $(i=1, 2, \ldots, k)$, т. е.

$$x_0\equiv c_i \pmod{m_i},\ i=1, 2, \ldots, k,$$

с което теоремата е доказана.

Ако модулите $m_1, m_2, \ldots, m_k$ от (2) не са два по два взаимно прости, системата (2) може и да няма решение.

Например лесно се вижда, че системата

$$\left|\begin{array}{l} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 6 \end{array}\right.$$

няма решение.

Едно необходимо (и достатъчно) условие системата (2) да има решение е най-големият общ делител $d_{ij}=(m_i, m_j)$ да дели разликата c_i-c_j при $i, j=1, 2, \ldots, k$. Наистина, ако системата (2) е съвместима, сравненията $x\equiv c_i \pmod{m_i}$ и $x\equiv c_j \pmod{m_j}$ ще образуват съвместима система. Всички числа, които удовлетворяват първото сравнение, са от вида $x=c_i+m_it$ $(t\in Z)$, а от тях второто сравнение удовлетворяват само онези числа, за които

$$m_it+c_i\equiv c_j \pmod{m_j}.$$

От предния параграф знаем, че това сравнение ще има решение относно t само тогава, когато $d_{ij}=(m_i, m_j)$ дели числото c_i-c_j. Достатъчността на посоченото условие за съществуване на решение на системата (2) може да се докаже с индукция по броя на сравненията.

Решаването на системи сравнения от вида (2) ще илюстрираме с един конкретен пример.

Пример. Да се реши системата

$$\left|\begin{array}{l} x\equiv 2 \pmod 5 \\ x\equiv 3 \pmod 6 \\ x\equiv 4 \pmod 7. \end{array}\right.$$

От първото сравнение намираме $x=2+5t$ $(t\in Z)$. Като заместим x във второто сравнение, получаваме сравнението

$$5t\equiv 1 \pmod 6,$$

чието решение е

$$t\equiv 5 \pmod 6.$$

Следователно $t=5+6u$ $(u\in Z)$ и тогава за x ще имаме

$$x=2+5(5+6u)=27+30u.$$

Заместваме така получения израз за x в третото сравнение и получаваме

$$30u+23\equiv 0 \pmod 7.$$

Решението за последното сравнение е $u\equiv 6 \pmod 7$ или $u=6+7v$ $(v\in Z)$. Следователно целите числа, които удовлетворяват дадената система, са от вида

$$x=27+30(6+7v)=207+210v \quad (v\in Z).$$

Тъй като $[5, 6, 7]=210$, решението на дадената система е

$$x\equiv 207 \pmod{210}.$$

Задача. Да се намерят цифрите x, y и z, ако е известно, че числото 138 xyz (записано в десетична система) при делението на 13 дава остатък 6, xyz 138 се дели на 7 и $x1y3z8$ при деление на 11 дава остатък 5.

§ 7. Сравнения от по-висока степен при прост модул

Тук ще разгледаме някои свойства на сравненията от вида

$$(1) \qquad f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\equiv 0 \pmod p,$$

където p е просто число. Най-напред ще докажем, че решаването на това сравнение може да се сведе до решаване на сравнение от степен, най-много равна на $p-1$.

Теорема 8. *Сравнението* (1) *е еквивалентно на сравнението*

$$r(x)\equiv 0 \pmod p,$$

където $r(x)$ *е остатъкът от делението на* $f(x)$ *с полинома* $h(x)=x^p-x$.

Доказателство. Нека

$$(2) \qquad f(x)=g(x)h(x)+r(x),$$

където $\deg r(x)<\deg h(x)=p$. Тъй като $f(x)$ и $h(x)$ са с цели коефициенти и старшият коефициент на $h(x)$ е равен на 1, то $g(x)$ и $r(x)$ са полиноми с цели коефициенти. Съгласно следствие 4 числото p дели $x^p-x=h(x)$ при всяка цяла стойност на x. Тогава непосредствено от равенство (2) следва, че всяко решение на сравнението $r(x)\equiv 0 \pmod p$ е решение на (1) и обратно. Теоремата е доказана.

Практически по-удобно е да се използува последната теорема, като се прилага към всяка степен на неизвестното x по следния начин:

$$x^s=x^{s-p}(x^p-x)+x^{s-(p-1)},$$

т. е. x^s веднага може да се замени с $x^{s-(p-1)}$.

Теорема 9. *Всяко сравнение от степен* $n\geqq 0$ *при прост модул* p *има най-много* n *различни решения.*

Доказателство. Ако $n=0$, сравнението е от вида $ax^0 \equiv 0 \pmod{p}$, където p не дели a и очевидно то няма решения. Да допуснем, че теоремата е вярна за всички сравнения, чиято степен е най-много равна на $n-1$ и нека

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\equiv 0 \pmod{p}$$

е произволно сравнение от степен n, $(a_0, p)=1$. Ако това сравнение няма решение, теоремата е вярна и за него. Ако пък това сравнение има решение $x\equiv x_0 \pmod{p}$, разделяме $f(x)$ с $x-x_0$ и получаваме

$$f(x)=(x-x_0)g(x)+f(x_0),$$

където $g(x)$ е полином с цели коефициенти от степен $n-1$ и със старши коефициент a_0. Понеже $f(x_0)\equiv 0 \pmod{p}$, даденото сравнение добива вида

$$(x-x_0)\,g(x)\equiv 0 \pmod{p}. \tag{3}$$

Нека $x\equiv x_1 \pmod{p}$ е решение на сравнението $f(x)\equiv 0 \pmod{p}$ което е различно от решението $x\equiv x_0 \pmod{p}$. Тогава $x_1 \not\equiv x_0 \pmod{p}$, т. е. p не дели разликата x_1-x_0. Тъй като сравнението (3) е еквивалентно на даденото, то

$$(x_1-x_0)\,g(x_1)\equiv 0 \pmod{p}.$$

Понеже p не дели x_1-x_0 и p е просто число, то $p/g(x_1)$, т.-е

$$g(x_1)\equiv 0 \pmod{p}.$$

С това установихме, че всяко решение на сравнението $f(x)\equiv 0 \pmod{p}$, което е различно от решението $x\equiv x_0 \pmod{p}$, ще бъде решение на сравнението от $(n-1)$-ва степен

$$g(x)\equiv 0 \pmod{p}.$$

По предположение последното сравнение има най-много $n-1$ различни решения и следователно даденото сравнение $f(x)\equiv 0 \pmod{p}$ от степен n ще има не повече от n решения. Теоремата е доказана.

Следствие 6 (теорема на Лагранж). *Нека полиномът $f(x)$ има цели коефициенти и е от степен n. Ако p е просто число и сравнението*

$$f(x)\equiv 0 \pmod{p}$$

има повече от n различни решения, то всички коефициенти на $f(x)$ се делят на p.

Доказателство. Нека

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$

където $a_i \in Z$. Да допуснем, че поне един от коефициентите на $f(x)$ не се дели на p и нека a_k е първият такъв коефициент. Тогава p/a_i $(i=0, 1, \ldots, k-1)$ и сравнението $f(x)\equiv 0 \pmod{p}$ е еквивалентно на сравнението

$$a_k x^{n-k}+a_{k+1}x^{n-k-1}+\ldots+a_{n-1}x+a_n\equiv 0 \pmod p,$$

което е от $(n-k)$-та степен. По предишната теорема последното сравнение има не повече от $n-k$ решения. Това противоречи на условието, че $f(x)\equiv 0 \pmod p$ има повече от n различни решения. Следователно всички коефициенти на $f(x)$ се делят на p. Следствието е доказано.

Трябва да отбележим, че в случая, когато коефициентите на $f(x)$ се делят на p, сравнението $f(x)\equiv 0 \pmod p$ има точно p различни решения, определени от остатъците $0, 1, 2, \ldots, p-1$.

С помощта на това следствие ще получим един критерий за установяване дали дадено цяло число q е просто, който за съжаление при големи стойности на q е практически неприложим.

Теорема 10 (теорема на Уилсън). *Естественото число q е просто тогава и само тогава, когато*

$$(q-1)!+1\equiv 0 \pmod q.$$

Доказателство. Да допуснем, че q е съставно число. Тогава съществува число t $(1<t<q)$, което дели q. Числото t дели и $(q-1)!$. Ако допуснем, че t дели $(q-1)!+1$, ще получим, че t дели 1, което е невъзможно. Следователно, когато q е съставно число, изпълнено е условието $(q-1)!+1\not\equiv 0 \pmod q$.

Нека q е просто число. Ако $q=2$, то $(2-1)!+1=2$ се дели на 2. Затова нека q е нечетно просто число. Да разгледаме сравнението

$$(4)\qquad \psi(x)=x^{q-1}-1-(x-1)(x-2)\ldots(x-q+1)\equiv 0 \pmod q.$$

Тъй като за всяко число x_0 от редицата $1, 2, \ldots, q-1$ имаме $\psi(x_0)=x_0^{q-1}-1$, по теоремата на Ферма получаваме

$$\psi(x_0)\equiv 0 \pmod q,\quad x_0=1, 2, \ldots, q-1.$$

Следователно сравнението (4) има поне $q-1$ различни решения. Тъй като $\psi(x)$ е полином от степен $q-2$, по доказаното следствие коефициентите на $\psi(x)$ ще се делят на q. Свободният член на $\psi(x)$ е равен на $\psi(0)=-1-(-1)^{q-1}(q-1)!$ и понеже $q-1$ е четно число, то $\psi(0)=-1-(q-1)!$ се дели на q, т. е.

$$(q-1)!+1\equiv 0 \pmod q.$$

Теоремата е доказана.

Практическото решаване на дадено сравнение $f(x)\equiv 0 \pmod p$ при прост модул p се извършва обикновено с непосредствена проверка кои от числата $0, 1, 2, \ldots, p-1$ го удовлетворяват. За тази цел е целесъобразно стойностите на $f(x)$ за $x=0, 1, 2, \ldots, p-1$ да се пресмятат по схемата на Хорнер. При това, ако $x\equiv x_0 \pmod p$ е решение на (1), както видяхме, сравненията (1) и (3) са еквивалентни и за следващите остатъци е достатъчно да проверяваме дали удовлетворяват сравнението $g(x)\equiv 0 \pmod p$. Но $x\equiv x_0 \pmod p$ също може да бъде решение на сравнението $g(x)\equiv 0 \pmod p$. В такъв случай, както при уравненията, може да се говори за многократни решения на дадено сравнение.

Задача. Нека $p>2$ е произволно просто число и $\sigma_1, \sigma_2, \ldots, \sigma_{p-2}$ са стойностите на елементарните симетрични полиноми за числата $1, 2, \ldots, p-1$. Докажете, че $\sigma_k \equiv 0 \pmod{p}$ за $k=1,2,\ldots,p-2$.

Задача. Нека p е просто число, а m е произволно естествено число. Докажете, че ако q е непълното частно, а r е остатъкът от делението на m с числото p, то всяко цяло число x удовлетворява сравнението

$$x^m \equiv x^{q+r} \pmod{p}.$$

§ 8. Сравнения при произволен модул

В този параграф ще разгледаме сравнения от произволна степен при съставен модул.

Теорема 11. *Ако $m=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ е каноничното представяне на естественото число m, то сравнението*

$$f(x) \equiv 0 \pmod{m} \tag{1}$$

е еквивалентно на системата

$$\left|\begin{array}{l} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}}. \end{array}\right. \tag{2}$$

Ако n_i е броят на решенията на i-тото сравнение от (2), където $i=1, 2, \ldots, k$, то сравнението (1) има не повече от $n_1 n_2 \ldots n_k$ различни решения.

Доказателство. Нека $x \equiv x_0 \pmod{m}$ е произволно решение на (1). Тогава числото m дели числото $f(x_0)$ и следователно числата $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$ делят $f(x_0)$, т. е. цялото число x_0 удовлетворява системата (2). Тъй като числата $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$ са две по две взаимно прости, тяхното най-малко общо кратно съвпада с произведението им $m=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Съгласно определението от § 6 на решение на система от сравнения $x \equiv x_0 \pmod{m}$ е решение на системата (2).

Обратно, нека $x \equiv x_0 \pmod{m}$ е решение на системата (2). Тогава $p_i^{\alpha_i} \mid f(x_0)$ $(i=1, 2, \ldots, k)$ и понеже $m=[p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}] = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, то $m \mid f(x_0)$. Това означава, че $x \equiv x_0 \pmod{m}$ е решение на сравнението (1).

Втората част на теоремата следва от общите бележки за системи сравнения в § 6 и от еквивалентността на (1) и (2). Теоремата е доказана.

Доказаната теорама показва, че решаването на сравнения при произволен модул се свежда към решаване на сравнения от вида

$$f(x) \equiv 0 \pmod{p^\alpha}, \tag{3}$$

където p е просто число, а $\alpha \geqq 1$. Затова по обстойно ще разгледаме този вид сравнения. Най-напред очевидно е, че всяко цяло-

число x_0, което удовлетворява сравнението (3), ще удовлетворява и сравнението

$$f(x)\equiv 0 \pmod{p}. \tag{4}$$

Поради това всяко решение $x\equiv x_0 \pmod{p^\alpha}$ на (3) определя съседен клас $A=x_0+(p^\alpha)$ на пръстена Z по идеала (p^α), който се съдържа в съседния клас $B=x_0+(p)$ на Z по идеала (p). В обратна посока важи следната

Теорема 12. *Нека $x\equiv c \pmod{p}$ е произволно решение на сравнението* (4) *и числото p не дели $f'(c)$. Тогава всички числа от съседния клас $c+(p)$ на пръстена Z по идеала (p), които удовлетворяват сравнението* (3), *образуват съседен клас на Z по идеала (p^α).*

Доказателство. Да означим с D_k подмножеството от всички числа на класа $c+(p)$, които удовлетворяват сравнението $f(x)\equiv 0 \pmod{p^k}$. Ясно е, че $D_1=c+(p)$ и че са изпълнени включванията

$$D_1 \supseteq D_2 \supseteq \ldots \supseteq D_\alpha .$$

Ще покажем, че D_k е съседен клас на Z по идеала (p^k) за всяко $k=1, 2, \ldots, \alpha$.

Ясно е, че при $k=1$ твърдението е вярно.

Да допуснем, че $D_1, D_2, \ldots, D_r$ са съседни класове съответно по идеалите $(p), (p^2), \ldots, (p^r)$. Тогава $D_r=a+(p^r)$, където $a\in D_1=c+(p)$. Числата от D_r имат вида

$$a+p^r t \quad (t\in Z).$$

От тези числа на D_{r+1} ще принадлежат онези, за които

$$f(a+p^r t)\equiv 0 \pmod{p^{r+1}}.$$

Да представим $f(a+p^r t)$ по формулата на Тейлър във вида

$$f(a+p^r t)=f(a)+\frac{f'(a)}{1!}p^r t+\frac{f''(a)}{2!}(p^r t)^2+\ldots+\frac{f^{(n)}(a)}{n!}(p^r t)^n,$$

където n е степента на $f(x)$. Понеже числата $\frac{f^{(s)}(a)}{s!}$ са цели и коефициентите пред $t^2, t^3, \ldots, t^n$ се делят на p^{r+1}, последното сравнение добива вида

$$f(a)+f'(a)p^r t\equiv 0 \pmod{p^{r+1}}.$$

Тъй като $a\in D_r$, то $p^r | f(a)$ и следователно това сравнение е еквивалентно на сравнението

$$f'(a)t+\frac{f(a)}{p^r}\equiv 0 \pmod{p}. \tag{5}$$

Ще покажем, че последното сравнение има точно едно решение относно t. Наистина a е елемент от $D_r\subseteq D_1=c+(p)$, т. е. $a\equiv c \pmod{p}$. Оттук следва, че $f'(a)\equiv f'(c) \pmod{p}$. Ако допуснем, че p дели $f'(a)$, ще получим, че p дели $f'(c)$, а това по условие

не е вярно. Следователно $(p, f'(a))=1$ и сравнението (5) има точно едно решение $t\equiv t_0 \pmod p$, т. е. $t=t_0+pz$ $(z\in \mathbf{Z})$. Тогава за числата $x=a+p^r t$ $(t\in \mathbf{Z})$ от D_r, които се съдържат в D_{r+1}, получаваме представянето

$$x=a+p^r(t_0+pz)=b+p^{r+1}z,$$

където z е произволно цяло число, а $b=a+p^r t_0$. Очевидно е, че за тези числа образуват съседния клас $b+(p^{r+1})$ на $\mathbf{Z}$ по идеал (p^{r+1}) и $D_{r+1}=b+(p^{r+1})$. Съгласно принципа на пълната математична индукция множеството D_k е съседен клас по идеала (p^k) за всяко k, с което теоремата е доказана.

Доказателството на горната теорема същевременно дава метода за намиране на решенията на сравнението (3), а именно: най-напред намираме всички решения на сравнението (3), а след това, като решаваме сравнения от вида (5), последователно намираме съседните класове $D_2, D_3, \ldots, D_{\alpha-1}, D_\alpha$.

Теорема 13. *Нека $f(x)$ е полином с цели коефициенти, p е просто число,*

$$x\equiv c \pmod{p^k},\ k\geqq 1, \tag{6}$$

е едно решение на сравнението $f(x)\equiv 0 \pmod{p^k}$ и p дели $f'(c)$. Тогава:

1) *ако p^{k+1} не дели $f(c)$, то съседният клас $D_k=c+(p^k)$ не съдържа числа, които удовлетворяват сравнението*

$$f(x)\equiv 0 \pmod{p^{k+1}}; \tag{7}$$

2) *ако p^{k+1} дели $f(c)$, всяко число от класа D_k удовлетворява сравнението (7) и D_k се разпада точно на p различни решения на сравнението (7).*

Доказателство. Както видяхме в доказателството на теорема 12, числото $x=c+p^k t$ $(t\in \mathbf{Z})$ от класа D_k точно тогава удовлетворява сравнението (7), когато c удовлетворява условието

$$f(c)+f'(c)p^k t\equiv 0 \pmod{p^{k+1}}. \tag{8}$$

1) Ако p^{k+1} не дели $f(c)$, последното сравнение няма решение, тъй като p^{k+1} дели числото $f'(c)p^k$. Но тогава няма число от D_k, което да удовлетворява сравнението (7).

2) Ако p^{k+1} дели $f(c)$, сравнението (8) се удовлетворява за всяко число t, защото коефициентите $f(c)$ и $f'(c)p^k$ се делят на p^{k+1}. Затова всяко число от D_k ще удовлетворява сравнението (7). В този случай класът $D_k=c+(p^k)$ се разпада точно на p различни съседни класа по идеала (p^{k+1}), които са решения на (7). Теоремата е доказана.

Доказаните теореми показват, че между числата $x=c+pt$ $(t\in \mathbf{Z})$, които образуват решение на сравнението $f(x)\equiv 0 \pmod p$, може да има 0, 1 или няколко решения на сравнението $f(x)\equiv 0 \pmod{p^\alpha}$.

§ 9. Показатели по даден модул

В следващите два параграфа ще разгледаме по-подробно мултипликативната група Z_m^* от обратимите елементи на фактор-пръстена $Z_m = Z/(m)$, където m е цяло положително число. Както вече знаем, редът $|Z_m^*|$ на групата Z_m^* е равен на $\varphi(m)$ и съседният клас $a+(m)$ принадлежи на Z_m^* тогава и само тогава, когато $(a, m)=1$. Всеки елемент $a+(m)$ от групата Z_m^* поражда крайна циклична подгрупа на Z_m^*, чийто ред ще означаваме с $P_m(a)$ и ще го наричаме *показател* на числото a по модул m. Следователно $P_m(a)$ е най-малкото цяло положително число, за което в Z_m^* е изпълнено равенството

$$[a+(m)]^{P_m(a)} = 1+(m)$$

или още $P_m(a)$ е най-малкото естествено число, за което

$$a^{P_m(a)} \equiv 1 \pmod m.$$

Ако $a \equiv b \pmod m$, то $a+(m)=b+(m)$ и затова $P_m(a)=P_m(b)$, т. е. $P_m(a)$ е показател по модул m на всяко цяло число, което се съдържа в съседния клас $a+(m)$.

Ще посочим някои основни свойства на функцията $P_m(a)$, за която трябва да помним, че е дефинирана само за онези цели числа a, които са взаимно прости с модула m.

1) *Числото $P_m(a)$ е делител на $\varphi(m)$.*

Наистина $P_m(a)$ е ред на циклична подгрупа на групата Z_m^* от ред $\varphi(m)$. Затова твърдението следва непосредствено от теоремата на Лагранж за крайни групи.

2) *Сравнението $a^n \equiv 1 \pmod m$ е изпълнено тогава и само тогава, когато $P_m(a)/n$.*

Наистина даденото сравнение е еквивалентно на равенството

$$[a+(m)]^n = 1+(m)$$

в групата Z_m^*, а от теорията на групите е известно, че последното равенство е възможно точно тогава, когато редът $P_m(a)$ на елемента $a+(m)$ дели числото n.

3) *Сравнението $a^s \equiv a^t \pmod m$ е изпълнено тогава и само тогава, когато $s \equiv t \pmod{P_m(a)}$.*

Да разгледаме случая, когато $s \geqq t$. Тъй като $(a, m)=1$, то и $(a^t, m)=1$. Тогава от даденото сравнение чрез съкращаване на a^t получаваме сравнението

$$a^{s-t} \equiv 1 \pmod m,$$

което е еквивалентно на даденото. Но от свойство 2 следва, че последното сравнение е изпълнено точно тогава, когато $s \equiv t \pmod{P_m(a)}$. Случаят $s<t$ се разглежда по същия начин.

4) *Ако числото a има показател $P_m(a)$ по модул m и n е естествено число, то*

$$P_m(a^n) = \frac{P_m(a)}{(n, P_m(a))},$$

където $(n, P_m(a))$ *е НОД на* n *и* $P_m(a)$.

Това твърдение следва от свойството на цикличните групи, но то може да бъде доказано и независимо от теорията на групите.

Нека $k=P_m(a^n)$, $s=P_m(a)$ и $d=(n, s)$. Тогава $n=n_1d$ и $s=s_1d$, където n_1 и s_1 са взаимно прости числа. Тъй като k е най-малкото естествено число, за което е изпълнено сравнението

$$(a^n)^k=a^{nk}\equiv 1 \pmod m,$$

съгласно свойство 2 числото

$$\frac{nk}{s}=\frac{n_1dk}{s_1d}=\frac{n_1k}{s_1}$$

е цяло положително. Тогава s_1/k, защото $(n_1, s_1)=1$. Но

$$a^{ns_1}=a^{n_1ds_1}=(a^s)^{n_1}\equiv 1 \pmod m,$$

защото $s=P_m(a)$ и $a^s\equiv 1 \pmod m$. Следователно $s_1\geqq k$ и понеже s_2/k, то $s_1=k$. Така получихме равенствата

$$P_m(a^n)=k=s_1=\frac{s}{d}=\frac{P_m(a)}{(n, P_m(a))},$$

с което свойство 4 е доказано.

По този начин фактически доказахме, че цикличната подгрупа, породена от елемента $a^n+(m)=[a+(m)]^n$, има индекс $d=(n, P_m(a))$ в цикличната група $\langle a+(m)\rangle$.

От 4) непосредствено се получава и следното свойство.

5) *Равенството* $P_m(a^n)=P_m(a)$ *е изпълнено тогава и само тогава, когато* n *и* $P_m(a)$ *са взаимно прости числа.*

6) *Нека* p *е просто число и* $P_p(a)=k$. *Тогава класовете*

$$x\equiv a^r \pmod p,\ r=0, 1, 2, \ldots, k-1, \tag{1}$$

са различни и са всичките решения на сравнението

$$x^k\equiv 1 \pmod p. \tag{2}$$

Действително, тъй като $a^k\equiv 1 \pmod p$, то

$$(a^r)^k=(a^k)^r\equiv 1 \pmod p$$

и следователно съседните класове (1) са решения на сравнението (2). Ако допуснем, че $a^s+(p)=a^t+(p)$, където $0\leqq s<t\leqq k-1$, ще имаме $a^t\equiv a^s \pmod p$.

Но съгласно свойство 3) последното сравнение е изпълнено точно тогава, когато k дели разликата $t-s$, което не е възможно, защото $0<t-s<k$. Следователно съседните класове (1) са различни и са точно k на брой. От друга страна, от теоремата на Лагранж за сравнения при прост модул следва, че сравнението (1) може да има най-много k различни решения. Оттук стигаме до извода, че класовете (1) са всичките решения на сравнението (2).

Ако m не е просто число и $P_m(a)=k$, за сравнението $x^k \equiv 1 \pmod m$ може да твърдим само, че класовете

$$x \equiv a^r \pmod m;\ r=0,\ 1,\ 2,\ldots,\ k-1,$$

са k на брой различни негови решения, но не можем да твърдим, че те са всичките му решения.

Пример. Нека $a=5$, $m=12$. Тогава $P_{12}(5)=2$, но сравнението

$$x^2 \equiv 1 \pmod{12}$$

има четири различни решения $1+(12)=5^0+(12)$, $5+(12)$, $7+(12)$ и $11+(12)$.

§ 10. Примитивни корени по даден модул

Естествено възниква въпросът, за кои m мултипликативната група Z_m^* на фактор-пръстена Z_m е циклична? Ако групата Z_m^* е циклична, всеки неин пораждащ елемент се нарича *примитивен корен по модул m*. Тъй като редът на Z_m^* е $\varphi(m)$, елементът $a+(m)$ ще бъде примитивен корен по модул m тогава и само тогава, когато $P_m(a)=\varphi(m)$. В този случай ще казваме още, че числото a е примитивен корен по модул m. Очевидно е, че примитивните корени следва да се търсят между остатъците $1, 2, \ldots, m-1$, тъй като те еднозначно определят ненулевите елементи на фактор-пръстена Z_m. Ясно е, че ако a е примитивен корен по модул m и $a \equiv b \pmod m$, то и числото b е примитивен корен по същия модул.

От свойство 5) на показателите по даден модул следва, че ако a е примитивен корен по модул m и числата n и $\varphi(m)$ са взаимно прости, то a^n е също примитивен корен по модул m.

Следователно, ако по модул m съществува поне един примитивен корен, общият брой на примитивните корени по модул m е поне $\varphi(\varphi(m))$. Всъщност от теорията на групите знаем, че този брой е точно равен на $\varphi(\varphi(m))$, защото цикличната група от ред k има точно $\varphi(k)$ на брой различни образуващи.

Може да се докаже, че примитивни корени по модул m съществуват тогава и само тогава, когато m е равно на едно от числата 2, 4, p^α и $2p^\alpha$, където p е нечетно просто число, а α е произволно цяло положително число. Това означава, че са циклични само мултипликативните групи Z_2^*, Z_4^*, $Z_{p^\alpha}^*$ и $Z_{2p^\alpha}^*$ (p—произволно нечетно просто число). Ще докажем само, че Z_p^* е циклична група за всяко просто число p. Най-напред ще установим следната

Лема 3. *Нека p е просто число и $\psi(k)$ е броят на онези числа от 1 до $p-1$, на които показателят по модул p е равен на k. Тогава $\psi(k)=0$, или $\psi(k)=\varphi(k)$.*

Доказателство. Ако $\psi(k)>0$, нека числото a $(1 \leqq a \leqq p-1)$ да принадлежи на показател k по модул p, т. е. $P_p(a)=k$. Съгласно свойство 6) от предишния параграф числата

(1) $$1,\ a,\ a^2,\ \ldots,\ a^{k-1}$$

определят всичките решения на сравнението

(2) $$x^k \equiv 1 \pmod{p},$$

т. е. решенията на (2) са

$$x \equiv a^r \pmod{p},\ r=0,\ 1,\ 2,\ \ldots,\ k-1.$$

Ако b е друг остатък по модул p, за който $P_p(b)=k$, то $x \equiv b \pmod{p}$ ще бъде решение на сравнението (2) и следователно $b \equiv a^l \pmod{p}$ за някое l $(0 \leqq l \leqq k-1)$. Затова всяко число от 1 до $p-1$, което принадлежи на показател k по модул p, ще бъде сравнимо по модул p с някое от числата (1). Тъй като числата (1) са несравними по модул p, то броят на остатъците 1, 2, ..., $p-1$, които имат показател k по модул p, е равен на броя на числата от редицата (1), които принадлежат на същия показател k по модул p. Съгласно свойство 5) на показателите броят на тези числа е $\varphi(k)$, с което лемата е доказана.

Теорема 14. *Нека p е просто число и $\psi(k)$ е броят на онези числа от* 1 *до $p-1$, на които показателят по модул p е равен на $k>0$. Тогава $\psi(k)=\varphi(k)$, когато k дели числото $\varphi(p)=p-1$, и $\psi(k)=0$, когато k не дели $p-1$.*

Доказателство. Ако a е произволен ненулев остатък по модул p и $P_p(a)=l$, то l дели $\varphi(p)=p-1$ съгласно свойство 1 на показателите. Затова $\psi(k)=0$, когато k не дели $\varphi(p)=p-1$. Нека $1=k_1<k_2<\ldots<k_s=p-1$ са всичките положителни делители на числото $p-1$. Ясно е, че

(3) $$\psi(k_1)+\psi(k_2)+\ldots+\psi(k_s)=p-1.$$

От следствие 5 за функцията сума на функцията φ на Ойлер е известно, че

(4) $$\sum_{d/(p-1)} \varphi(d)=\varphi(k_1)+\varphi(k_2)+\ldots+\varphi(k_s)=p-1.$$

От равенствата (3) и (4) чрез изваждане получаваме

$$[\varphi(k_1)-\psi(k_1)]+[\varphi(k_2)-\psi(k_2)]+\ldots+[\varphi(k_s)-\psi(k_s)]=0.$$

Тъй като разликите в средните скоби съгласно доказаната лема са неотрицателни, от горното равенство получаваме

$$\psi(k_i)=\varphi(k_i)\ (i=1,\ 2,\ \ldots,\ s).$$

Теоремата е доказана.

Следствие 7. *Броят на примитивните корени по модул простото число p е равен на $\varphi(p-1)$ и затова мултипликативната група Z_p^* на фактор-пръстена Z_p е циклична.*

§ 11. Индекси. Приложение на индексите за решаване на двучленни сравнения

Добре е известно, че функцията логаритъм при дадена основа има много приложения в различни раздели на математиката. Ла напомним, че логаритъм на числото a при основа g $(g>0)$ се нарича това число k, за което $a=g^k$, и пишем $k=\log_g a$. До известна степен по аналогичен начин се постъпва при въвеждането на понятието *индекс*, което ще разгледаме само при прост модул.

Нека g е примитивен корен по модул просто число p, т. е. $\varphi(p)=p-1$ е най-малкото цяло положително число, за което

$$g^{p-1}\equiv 1 \pmod p.$$

Тогава числата

(1) $$1=g^0,\ g,\ g^2,\ldots,\ g^{p-2}$$

не се делят на p, две по две са несравними по модул p и понеже броят им е точно равен на $p-1$, те заедно с числото 0 образуват пълна система от остатъци по модул p. Следователно всяко от числата

(2) $$1,\ 2,\ldots,\ p-1,\ p-2$$

се получава като остатък от делението на p на точно едно от числата (1). Ако a е произволно цяло число, което не се дели на p, неговият остатък по модул p ще бъде равен на някое от числата (2), което от своя страна е сравнимо по модул p точно с едно число от редицата (1). Това показва, че за разглежданото число a съществува точно едно цяло число $s\ (0\leqq s\leqq p-2)$, за което е изпълнено сравнението

(3) $$a\equiv g^s \pmod p.$$

Числото $s\ (0\leqq s\leqq p-2)$ от сравнението (3) *наричаме индекс на a по модул p при основа g и пишем* $s=\operatorname{ind}_g a$.

Ще посочим някои основни свойства на индексите, които се използуват в приложенията. Понеже модулът p и основата g при повечето случаи ще бъдат фиксирани, то $\operatorname{ind}_g a$ ще означаваме с $\operatorname{ind} a$.

1) *Сравнението $a\equiv b \pmod p$ е изпълнено тогава и само тогава, когато*

$$\operatorname{ind} a\equiv \operatorname{ind} b \pmod{p-1}.$$

Наистина числото $\operatorname{ind} a=s$ е такова, че

(4) $$a\equiv g^s \pmod p,$$

а за числото $\operatorname{ind} b=t$ е изпълнено сравнението

(5) $$b\equiv g^t \pmod p.$$

Тогава сравнението $a\equiv b \pmod p$ е еквивалентно на сравнението

$$g^s\equiv g^t \pmod p$$

и съгласно свойство 3) на показателите последното сравнение е изпълнено тогава и само тогава, когато $s \equiv t \pmod{P_p(g)}$, т. е.

$$\operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1},$$

тъй като $P_p(g) = p-1$.

2) *Ако целите числа a и b не се делят на p, то*

$$\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}.$$

Действително от (4) и (5) получаваме

$$ab \equiv g^{\operatorname{ind} a + \operatorname{ind} b} \pmod{p},$$

а от определението на $\operatorname{ind}(ab)$ имаме

$$ab \equiv g^{\operatorname{ind}(ab)} \pmod{p}.$$

От последните две сравнения следва, че

$$g^{\operatorname{ind}(ab)} \equiv g^{\operatorname{ind} a + \operatorname{ind} b} \pmod{p},$$

откъдето пак от свойствата на показателите заключаваме, че

$$\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}.$$

С индукция лесно се получава, че предишното свойство е в сила и за повече множители:

$$(6) \quad \operatorname{ind}(a_1 a_2 \dots a_n) \equiv \operatorname{ind} a_1 + \operatorname{ind} a_2 + \dots + \operatorname{ind} a_n \pmod{p-1}.$$

В частния случай, когато $a_1 = a_2 = \dots = a_n$, се получава сравнението

$$(7) \quad \operatorname{ind}(a^n) \equiv n \operatorname{ind} a \pmod{p-1}.$$

Да разгледаме сега двучленното сравнение

$$(8) \quad ax^n \equiv b \pmod{p},$$

където p е просто число, което не дели a и b.

Лема 4. *Сравнението* (8) *има решения тогава и само тогава, когато* $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{d}$, *където d е най-големият общ делител на числата n и $p-1$.*

Доказателство. Ако сравнението (8) има решение $x \equiv x_0 \pmod{p}$, то $ax_0^n \equiv b \pmod{p}$. Като индексираме това сравнение, ще получим

$$\operatorname{ind} a + n \operatorname{ind} x_0 \equiv \operatorname{ind} b \pmod{p-1};$$

а това означава, че $\operatorname{ind} x \equiv \operatorname{ind} x_0 \pmod{p-1}$ е решение на сравнението от първа степен

$$(9) \quad \operatorname{ind} a + n \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1}$$

спрямо неизвестното $\operatorname{ind} x$, което е възможно само когато $d = (n, p-1)$ дели разликата $\operatorname{ind} b - \operatorname{ind} a$. Следователно $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{d}$.

Обратно, нека $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{d}$ и g е примитивният корен по модул p, при който се разглеждат индексите. Оттук следва, че сравнението (9) ще има точно d решения и нека

(10) $$\text{ind}\, x \equiv k \pmod{p-1};$$

е едно от тях. Тогава

(11) $$x \equiv g^k \pmod{p}$$

ще бъде решение на сравнението (8).

Наистина, тъй като (10) е решение на сравнението (9) числото nk е от вида

$$nk = \text{ind}\, b - \text{ind}\, a + s(p-1), \quad s \in Z.$$

Като заместим в (8) неизвестното x с числото g^k, ще получим:

$$a(g^k)^n \equiv a g^{kn} \equiv g^{\text{ind}\, a} \cdot g^{\text{ind}\, b - \text{ind}\, a + s(p-1)} \equiv$$

$$\equiv g^{\text{ind}\, b} g^{(p-1)s} \equiv b \pmod{p},$$

където сме използували определенията за индекс и примитивен корен. Лемата е доказана.

Доказателството на горната лема същевременно ни дава и метод за решаване на двучленни сравнения от вида (8), а именно: най-напред намираме всички решения (10) на сравнението (9), а след това по формула (11) определяме всички решения и на даденото сравнение (8).

По аналогичен начин чрез индексиране могат да бъдат решавани и показателни сравнения от вида

$$a^x \equiv b \pmod{p},$$

където p е просто число.

От особена важност за теорията на числата е сравнението

(12) $$x^n \equiv a \pmod{p}, \quad (a, p) = 1.$$

Всяко число a, за което сравнението (12) има решение, се нарича: *n-ти степенен остатък* по модул p. В обратния случай a се нарича *n-ти степенен неостатък*. При $n=2$ се говори съответно за *квадратични остатъци и квадратични неостатъци*. Очевидно е, че по модул 2 всяко цяло число е n-ти степенен остатък, тъй като то е сравнимо или с нула, или с единица. Ако p е нечетно просто число и цялото число a се дели на p, то a е n-ти степенен остатък по модул p; ако a не се дели на p, то е в сила следната

Теорема 15. *Числото a, което не се дели на нечетното просто число p, е n-ти степенен остатък по модул p тогава и само тогава, когато*

(13) $$a^{\frac{p-1}{d}} \equiv 1 \pmod{p},$$

където d е най-големият общ делител на числата n и $p-1$.

Доказателство. Нека числото a е n-ти степенен остатък по модул p, т. е. сравнението (12) има решение. По предишната лема оттук следва, че d дели числото $\text{ind}_g a$, тъй като $\text{ind}_g 1 = 0$. Ако $\text{ind}_g a = dm$ $(m \in Z)$, то $a \equiv g^{dm} \pmod{p}$ и като повдигнем в:

степен $\frac{p-1}{d}$, ще получим

$$a^{\frac{p-1}{d}} \equiv g^{m(p-1)} \equiv 1 \pmod{p}.$$

Обратно, ако сравнението (13) е изпълнено, то

$$\frac{p-1}{d} \operatorname{ind} a \equiv 0 \pmod{p-1}$$

и от свойствата на сравненията следва, че d дели $\operatorname{ind} a$, т. е

$$\operatorname{ind} a \equiv 0 \equiv \operatorname{ind} 1 \pmod{d}.$$

Съгласно лема 4 това означава, че сравнението (12) има решение и a е n-ти степенен остатък. Теоремата е доказана.

Следствие 8 (критерий на Ойлер). *Числото a, което не се дели на нечетното просто число p, е квадратичен остатък по модул p тогава и само тогава, когато*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{14}$$

и квадратичен недостатък тогава и само тогава, когато

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{15}$$

Действително първата част на твърдението следва непосредствено от теорема 15. Нека $(a, p) = 1$ и p е нечетно просто число. Тъй като от теоремата на Ферма следва, че

$$a^{p-1} \equiv 1 \pmod{p}$$

или

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}, \tag{16}$$

то p дели поне едно от числата $a^{\frac{p-1}{2}} - 1$ и $a^{\frac{p-1}{2}} + 1$. Двете числа едновременно не се делят на p, защото в противен случай p ще дели и тяхната разлика, а това би означавало p да дели числото 2, което не е вярно. По такъв начин a е квадратичен неостатък точно тогава, когато не е изпълнено сравнението (14), следователно по (16) тогава и само тогава, когато p дели $a^{\frac{p-1}{2}} + 1$, т. е. когато е изпълнено сравнението (15). Твърдението е доказано.

§ 12. Символ на Льожандър

В редица раздели от теория на числата широко приложение намира така нареченият символ на Льожандър $\left(\frac{a}{p}\right)$, където p

е нечетно просто число и $(p, a)=1$ (четем „символ на Льожандър на a по отношение на p“). Символът $\left(\frac{a}{p}\right)$ се определя така: ако a е квадратичен остатък по модул p, то $\left(\frac{a}{p}\right)=1$ и $\left(\frac{a}{p}\right)=-1$ — в обратния случай. Например $\left(\frac{1}{p}\right)=1$, $\left(\frac{a^2}{p}\right)=1$, $\left(\frac{7}{19}\right)=1$, $\left(\frac{5}{17}\right)=-1$ и т. н. С помощта на този символ критерият на Ойлер (следствие 8) може да се формулира по следния начин.

Теорема 16. *Ако p е нечетно просто число и $(a, p)=1$, то*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Оттук могат лесно да бъдат изведени в редица свойства на символа $\left(\frac{a}{p}\right)$, които значително улесняват установяването на факта дали a е квадратичен остатък или неостатък по даден модул p. Например непосредствено се установяват следните свойства:

1) *ако* $a \equiv b \pmod{p}$, *то* $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$;

2) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

3) $\left(\frac{a^2}{p}\right)=1$;

4) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Наистина, за да докажем например свойство 4), достатъчно е да забележим, че съгласно критерия на Ойлер е изпълнено сравнението

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Но тъй като $\left(\frac{-1}{p}\right)$ и $(-1)^{\frac{p-1}{2}}$ приемат стойности 1 или -1 и p е нечетно просто число, горното сравнение е изпълнено точно тогава, когато е изпълнено равенството 4).

Ще посочим и някои други свойства на символа $\left(\frac{a}{p}\right)$, но преди това ще докажем следната

Лема 5. *Нека p е нечетно просто число и a е цяло число, което не се дели на p. За всяко $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ определяме целите числа q_k и r_k така, че $ka=q_k p+r_k$, $\frac{-p}{2}<r_k<\frac{p}{2}$. Тогава*

$$\left\{1,\ 2,\ \ldots,\ \frac{p-1}{2}\right\}=\left\{|r_k|\,|\,r_k\in\left(-\frac{p}{2},\frac{p}{2}\right)\right\}.$$

Доказателство. Да положим $A=\left\{1,\ 2,\ \ldots,\ \frac{p-1}{2}\right\}$ и $B=\left\{|r_k|\,|\,r_k\in\left(-\frac{p}{2},\frac{p}{2}\right)\right\}$. Очевидно $B\subseteq A$. Ще покажем, че ако $k\neq l$ и $k,\ l\in A$, то $|r_k|\neq|r_l|$. Действително ако $|r_k|=|r_l|$, то $r_k^2=r_l^2$ и от $r_k\equiv ka\pmod p$, $r_l\equiv la\pmod p$ следва, че $k^2a^2\equiv l^2a^2\pmod p$. Понеже $a\not\equiv 0\pmod p$, то $k^2\equiv l^2\pmod p$. Оттук получаваме сравнението $(k-l)(k+l)\equiv 0\pmod p$, което е равносилно на $k\equiv l\pmod p$ или $k\equiv -l\pmod p$, защото p е просто число. Но тези сравнения са невъзможни, тъй като $k\neq l$ и $k,\ l\in A$.

Доказаното свойство показва, че броят на елементите в множеството B е равен на $\frac{p-1}{2}$. Но броя на елементите в A е също $\frac{p-1}{2}$ и $B\subseteq A$. Следователно $A=B$.

Лема 6 (лема на Гаус). *Нека p е нечетно просто число и a е цяло число, което не се дели на p. За всяко $k\in\left\{1,2,\ldots,\frac{p-1}{2}\right\}$ определяме такива цели числа q_k и r_k, че $ka=q_kp+r_k$ и $-\frac{p}{2}<r_k<\frac{p}{2}$. Тогава ако m е броят на отрицателните числа в множеството $\left\{r_k\,|\,k=1,2,\ldots,\frac{p-1}{2}\right\}$, то $\left(\frac{a}{p}\right)=(-1)^m$.*

Доказателство. От условието на лемата следва, че

$$a^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}k=\prod_{k=1}^{\frac{p-1}{2}}(ka)\equiv\prod_{k=1}^{\frac{p-1}{2}}r_k\pmod p.$$

От предишната лема получаваме равенството

$$\prod_{k=1}^{\frac{p-1}{2}}r_k=(-1)^m\prod_{k=1}^{\frac{p-1}{2}}k.$$

Следователно

$$a^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}k\equiv(-1)^m\prod_{k=1}^{\frac{p-1}{2}}k\pmod p.$$

Понеже k взема стойностите $1,\ 2,\ \ldots,\ \frac{p-1}{2}$, които са взаимно

прости с p, то $a^{\frac{p-1}{2}} \equiv (-1)^m \pmod p$ и по критерия на Ойлер следва, че $\left(\frac{a}{p}\right) = (-1)^m$.

Теорема 17 (закон на Гаус за реципрочност на квадратичните остатъци). *Ако p и q са различни нечетни прости числа, то*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Доказателство. За всяко $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ определяме такива цели числа q_k и r_k, че

$$kq = q_k p + r_k;\ r_k \in \left(-\frac{p}{2}, \frac{p}{2}\right). \tag{1}$$

Сумираме равенствата (1) по модул 2 за $k = 1, 2, \ldots, \frac{p-1}{2}$ и получаваме сравнението

$$q \sum_{k=1}^{\frac{p-1}{2}} k \equiv p \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} r_k \pmod 2. \tag{2}$$

Като вземем предвид, че $q \equiv 1 \pmod 2$, $p \equiv 1 \pmod 2$ и

$$\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2,$$

то от (2) следва, че

$$\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv 0 \pmod 2. \tag{3}$$

Очевидно $r_k \neq 0$, понеже $p \nmid q$ и $(k, p) = 1$. Тогава от (1) получаваме $r_k \in \left(0, \frac{p}{2}\right)$ или $r_k \in \left(-\frac{p}{2}, 0\right)$. Ако $r_k \in \left(0, \frac{p}{2}\right)$, от (1) имаме $q_k = \left[\frac{kq}{p}\right]$, където $[x]$ означава най-голямото цяло число, което не надминава x. Ако $r_k \in \left(-\frac{p}{2}, 0\right)$, от (1) имаме $kq = (q_k - 1)p + p + r_k'$ при което $p + r_k \in \left(\frac{p}{2}, p\right)$. Тогава $q_k = 1 + \left[\frac{kq}{p}\right]$. Като означим с m броя на отрицателните числа в множеството $\left\{r_k \mid k = 1, 2, \ldots, \frac{p-1}{2}\right\}$ и заместим числата q_k в (3), ще получим

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p} \right] (\mathrm{mod}\ 2). \tag{4}$$

Оттук съгласно лемата на Гаус следва, че

$$\left(\frac{q}{p}\right) = (-1)^{\alpha}, \quad \alpha = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p} \right]. \tag{5}$$

Аналогично получаваме

$$\left(\frac{p}{q}\right) = (-1)^{\beta}, \quad \beta = \sum_{l=1}^{\frac{q-1}{2}} \left[\frac{lp}{q} \right]. \tag{6}$$

Следователно

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\alpha+\beta}. \tag{7}$$

Ще докажем, че $\alpha+\beta = \frac{p-1}{2} \cdot \frac{q-1}{2}$. За тази цел разглеждаме множеството M от всички наредени двойки числа (k, l), където $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, $l \in \left\{1, 2, \ldots, \frac{q-1}{2}\right\}$. Очевидно броят на елементите в M е равен на $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Ясно е също така, че $kq - lp \neq 0$ при $1 \leqq k \leqq \frac{p-1}{2}$ и $1 \leqq l \leqq \frac{q-1}{2}$, тъй като в противен случай p ще дели kq, което е невъзможно поради условията $p \nmid q$ и $0 < k < p$. Следователно разликите $kq - lp$ са или положителни, или отрицателни. Нека M_1 е подмножество на M, съставено от всички наредени двойки (k, l), за които $kq - lp < 0$. При фиксирано $l \in \left\{1, 2, \ldots, \frac{q-1}{2}\right\}$ наредената двойка (k, l) принадлежи на M_1 тогава и само тогава, когато k е решение на системата неравенства

$$\left| \begin{array}{l} 1 \leqq k \leqq \frac{lp}{q}, \\ k \leqq \frac{p-1}{2}. \end{array} \right. \tag{8}$$

Ако k е решение на $1 \leqq k \leqq \frac{lp}{q}$, понеже $l \in \left(0, \frac{q}{2}\right)$, то $k \leqq \frac{lp}{2} < \frac{\frac{q}{2} p}{p} = \frac{q}{2}$, т. е. $k \leqq \frac{p-1}{2}$, което показва, че последното неравенство в (8) е следствие от другите две. Следователно системата (8) е еквивалентна на системата неравенства

(9) $$1 \leqq k \leqq \frac{lp}{q}.$$

От определението на функцията $[x]$ се вижда, че броят на решенията на системата (9) е $\left[\frac{lp}{q}\right]$. Като оставим l да се мени в множеството $\left\{1, 2, \ldots, \frac{q-1}{2}\right\}$, получаваме, че броят на елементите в M_1 е равен на

$$\beta = \sum_{i=1}^{\frac{q-1}{2}} \left[\frac{lp}{q}\right].$$

Нека сега M_2 е подмножеството на M, съответно от всички наредени двойки (k, l), за които $kq - lp > 0$. Аналогично се установява, че броят на елементите в M_2 е равен на

$$\alpha = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right].$$

От друга страна, съгласно определението на множествата M_1 и M_2 се вижда, че $M = M_1 \cup M_2$ и $M_1 \cap M_2 = \varnothing$. Следователно $\alpha + \beta = \frac{p-1}{2} \cdot \frac{q-1}{2}$, с което теоремата е доказана.

Законът за реципрочност на квадратичните остатъци може да се запише и във вида

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right),$$

тъй като $\left(\frac{q}{p}\right) = \pm 1$. Това ни дава възможност да сведем пресмятането на $\left(\frac{p}{q}\right)$, като използуваме свойствата 1) и 2), към пресмятане на символа на Льожандър на по-малки остатъци и при по-малки модули. При това понякога ще възниква необходимостта да се пресмята и символът $\left(\frac{2}{p}\right)$, за който законът за реципрочност не може да бъде използуван. За него обаче е в сила следното

Твърдение 5. *Ако p е нечетно просто число, то*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Доказателство. За всяко $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ ще определим такива цели числа a_k и r_k, че

(10) $$2k = a_k p + r_k, \quad -\frac{p}{2} < r_k < \frac{p}{2}.$$

Лесно се вижда, че ако $k\in\left(0, \frac{p}{4}\right)$, то $a_k=0$, $r_k=2k$, а ако $k\in\left(\frac{p}{4}, \frac{p}{2}\right)$, то $a_k=1$, $r_k=2k-p$. Като сумираме равенствата (10) по модул 2 за $k=1, 2, \ldots, \frac{p-1}{2}$, ще получим

$$\sum_{k=1}^{\frac{p-1}{2}} a_k \equiv \sum_{k=1}^{\frac{p-1}{2}} r_k \pmod 2. \tag{11}$$

В полученото сравнение ще използуваме, че $a_k=1$ тогава и само тогава, когато $k\in\left(\frac{p}{4}, \frac{p}{2}\right)$, т. е. a_k се замества с 1 толкова пъти, колкото е броят m на отрицателните числа r_k. Тогава (11) приема вида

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} r_k \pmod 2. \tag{12}$$

В това сравнение числото r_k заместваме или с $2k$, ако $k\in\left(0, \frac{p}{4}\right)$, т. е. ако $r_k=2k\in\left(0, \frac{p}{2}\right)$, или с $p-2k$, когато $k\in\left(\frac{p}{4}, \frac{p}{2}\right)$, т. е. когато $-r_k=p-2k\in\left(0, \frac{p}{2}\right)$. Тогава от лема 5 следва, че

$$\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2,$$

т (12) получаваме, че

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} k \equiv \frac{p^2-1}{8} \pmod 2.$$

рдението е доказано.

ГЛАВА VIII

ЕЛЕМЕНТИ ОТ ТЕОРИЯ НА ПОЛЕТАТА

§ 1. Подполета. Прости полета

Полетата образуват един от най-важните класове от пръстени. В тази глава ще се запознаем с някои от основните свойства на полетата и с тяхното използуване в изследването на геометричните задачи за построение с линийка и пергел.

Нека L е произволно поле. Важна информация за строежа на полето L носят тези от неговите подпръстени, които са полета. Те се наричат *подполета* на полето L. По друг начин казано, непразното подмножество P на полето L се нарича негово подполе, ако P е поле спрямо операциите на полето L.

Примери

1. Самото поле L е подполе на себе си.

2. Полето $\mathbf{Q}$ на рационалните числа е подполе на полето $\mathbf{R}$ на реалните числа, а двете са подполета на полето $\mathbf{C}$ на комплексните числа.

Твърдение 1. *Подмножеството P на полето L е негово подполе тогава и само тогава, когато P има поне два различни елемента и съдържа разликата $a-b$ и частното ab^{-1} (при $b\neq 0$) на всеки два свои елемента a и b.*

Наистина в P се съдържа поне един ненулев елемент c и затова единицата $e=cc^{-1}$ на полето L се съдържа в P. Ако $b\in P$ и $b\neq 0$, то $b^{-1}=eb^{-1}\in P$, т. е. P съдържа заедно с всеки ненулев елемент и неговия обратен. Подмножеството P съдържа и нулевия елемент 0 на L, тъй като $0=b-b$ $(0\neq b\in P)$. Ако $a, b\in P$, то при $b=0$ имаме $ab=0\in P$, а при $b\neq 0$ елементът $ab=a(b^{-1})^{-1}\in P$, т. е. P е затворено относно умножението. Тъй като P е затворено и спрямо изваждането, то P е подпръстен на L. Понеже всеки ненулев елемент на P има обратен в P, то P е поле, т. е. подполе на L. Обратното твърдение е очевидно.

Твърдение 2. *Сечението на произволен (краен или безкраен) брой подполета на дадено поле L е подполе на L.*

Доказателство. Нека P_i $(i\in I)$ са подполета на L, а $P=\bigcap_{i\in I} P_i$. Тъй като нулевият елемент 0 и единичният елемент 1 на L се съдържат във всяко подполе на L, то $0, e\in P$. Нека $a, b\in P$ и $b\neq 0$. Тогава $a, b\in P_i$ за всяко $i\in I$. Понеже P_i е подполе, то $a-b$ и ab^{-1} са елементи на P_i $(i\in I)$. Следователно $a-b$ и ab^{-1} се съдържат в P. От предишното твърдение следва, че сечението P на подполетата P_i $(i\in I)$ е също подполе на L.

Определение 1. Сечението на всички подполета на полето

се нарича *просто подполе* на L. Полето L се нарича *просто поле*, ако то съвпада със своето просто подполе.

Очевидно простото подполе на дадено поле L е единственото минимално подполе на L, т. е. подполе на L, което не съдържа собствени (истински) подполета. Затова простото подполе на L е просто поле.

Теорема 1. *Ако P е поле с характеристика нула, то P е просто тогава и само тогава, когато е изоморфно на полето $\mathbf{Q}$ на рационалните числа. Ако P е с крайна характеристика p, то P е просто поле тогава и само тогава, когато P е изоморфно на полето Z_p на класовете остатъци по модул p.*

Доказателство. Най-напред ще установим, че полетата $\mathbf{Q}$ и Z_p (p — просто число) са прости. За Z_p този факт е очевиден, защото адитивната му група $Z_p(+)$ е от прост ред p и тя няма ненулеви собствени подгрупи, т. е. всяко подполе на Z_p съвпада със Z_p. Нека L е подполе на полето $\mathbf{Q}$ на рационалните числа, т. е. $L \subseteq \mathbf{Q}$. Тогава числото 1 ще се съдържа в L и затова неговите целократни също ще бъдат елементи от L. Следователно пръстенът Z на целите числа е подпръстен на L. Ако r е произволно рационално число, то $r = \frac{s}{t} = st^{-1}$, където $s, t \in Z$ и $t \neq 0$. Тъй като $Z \subseteq L$, то $s, t \in L$. Съгласно твърдение 1 числото $r = st^{-1}$ е елемент от L. Следователно $\mathbf{Q} \subseteq L$ и затова подполето L на $\mathbf{Q}$ съвпада с $\mathbf{Q}$, с което простотата на $\mathbf{Q}$ е доказана.

Нека P е произволно просто поле. Ако характеристиката p на P е крайна, то p е просто число. Да означим с L подмножеството на P, съставено от елементите $0, e, 2e, \ldots, (p-1)e$, където e е единицата на P. Понеже за разликата на два произволни елемента ke и le от L имаме $(k-l)e = (qp+r)e = re$, $0 \leq r \leq p-1$ и аналогично за произведението $ke \cdot le = (kl)e = r_1 e \in L$, $0 \leq r_1 \leq p-1$, то L е подпръстен на P. Тъй като $L \subseteq P$, то L е краен комутативен пръстен без делители на нулата. Следователно L е поле (виж теорема 7 от глава V). Понеже P е просто поле, то $P = L = \{0, e, 2e, \ldots, (p-1)e\}$. Лесно се вижда, че изображението $\varphi: Z_p \to P$, което изобразява класовете остатъци $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}$ съответно в елементите $0, e, 2e, \ldots, (p-1)e$, е изоморфизъм между Z_p и полето P.

Нека P е с характеристика нула. Да означим с φ изображението на $\mathbf{Q}$ в P, което на рационалното число $r = \frac{s}{t}$ ($s, t \in Z, t \neq 0$) съпоставя елемента $(se)(te)^{-1}$ от P. Ако $s = s_1 d$, $t = t_1 d$, където $0 \neq d \in Z$, то $r = \frac{s}{t} = \frac{s_1}{t_1}$. Ще покажем, че елементите $(se)(te)^{-1}$ и $(s_1 e)(t_1 e)^{-1}$ са равни в P. Действително

$$(se)(te)^{-1} = [(s_1 d)e][(t_1 d)e]^{-1} = [(s_1 e)(de)][(t_1 e)(de)]^{-1} =$$
$$= (s_1 e)(de)(de)^{-1}(t_1 e)^{-1} = (s_1 e)(t_1 e)^{-1},$$

откъдето следва, че φ е коректно определено изобра жение. Ако

$r'=\frac{s'}{t'}$ $(s', t' \in Z,\ t' \neq 0)$, то

$$\varphi(r+r')=\varphi\left(\frac{st'+s't}{tt'}\right)=[(st'+s't)\,e][(tt')\,e]^{-1}=(st')\,e\,[(tt')\,e]^{-1}+$$

$$+(s't)\,e\,[(tt')\,e]^{-1}=(se)(te)^{-1}+(s'e)(t'e)^{-1}=\varphi(r)+\varphi(r'),$$

$$\varphi(rr')=\varphi\left(\frac{ss'}{tt'}\right)=[(ss')\,e]\,[(tt')\,e]^{-1}=(se)(s'e)\,[(te)(t'e)]^{-1}=$$

$$=(se)(s'e)(t'e)^{-1}(te)^{-1}=[(se)(te)^{-1}][(s'e)(t'e)^{-1}]=\varphi(r)\varphi(r'),$$

което показва, че φ е хомоморфизъм на $\mathbf{Q}$ в P. Хомоморфизъм φ изобразява 1 в e и затова ядрото $\ker\varphi$ на φ не съвпада с $\mathbf{Q}$. Тъй като полето $\mathbf{Q}$ има само два идеала — нулевия и цялото поле $\mathbf{Q}$, то $\ker\varphi=(0)$, т. е. φ изобразява $\mathbf{Q}$ изоморфно върху образа $I_m\varphi=\varphi(\mathbf{Q})$ на $\mathbf{Q}$ при φ. Следователно $\varphi(\mathbf{Q})$ е подполе на P. Понеже P е просто поле, то $\varphi(\mathbf{Q})=P$ и полетата $\mathbf{Q}$ и P са изоморфни. Теоремата е доказана.

Следствие 1. *Нека L е поле, а P е неговото просто подполе. Тогава ако L е с характеристика нула, то P е изоморфно на полето $\mathbf{Q}$ на рационалните числа, а ако L е с характеристика $p>0$, то P е изоморфно на полето Z_p на класовете остатъци по модул p.*

Наистина простото подполе P е просто поле и неговата характеристика съвпада с характеристиката на полето L. Следователно P е изоморфно на някое от полетата $\mathbf{Q}$ или Z_p (p — просто число) в зависимост от характеристиката на полето L.

§ 2. Разширения на поле

Нека полето P е подполе на полето L. Лесно се вижда, че полето L относно операцията събиране и умножение на елементите от L с елементи от P е линейно пространство над P. Размерността на това линейно пространство над P се нарича *степен* (или *размерност*) на полето L над неговото подполе P и се означава с $[L:P]$. Ще казваме, че полето L е *разширение* на полето P и това разширение ще наричаме *краймерно* или *безкрайномерно* в зависимост от това, дали степента на L над P е крайна или безкрайна. Всеки базис на линейното пространство L над полето P се нарича *базис на разширението* L на P. Очевидно е, че разширението L на полето P е крайномерно тогава и само тогава, когато съществува такава крайна система $\alpha_1, \alpha_2, \ldots, \alpha_m$ от елементи на L, че всеки елемент β от L се записва във вида

$$\beta=p_1\alpha_1+p_2\alpha_2+\ldots+p_m\alpha_m, \tag{1}$$

където $p_1, p_2, \ldots, p_m$ са елементи от P. При това всяка максимална линейно независима над P подсистема на системата от елементи $\alpha_1, \alpha_2, \ldots, \alpha_m$ ще бъде базис на L над P и поради това $[L:P]\leqq m$. Равенството $m=[L:P]$ ще бъде изпълнено точно тога-

ва, когато $\alpha_1, \alpha_2, \ldots, \alpha_m$ са линейно независими над P, т. е. когато записът (1) на всеки елемент от L е еднозначно определен.

Примери

1. Полето $\mathbf{C}$ на комплексните числа е крайномерно разширение на полето $\mathbf{R}$ на реалните числа и $[\mathbf{C}:\mathbf{R}]=2$, защото 1 и i образуват базис на $\mathbf{C}$ над $\mathbf{R}$.

2. Полето $\mathbf{Q}(i)=\{a+bi \mid a, b \in \mathbf{Q}\}$ на гаусовите числа е крайномерно разширение на полето $\mathbf{Q}$ на рационалните числа с базис 1, i над $\mathbf{Q}$, т. е. $[\mathbf{Q}(i):Q]=2$.

3. Полето $\mathbf{R}$ е безкрайномерно разширение на полето $\mathbf{Q}$. Наистина да допуснем, че степента на $\mathbf{R}$ над $\mathbf{Q}$ е крайна и нека $n=[\mathbf{R}:\mathbf{Q}]$. Ако α е произволно реално число, то $1, \alpha, \alpha^2, \ldots, \alpha^n$ са $n+1$ реални числа, поради което тази система от числа ще бъде линейно зависима над $\mathbf{Q}$. Следователно съществуват такива рационални числа $r_0, r_1, \ldots, r_n$, поне едно от които е различно от нула, че е изпълнено равенството

$$r_0 \cdot 1 + r_1\alpha + r_2\alpha^2 + \ldots + r_n\alpha^n = 0.$$

Така α се оказва корен на ненулевия полином $f(x)=r_0+r_1x+\ldots+r_nx^n$ от $\mathbf{Q}[x]$, който е от степен, не по-голяма от n. Следователно всяко реално число е корен на ненулев полином с рационални коефициенти и степен, която не надминава n. За да видим, че последното не е вярно, да вземем аритметичния m-ти корен $\beta=\sqrt[m]{2}$ при $m>n$. Реалното число β е корен на полинома $g(x)=x^m-2$. От критерия на Айзенщайн—Шонеман следва, че $g(x)$ е неразложим полином над полето $\mathbf{Q}$. Нека $h(x)$ е полином, който има най-малка степен сред ненулевите полиноми от $\mathbf{Q}[x]$, за които β е корен. Тогава $\deg h(x) \leqq n$. Тъй като $\deg h(x) \leqq n < m = \deg g(x)$ и $g(x)$ е неразложим над $\mathbf{Q}$ полином, то $h(x)$ и $g(x)$ са взаимно прости полиноми, т. е. ще съществуват такива полиноми $u(x)$, $v(x) \in \mathbf{Q}[x]$, че $1=u(x)h(x)+v(x)g(x)$. От последното равенство получаваме $1=u(\beta)h(\beta)+v(\beta)g(\beta)=u(\beta)\times 0+v(\beta)\cdot 0=0$, което е противоречие. Следователно $\mathbf{R}$ е безкрайномерно разширение на $\mathbf{Q}$.

4. От пример 3 непосредствено следва, че и полето $\mathbf{C}$ на комплексните числа е безкрайномерно разширение на $\mathbf{Q}$.

Твърдение 3. *Нека K е крайно поле с характеристика p. Тогава съществува такова естествено число n, че броят на елементите на K е равен на p^n, т. е. $|K|=p^n$.*

Доказателство. Нека P е простото подполе на K. Тъй като $\operatorname{char} P=p$, полето P е изоморфно на полето $\mathbf{Z}_p$ на класовете остатъци по модул p. Затова P има p на брой елементи. Тъй като K е крайно поле, то K е крайномерно разширение на P. Нека $n=[K:P]$ и $e_1, e_2, \ldots, e_n$ е произволен базис на K над P. Всеки елемент x от K еднозначно се записва във вида $x=x_1e_1+x_2e_2+\ldots+x_ne_n$, където $x_i \in P (i=1, 2, \ldots, n)$. Следователно броят на различните елементи на полето K е равен на броя на

различните n-торки $(x_1, x_2, \ldots, x_n)$ от елементи на P. Всяко x_i може да приема p на брой различни стойности, т. е. броят на елементите на полето K е равен на p^n, където $n=[K:P]$. Твърдението е доказано.

По-нататък ще покажем, че за всяко просто число p и за всяко естествено число n съществува едно-единствено (с точност до изоморфизъм) крайно поле с p^n елемента.

Теорема 2. *Нека полето K е подполе на полето L, а полето L е подполе на полето M, т. е. $K \subseteq L \subseteq M$. Степента $[M:K]$ е крайна тогава и само тогава, когато степените $[L:K]$ и $[M:L]$ са крайни и в този случай е изпълнено равенството*

$$[M:K]=[M:L].[L:K]. \tag{2}$$

Доказателство. Нека M е крайно разширение на K, т. е. степента $[M:K]$ е крайна. Ако $\alpha_1, \alpha_2, \ldots, \alpha_m$ е базис на M над K, то всеки елемент от M се записва като линейна комбинация на базисните елементи $\alpha_1, \alpha_2, \ldots, \alpha_m$ с коефициенти от K, а следователно и с коефициенти от L, защото $K \subseteq L$. По този начин всяка максимална линейно независима над L подсистема на $\alpha_1, \alpha_2, \ldots, \alpha_m$ ще образува базис на M над L. Затова степента $[M:L]$ е крайна и даже $[M:L] \leqq m$. Освен това, тъй като L е подпространство на M (като линейно пространство над K), то степента $[L:K]$ е също крайна.

Обратно, нека степените $n=[L:K]$ и $k=[M:L]$ са крайни. Ако $\beta_1, \beta_2, \ldots, \beta_n$ е базис на L над K, а $\gamma_1, \gamma_2, \ldots, \gamma_k$ е базис на M над L, ще покажем, че системата от елементи $\beta_i \gamma_j$ $(i=1, \ldots, n;$ $j=1, \ldots, k)$ на M е базис на M над K. За тази цел трябва да покажем, че всеки елемент от M е линейна комбинация на тези елементи с коефициенти от K и че те са линейно независими над K.

Нека α е произволен елемент от M. Можем да запишем α във вида

$$\alpha=\sum_{j=1}^{k} l_j \gamma_j \quad (l_j \in L),$$

защото $\gamma_1, \gamma_2, \ldots, \gamma_k$ образуват базис на M над L. Всяко l_j $(j=1, 2, \ldots, k)$ може да се запише във вида

$$l_j=\sum_{i=1}^{n} p_{ij} \beta_i \quad (p_{ij} \in K),$$

защото $\beta_1, \beta_2, \ldots, \beta_k$ образуват базис на L над K. Тогава

$$\alpha=\sum_{j=1}^{k} l_j \gamma_j=\sum_{j=1}^{k} \sum_{i=1}^{n} p_{ij} \beta_i \gamma_j,$$

т. е. α се записва като линейна комбинация на елементите $\beta_i\gamma_j$ с коефициенти от K.

Да допуснем, че

$$\sum_{i=1}^{n}\sum_{j=1}^{k} c_{ij}\beta_i\gamma_j=0,$$

където $c_{ij}\in K$. Трябва да покажем, че коефициентите c_{ij} са равни на нула. Да положим

$$b_j=\sum_{i=1}^{n} c_{ij}\beta_i \ (j=1, 2, \ldots, k).$$

Ясно е, че $b_1, b_2, \ldots, b_k$ са елементи от L и че имаме

$$\sum_{j=1}^{k} b_j\gamma_j=0.$$

Понеже $\gamma_1, \gamma_2, \ldots, \gamma_k$ е базис на M над L, то от последното равенство следват равенствата $b_1=b_2=\ldots=b_k=0$, т. е.

$$\sum_{i=1}^{n} c_{ij}\beta_i=0 \ (j=1, 2, \ldots, k).$$

Тъй като $c_{ij}\in K$, а $\beta_1, \beta_2, \ldots, \beta_n$ са линейно независими над K, от последните k равенства следват равенствата $c_{ij}=0$ ($i=1, \ldots, n$; $j=1, 2, \ldots, k$). Следователно елементите $\beta_i\gamma_j$ са линейно независими над K.

Посоченият базис на M над K съдържа точно nk елемента. Поради това степента $[M:K]$ е крайна и е изпълнено равенството

$$[M:K]=[M:L]\ [L:K]=kn.$$

Теоремата е доказана.

Сега не е трудно с помощта на пълната математична индукция да се докаже следното обобщение на теорема 2.

Следствие 2. *Нека $L_0, L_1, \ldots, L_s (s>1)$ са полета и L_i е подполе на полето L_{i+1}, където $i=0, 1, \ldots, s-1$. Степента $[L_s:L_0]$ е крайна тогава и само тогава, когато степените $[L_1:L_0]$, $[L_2:L_1], \ldots, [L_s:L_{s-1}]$ са крайни и в този случай е изпълнено равенството*

$$[L_s:L_0]=[L_s:L_{s-1}][L_{s-1}:L_{s-2}]\ldots[L_1:L_0]. \tag{3}$$

Следствие 3. *Ако M е крайномерно разширение на полето K, а L е междинно поле, т. е. $K\subseteq L\subseteq M$, то степените $[L:K]$ и $[M:L]$ делят числото $[M:K]$.*

Следствието се получава директно от теорема 7.

Следствие 4. *Ако M е крайномерно разширение на полето K, а L е междинно поле, т. е. $K\subseteq L\subseteq M$, то равенството*

$[M:K]=[M:L]$ *е равносилно с равенството* $L=K$, *а равенството* $[M:K]=[L:K]$ *е равносилно с равенството* $M=L$.

Действително от теорема 2 следва, че равенствата $[M:K]=[M:L]$ и $[M:K]=[L:K]$ са равносилни съответно на равенствата $[L:K]=1$ и $[M:L]=1$. Но разширение на дадено поле има степен 1 тогава и само тогава, когато разширението съвпада с даденото поле (докажете тогава!). Поради това равенствата $[L:K]=1$ и $[M:L]=1$ са равносилни съответно на равенствата $L=K$ и $M=L$.

§ 3. Алгебрични елементи. Строеж на простите алгебрични разширения

Нека K е разширение на полето P. Елементът α от полето K се нарича *алгебричен* над P, ако α е корен на ненулев полином с коефициенти от P. Ако не съществува ненулев полином $f(x)$ с коефициенти от P такъв, че $f(\alpha)=0$, то ще казваме, че α е трансцендентен елемент над P.

Твърдение 4. *Нека полето* K *е разширение на полето* P. *Тогава ако* α *е алгебричен над* P *елемент от* K, *то съществува точно един неразложим над* P *нормиран полином* $p(x)$, *на който* α *е корен. Ако* $f(x)$ *е полином с коефициенти от* P, *то* α *е корен на* $f(x)$ *тогава и само тогава, когато* $p(x)$ *дели* $f(x)$.

Доказателство. Тъй като елементът α е алгебричен над P, то α е корен поне на един ненулев полином от $P[x]$. Измежду всички ненулеви полиноми от $P[x]$, на които α е корен, избираме полином $q(x)$ с най-малка степен. Нека $\deg q(x)=n$ и $q(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$, $a_0, a_1, \ldots, a_n \in P$. Да означим с $p(x)$ нормирания полином $a_0^{-1}q(x)$. Очевидно α е корен на полинома $p(x)$. Понеже $p(x)\in P[x]$ и $n=\deg p(x)=\deg q(x)$, то $p(x)$ е нормиран ненулев полином от $P[x]$, който има най-малка степен сред ненулевите полиноми от $P[x]$, на които α е корен.

Да допуснем, че $p(x)$ е разложим над P. Тогава $p(x)=g(x)h(x)$, където $g(x), h(x)\in P[x]$ и $\deg g(x)>0$, $\deg h(x)>0$. Тъй като $p(\alpha)=0$, то $0=g(\alpha)h(\alpha)$. Ако $g(\alpha)=0$, то α е корен на ненулевия полином $g(x)$ със степен $\deg g(x)=\deg p(x)-\deg h(x)=n-\deg h(x)<n$, което е противоречие. Ако $h(\alpha)=0$, то α е корен на ненулевия полином $h(x)$ от $P[x]$ от степен $\deg h(x)<n$, което също е противоречие. Следователно $p(x)$ е неразложим над P.

Нека $f(x)\in P[x]$ и $f(\alpha)=0$. Да разделим $f(x)$ на $p(x)$ и нека $f(x)=g(x)p(x)+r(x)$, където $g(x), r(x)\in P[x]$ и $\deg r(x)<\deg p(x)$ или $r(x)=0$. Ако $r(x)\neq 0$, от равенствата $0=f(\alpha)=g(\alpha)p(\alpha)+r(\alpha)=r(\alpha)$ следва, че α е корен на ненулевия полином $r(x)$ от степен, по-малка от n, което е невъзможно. Следователно $r(x)=0$ и $p(x)$ дели $f(x)$. Обратното е очевидно.

Ако $p_1(x)$ е друг нормиран неразложим полином над P, на който α е корен, то $p(x)$ ще дели $p_1(x)$. Но $p_1(x)$ се дели само

на полиномите от нулева степен и на своите асоциирани, т. е. $p(x)$ и $p_1(x)$ ще бъдат асоциирани. Понеже и двата полинома са нормирани, то $p(x)=p_1(x)$.

Определение 2. Единственият неразложим над полето P нормиран полином $p(x)$, на който алгебричният елемент α над P е корен, се нарича *минимален полином* на α. Степента на минималния полином на α се нарича степен на алгебричност на α над P.

Лесно се вижда, че степента на алгебричност на α над P е равна на 1 точно в случая, когато $\alpha \in P$.

Твърдение 5. *Нека K е разширение на полето P и L е произволно междинно поле, т. е. $P \subseteq L \subseteq K$. Ако α е елемент от K и α е алгебричен над P, то α е алгебричен и над L. Минималният полином $q(x)$ на α над L дели минималния полином $p(x)$ на α над P и затова степента на алгебричност на α над L не надминава степента на алгебричност на α над P.*

Доказателство. По условие α е алгебричен над P и $p(x)$ е неговият минимален полином. Тъй като $p(\alpha)=0$ и коефициентите на $p(x)$, които са от P, са елементи и от L, то α е алгебричен и над L. От твърдение 4 следва, че минималният полином $q(x)$ на α над L дели полинома $p(x)$ и затова е изпълнено неравенството $\deg q(x) \leqq \deg p(x)$. Твърдението е доказано.

Знаем, че сечението на произволен брой подполета на дадено поле K е подполе на K. Затова ако S е произволно подмножество на полето K, то съществува единствено най-малко подполе на K, което съдържа подмножеството S. Това подполе е сечението на всички подполета на K, които съдържат S.

Определение 3. Ако K е разширение на полето P и α е произволен елемент от K, то най-малкото подполе на K, което съдържа елементите на P и елемента α, се означава с $P(\alpha)$ и се нарича *просто разширение* на P, получено с присъединяването на елемента α към P. Ако α е алгебричен елемент над P, то $P(\alpha)$ се нарича *просто алгебрично разширение* на P, а ако α е трансцендентен над P, то за $P(\alpha)$ се казва, че е *чисто трансцендентно разширение* на P с *базис на трансцендентност* α.

Твърдение 6. *Нека елементът α на разширението K на полето P е трансцендентен над P. Тогава простото разширение $P(\alpha)$ на P е изоморфно на полето $P(x)$ на рационалните функции на променливата x, т. е. $P(\alpha)$ е изоморфно на полето от частни $P(x)$ на пръстена $P[x]$ от полиномите на променливата x.*

Доказателство. Всеки елемент $r(x)$ от $P(x)$ има вида $r(x)=\frac{f(x)}{g(x)}$, където $f(x)$, $g(x) \in P[x]$ и $g(x) \neq 0$. Тъй като α е трансцендентен елемент, то $g(\alpha) \neq 0$ за всеки ненулев полином $g(x)$ от $P[x]$. Нека $\varphi: P(x) \to K$ е изображението, определено с равенството $\varphi[r(x)]=r(\alpha)=\frac{f(\alpha)}{g(\alpha)}$. Лесно се вижда, че φ е хомоморфизъм на $P(x)$ в K. Тъй като полето $P(x)$ има само два

идеала (0) и $P(x)$ и φ не е нулевият хомоморфизъм, то $\ker\varphi$, $=(0)$ и φ изобразява полето $P(x)$ изоморфно върху подполе $\varphi[P(x)]=I_m\varphi$ на K. Понеже елементите на P са елементи и от $P(x)$, а φ ги изобразява в себе си, то $P\subseteq\varphi[P(x)]$. Освен това, $\alpha=\varphi(x)\in\varphi[P(x)]$, т. е. подполето $\varphi[P(x)]$ съдържа $P(\alpha)$. От друга страна, ако $h(x)=p_0x^n+p_1x^{n-1}+\ldots+p_{n-1}x+p_n$ е полином с коефициенти от P, то $\varphi(h(x))=p_0\alpha^n+p_1\alpha^{n-1}+\ldots+p_n$ е елемент от $P(\alpha)$. Тъй като $\varphi(r(x))=r(\alpha)=f(\alpha)g(\alpha)^{-1}$ и $f(\alpha)$, $g(\alpha)\in P(\alpha)$, то $\varphi(r(x))\in P(\alpha)$ за всяко $r(x)\in P(x)$. Затова $\varphi[P(x)]\subseteq P(\alpha)$. Двете включвания доказват равенството $\varphi[P(x)]=P(\alpha)$, т. е. φ е изоморфизъм на полето $P(x)$ върху простото разширение на P, получено с присъединяването на трансцендентния елемент α над P.

Теорема 3. *Нека елементът α от разширението K на полето P има степен n на алгебричност над P. Тогава елементите* $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *образуват базис на простото алгебрично разширение $P(\alpha)$ над P и затова $P(\alpha)$ е крайномерно разширение на P, а неговата степен $[P(\alpha):P]$ съвпада със степента n на алгебричност на α над P.*

Доказателство. Нека $p(x)$ е минималният полином на α над P. По условие имаме $n=\deg p(x)$. Да допуснем, че системата $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ от елементи на $P(\alpha)$ е линейно зависима над P. Тогава ще съществуват такива елементи $p_0, p_1, \ldots, p_{n-1}$ от P, поне един от които е различен от нула, че да е изпълнено равенството.

$$p_0\cdot 1+p_1\alpha+p_2\alpha^2+\ldots+p_{n-1}\alpha^{n-1}=0.$$

Полиномът $g(x)=p_0+p_1x+\ldots+p_{n-1}x^{n-1}$ е от $P[x]$, той е ненулев и $g(\alpha)=0$. Съгласно твърдение 4 полиномът $p(x)$ от степен n щe дели полинома $g(x)$, който има степен, по-малка от n. Полученото противоречие показва, че системата $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ от $P(\alpha)$ е линейно независима над P.

Нека T е линейното подпространство на K, което се състои от всички линейни комбинации от вида $q_0+q_1\alpha+q_2\alpha^2+\ldots+q_{n-1}\alpha^{n-1}$, $(q_i\in P)$.

Ясно е, че T се съдържа в $P(\alpha)$ и че T има за базис над P системата $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. В подпространството T се съдържат елементът α и всички елементи на P. Следователно, ако покажем, че T е подполе на K, от включванията $P\subseteq T\subseteq P(\alpha)$, $\alpha\in T$, и от определението на $P(\alpha)$ ще следва, че $P(\alpha)=T$, а базисът $1, \alpha, \ldots, \alpha^{n-1}$ на T ще бъде базис и на $P(\alpha)$ над P.

За да покажем, че T е подполе, достатъчно е да установим, че: 1) ако $a, b\in T$, то $ab\in T$; и 2) ако $a\in T$ и $a\neq 0$, то $a^{-1}\in T$.

Най-напред ще докажем, че $\alpha^k\in T$ $(k\geqq 0)$. Това е така за $k=0,1,\ldots,n-1$. Ако

$$p(x)=x^n+b_1x^{n-1}+\ldots+b_{n-1}x+b_n \quad (b_i\in P)$$

е минималният полином на α над P, доколкото $p(\alpha)=0$, имаме

(1) $$\alpha^n=(-b_1)\alpha^{n-1}+(-b_2)\alpha^{n-2}+\ldots+(-b_{n-1})\alpha-(b_n)\cdot 1,$$

т. е. $\alpha^n\in T$.

Да допуснем, че $k>n$ и $\alpha^{k-1} \in T$. Тогава

$$\alpha^{k-1}=r_0 . 1+r_1\alpha+r_2\alpha^2+\ldots+r_{n-1}\alpha^{n-1},$$

където $r_0, r_1, \ldots, r_{n-1} \in P$. Умножаваме двете страни на последното равенство с α и получаваме

$$\alpha^k=r_0\alpha+r_1\alpha^2+\ldots+r_{n-1}\alpha^n.$$

Като заместим α^n с неговото равно от (1) и извършим приведение, ще получим, че α^k е линейна комбинация на $1, \alpha, \ldots, \alpha^{n-1}$ с коефициенти от P, т. е. $\alpha^k \in T$. Ако $a, b \in T$, то a и b са полиноми на α с коефициенти от P. Следователно ab е полином на α с коефициенти от P. Тъй като $\alpha^k \in T$, то $ab \in T$. С това свойство 1) е доказано.

Нека

$$a=\sum_{i=0}^{n-1} r_i\alpha^i \quad (r_i \in P)$$

е ненулев елемент от T. Полиномът $g(x)=r_0+r_1x+\ldots+r_{n-1}x^{n-1}$ е от $P[x]$ и е взаимно прост с $p(x)$, защото $p(x)$ е неразложим и има степен, по-голяма от степента на $g(x)$. Затова съществуват такива полиноми $u(x)$ и $v(x)$ от $P[x]$, че $u(x)g(x)+v(x)p(x)=1$.

Но тогава, като заместим x с α и вземем предвид, че $p(\alpha)=0$, получаваме $u(\alpha)g(\alpha)=1$, т. е. $u(\alpha)a=au(\alpha)=1$. Тъй като $u(\alpha)$ е полином на α с коефициенти от P, а степените на α са от T, то $u(\alpha)$ е елемент от T. Следователно $a^{-1}=u(\alpha)$ е от T и условието 2) е доказано.

С това показахме, че подпространството T, което се съдържа в $P(\alpha)$, е поле. Но T съдържа P и α и от минималността на $P(\alpha)$ следва, че $T=P(\alpha)$. Теоремата е доказана.

Следствие 5. *Ако n е степента на алгебричност на елемента α над P, то всеки елемент от $P(\alpha)$ се представя по единствен начин като полином на α от степен, по-ниска от n, с коефициенти от P.*

§ 4. Някои видове алгебрични разширения

Нека полето P е подполе на полето K. Ако всеки елемент от K е алгебричен над P, то K се нарича *алгебрично разширение* на P. В противен случай, т. е. когато поне един елемент от K е трансцендентен над P, K се нарича *трансцендентно разширение* на P.

Примери

1. Полето $\mathbf{C}$ на комплексните числа е алгебрично разширение на полето $\mathbf{R}$ на реалните числа, защото всяко комплексно число c е корен на полином от $\mathbf{R}[x]$ от степен 2 (например комплексното число c е корен на полинома $(x-c)(x-\bar{c})=x^2-(c+\bar{c})x+c\bar{c} \in \mathbf{R}[x]$).

2. Полето $P(x)$ на рационалните функции с коефициенти от полето P е трансцендентно разширение на полето P, тъй като елементът $x \in P(x)$ е трансцендентен над P.

Твърдение 7. *Всяко крайномерно разширение е алгебрично разширение.*

Доказателство. Нека K е крайномерно разширение на полето P и $n=[K:P]$, а β е произволен елемент от K. Елементите $1, \beta, \beta^2, \ldots, \beta^n$ са $n+1$ на брой и образуват линейно зависима система в n-мерното пространство K над P. Затова съществуват елементи $p_0, p_1, \ldots, p_n$ от P, поне един от които е различен от нула, за които е изпълнено равенството

$$p_0 . 1 + p_1\beta + p_2\beta^2 + \ldots + p_n\beta^n = 0.$$

Оказа се, че елементът β е корен на ненулевия полином $f(x)=p_0+p_1x+\ldots+p_nx^n$ от $P[x]$, т. е. β е алгебричен над P. С това доказахме, че всеки елемент от K е алгебричен над P.

От теорема 3 и от доказаното твърдение се получава следното

Следствие 6. *Всяко просто алгебрично разширение е алгебрично разширение.*

Следствие 7. *Ако K е крайномерно разширение на полето P и $n=[K:P]$, то степента на алгебричност над P на всеки елемент от K е делител на n и затова не надминава n.*

Доказателство. Нека β е произволен елемент от K. Съгласно твърдение 7 β е алгебричен елемент над P. Нека m е степента на алгебричност над P на елемента β, а $P(\beta)$ е простото алгебрично разширение, получено с присъединяването на β към P. По теорема 3 имаме равенството $m=[P(\beta):P]$. Тъй като $P \subseteq P(\beta) \subseteq K$, по теорема 2 изпълнено е равенството $[K:P] = [K:P(\beta)][P(\beta):K]$, т. е. $n=[K:P(\beta)]\,m$ и затова m е делител на n. Следствието е доказано.

Твърдение, обратно на твърдение 7, невинаги е вярно, т. е. не всяко алгебрично разширение е крайномерно.

Ще въведем още два типа разширения, за които ще докажем, че съвпадат с крайномерните разширения.

Нека K е разширение на полето P, а $\alpha_1, \alpha_2, \ldots, \alpha_s$ са елементи от K. Най-малкото подполе на K, което съдържа P и елементите $\alpha_1, \alpha_2, \ldots, \alpha_s$, се бележи с $P(\alpha_1, \alpha_2, \ldots, \alpha_s)$ и се нарича разширение на P, получено с присъединяването на елементите $\alpha_1, \alpha_2, \ldots, \alpha_s$ към P. Ако $\alpha_1, \ldots, \alpha_s$ са алгебрични елементи над P, то $P(\alpha_1, \ldots, \alpha_s)$ се нарича *алгебрично породено разширение* на P, получено чрез присъединяване на $\alpha_1, \ldots, \alpha_s$ към P.

Очевидно е, че понятието просто алгебрично разширение е частен случай на понятието алгебрично породено разширение.

Разширението K на полето P се нарича *съставно алгебрично разширение*, ако съществува крайна редица от вложени едно в друго подполета на K:

$$(1) \qquad P = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_{m-1} \subseteq L_m = K,$$

която започва с P, завършва с K и в която всяко подполе L_i е просто алгебрично разширение на предишното L_{i-1}. Ако $L_i = L_{i-1}(\beta_i)$, $i = 1, 2, \ldots, m$, то съставното разширение K ще означаваме с $P(\beta_1)(\beta_2)\ldots(\beta_m)$. С други думи, съставното алгебрично разширение е поле, построено от краен брой последователно взети прости алгебрични разширения.

Теорема 4. *Нека K е разширение на полето P. Следните три твърдения са еквивалентни:*

(i) K е крайномерно разширение на P;

(ii) K е алгебрично породено разширение на P;

(iii) K е съставно алгебрично разширение на P.

Доказателство. $(i) \Rightarrow (ii)$. Нека K е произволно крайномерно разширение на P и $\alpha_1, \alpha_2, \ldots, \alpha_n$ е произволен базис на K над P. Според твърдение 7 елементите $\alpha_1, \alpha_2, \ldots, \alpha_n$ са алгебрични над P. Да разгледаме алгебрично породеното разширение $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Ясно е, че $P(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K$. Тъй като всеки елемент β от K е линейна комбинация от вида $\beta = \sum_{i=1}^{n} p_i \alpha_i$ $(p_1, p_2, \ldots, p_n \in P)$, а $\alpha_i \in P(\alpha_1, \alpha_2, \ldots, \alpha_n)$, то всеки елемент от K е елемент от полето $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$, т. е. $K = P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ и K се оказва алгебрично породено разширение на P.

$(ii) \Rightarrow (iii)$. Нека $K = P(\beta_1, \beta_2, \ldots, \beta_m)$ е алгебрично породено разширение. Елементите $\beta_1, \beta_2, \ldots, \beta_m$ са алгебрични над P и затова те са алгебрични над всяко подполе на K, което съдържа P. Тогава да разгледаме редицата

$$P = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_{m-1} \subseteq L_m = M$$

от подполета на K, където $L_i = L_{i-1}(\beta_i)$, $i = 0, 1, \ldots, m-1$. Ще покажем, че съставното алгебрично разширение $M = P(\beta_1)\ldots(\beta_m)$ на P съвпада с K. Полето M е подполе на K и за да докажем равенството $K = M$, е достатъчно да покажем, че всеки елемент от K е елемент и от M. Но $K = P(\beta_1, \beta_2, \ldots, \beta_m)$ е най-малкото поле, което съдържа P и елементите $\beta_1, \beta_2, \ldots, \beta_m$. Затова всяко подполе на K, което съдържа P и елементите $\beta_1, \beta_2, \ldots, \beta_m$, ще съвпада с K. Очевидно подполето $M = P(\beta_1)(\beta_2)\ldots(\beta_m)$ съдържа P и елементите $\beta_1, \beta_2, \ldots, \beta_m$. Затова $K = M$ и K е съставно алгебрично разширение.

$(iii) \Rightarrow (i)$. Нека $K = P(\gamma_1)(\gamma_2)\ldots(\gamma_k)$ е съставно алгебрично разширение и

$$P = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_k = K,$$

където $L_i = L_{i-1}(\gamma_i)$, $i = 1, 2, \ldots, k$, е съответната редица от последователно вложени прости алгебрични разширения. Според теорема 3 за всяко $i = 1, 2, \ldots, k$ степента $[L_i : L_{i-1}]$ е крайна. Тогава според следствие 2 степента $[L_k : L_0] = [K : P]$ е също крайна. Следователно K е крайномерно разширение на P. Теоремата е доказана.

По този начин за следните пет класа разширения на дадено поле:

1) прости алгебрични разширения,
2) крайномерни разширения,
3) алгебрично породени разширения,
4) съставни алгебрични разширения,
5) алгебрични разширения,

показахме, че класът 1) се съдържа в класа 2), че класовете 2), 3) и 4) съвпадат и се съдържат в класа 5), който (както ще видим по-късно) е по-широк, защото съдържа и някои безкрайномерни разширения. Остава неизяснен само въпросът за това, дали класът 4) не се изчерпва с простите алгебрични разширения. Без да даваме конкретен пример, само ще споменем, че в общия случай има съставни алгебрични разширения, които не са прости алгебрични. По-късно ще докажем, че във важния случай на полета с характеристика нула съставните алгебрични разширения са прости алгебрични разширения. Ще завършим този параграф със следната

Теорема 5. *Нека P е произволно поле, а K е разширение на P. Множеството L от всички елементи на полето K, които са алгебрични над P, е подполе на K. При това всеки елемент от K, който е алгебричен над L, се съдържа в полето L.*

Доказателство. Ясно е, че $P \subseteq L$. За да покажем, че L е подполе на K, трябва да покажем, че L има следните свойства:

a) ако $\alpha, \beta \in L$, то $\alpha+\beta$ и $\alpha-\beta$ са от L;

b) ако $\alpha, \beta \in L$, то $\alpha\beta \in L$;

c) ако $\alpha \in L$ и $\alpha \neq 0$, то $\alpha^{-1} \in L$.

Нека α и β са произволни елементи от L, т. е. α и β са алгебрични над P елементи от K. Да разгледаме алгебрично породеното разширение $M = P(\alpha, \beta)$. Тъй като M е алгебрично разширение на P, то подполето M на K се съдържа в L. Но $\alpha, \beta \in M$ и M е поле. Затова $\alpha \pm \beta$, $\alpha\beta$ и α^{-1} (при $\alpha \neq 0$) се съдържат в M. Тъй като $M \subseteq L$, то $\alpha \pm \beta$, $\alpha\beta$ и α^{-1} (при $\alpha \neq 0$) се съдържат и в L. Следователно L е подполе на K.

Нека τ е елемент от K, който е алгебричен над полето L, а

$$p(x) = x^n + l_1 x^{n-1} + \ldots + l_{n-1}x + l_n \quad (l_i \in L)$$

е минималният над L полином на τ. Да означим с N алгебрично породеното разширение $P(l_1, l_2, \ldots, l_n)$ на P. Тъй като коефициентите на $p(x)$ се съдържат в N, то τ ще бъде алгебричен и над N и можем да образуваме простото алгебрично разширение $N(\tau)$ на N. Според теорема 3 степента $[N(\tau) : N]$ е крайна. Понеже N е алгебрично породено разширение на P, съгласно теорема 4 и степента $[N : P]$ е крайна. Тогава според теорема 2 полето $N(\tau)$ е крайномерно разширение на P. Тъй като $\tau \in N(\tau)$ и $N(\tau)$ е алгебрично разширение на P (твърдение 7), то τ е алгебричен елемент над P. Следователно елементът τ се съдържа в L. Теоремата е доказана.

§ 5. Съществуване на разширение на основното поле, в което даден полином има корен

Неиа $f(x)$ е полином с коефициенти от полето P. Полиномът $f(x)$ може да няма корени в полето P. Например полиномът x^2+1 с коефициенти от полето R на реалните числа няма корен в R, но има корени в полето C на комплексните числа, което е разширение на R. Така възниква следният въпрос: дали за всеки полином $f(x)$ с коефициенти от полето P, степента на който е положителна, може да се намери разширение на P, което да съдържа поне един корен на $f(x)$?

Ще разгледаме първо случая, когато полиномът $f(x)=p(x)$ е неразложим над P нормиран полином от степен $n\geqq 1$.

Да допуснем, че разширението K на полето P съдържа корен α на полинома $p(x)$, т. е. $\alpha\in K$ и $p(\alpha)=0$. Тъй като α е корен на $p(x)$ и $p(x)$ е нормиран и неразложим над P, то минималният полином на α над P ще бъде полиномът $p(x)$. Да разгледаме подполето $P(\alpha)$ на K. Както показахме в § 3, простото алгебрично разширение $P(\alpha)$ има степен над P, равна на n, и всеки негов елемент се представя еднозначно като полином на α от степен, по-малка от n, с коефициенти от P. Най-напред ще докажем следното

Твърдение 8. *Нека $P(\alpha)$ е просто алгебрично разширение на полето P, а $I=(p(x))$ е главният идеал на пръстена $P[x]$, породен от минималния полином $p(x)$ над полето P на елемента α. Тогава фактор-пръстенът $P[x]/I$ е поле, което е изоморфно на полето $P(\alpha)$.*

Доказателство. Тъй като $P(\alpha)$ е поле, достатъчно е да установим, че $P(\alpha)$ и $P[x]/I$ са изоморфни като пръстени.

Да разгледаме изображението $\varphi: P[x]\to P(\alpha)$, което на произволен полином $f(x)$ от $P[x]$ съпоставя елемента $f(\alpha)$ от $P(\alpha)$, т. е.

$$\varphi(f(x))=f(\alpha),\ f(x)\in P[x].$$

Лесно се проверява, че е изпълнено равенството $\varphi[f(x)+g(x)]=\varphi(f(x))+\varphi(g(x))$, а също така и равенството $\varphi(f(x)\,g(x))=\varphi(f(x))\varphi(g(x))$. Следователно изображението φ е хомоморфизъм. Понеже всеки елемент от $P(\alpha)$ е полином на α с коефициенти от P, то φ е хомоморфизъм на $P[x]$ върху $P(\alpha)$.

Ще покажем, че ядрото $\ker\varphi$ на хомоморфизма φ съвпада с идеала $I=(p(x))$. Наистина полиномът $f(x)$ от пръстена $P[x]$ принадлежи на ядрото $\ker\varphi$ точно тогава, когато α е корен на $f(x)$. Но съгласно твърдение 4 равенството $f(\alpha)=0$ е възможно тогава и само тогава, когато $p(x)$ дели $f(x)$, което е еквивалентно с условието $f(x)$ да принадлежи на идеала I. Сега прилагаме теоремата за хомоморфизмите на пръстени и доказателството е завършено.

Доказаното просто твърдение ни подсказва пътя за решаване на поставения по-горе въпрос.

Нека неразложимият нормиран полином $p(x)$ с коефициенти от полето P няма корени в P. Тогава означаваме с $P[y]$ пръстена на полиномите на променливата y и разглеждаме фактор-пръстена $L=P[y]/I$ на пръстена $P[y]$ по идеала $I=(p(y))$, породен от полинома $p(y)$. Ясно е, че $p(y)$ е също неразложим. Най-напред ще докажем, че L е поле, т. е. че всеки негов ненулев елемент притежава обратен.

Действително нека $f(y)+I$ е произволен ненулев елемент от L. Това означава, че неразложимият полином $p(y)$ не дели $f(y)$ и следователно $p(y)$ и $f(y)$ са взаимно прости. Тогава ще съществуват такива полиноми $u(y)$ и $v(y)$ с коефициенти от P, че $u(y)f(y)+v(y)p(y)=1$. Оттук получаваме, че $1+I=u(y)f(y)+v(y)p(y)+I=u(y)f(y)+I=[u(y)+I].[v(y)+I]$, където във второто равенство сме използували факта, че $v(y)p(y)\in I$. Следователно съседният клас $u(y)+I$ от L е обратен на ненулевия елемент $f(y)+I$.

Очевидно е, че подмножеството $P'=\{a+I|a\in P\}$ на фактор-пръстена $L=P[y]/I$, състоящо се от всички съседни класове от вида $a+I$ $(a\in P)$, образува подполе на полето L. Освен това изображението $\psi: P\to P'$, което на всеки елемент a от полето P съпоставя елемента $\psi(a)=a+I$ от полето P', е изоморфизъм между P и P' (защо?). Този изоморфизъм ни дава основание да отъждествяваме съответните елементи от P и P' или, както се казва още, да вложим полето P в полето L. (Например полето на реалните числа $\mathbf{R}$ е вложено в полето на комплексните числа $\mathbf{C}$ чрез отъждествяване на всяко комплексно число от вида $a+0i$ с реалното число a.) Следователно можем да считаме, че полето L е разширение на полето P и по такъв начин дадения полином $p(x)$ ще разглеждаме като полином с коефициенти от L. Ще докажем, че елементът $\alpha=y+I$ от полето L е корен на полинома $p(x)$. Наистина нека $p(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ $(n\geqq 1)$, където коефициентите $a_1, a_2, \ldots, a_n$ са от полето P. Разглеждан като полином от $L[x]$, $p(x)$ ще има представянето $p(x)=(1+I)x^n+(a_1+I)x^{n-1}+\ldots+(a_{n-1}+I)x+(a_n+I)$. Тогава

$$\begin{aligned} p(\alpha) &= (1+I)(y+I)^n+(a_1+I)(y+I)^{n-1}+\ldots \\ &\quad +(a_{n-1}+I)(y+I)+(a_n+I) \\ &= (y^n+I)+(a_1y^{n-1}+I)+\ldots+(a_{n-1}y+I)+(a_n+I) \\ &= p(y)+I=I, \end{aligned}$$

т. е. стойността $p(\alpha)$ съвпада с нулевия елемент I на полето L, а това означава, че α е корен на $p(x)$.

Задача. Докажете, че L е просто алгебрично разширение на полето P и $L=P(y+I)$.

Дотук доказахме, че за всеки неразложим над P полином $p(x)$ съществува разширение на P, което съдържа корен на $p(x)$.

Нека сега $f(x)$ е произволен полином от положителна степен

и с коефициенти от P. Тогава $f(x)$ ще се дели поне на един неразложим над P полином $p(x)$. Ако L е разширение на P, което съдържа корен на $p(x)$, този корен ще бъде корен и на полинома $f(x)$. Така получихме следната теорема, която отговаря положително на поставения в началото въпрос.

Теорема 6. *Нека P е произволно поле, а $f(x)$ е полином с коефициенти от P, степента на който е положителна. Тогава съществува разширение на полето P, което съдържа поне един корен на полинома $f(x)$.*

Нека σ е изоморфизъм на полето P върху полето F. За удобство образът в F на елемента a от P ще бележим с a^σ. Изоморфизмът σ се разширява по естествен начин до изоморфизъм на пръстена $P[x]$ върху пръстена $F[x]$. А именно полагаме образа на полинома $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ да бъде полиномът $a_0^\sigma x^n+a_1^\sigma x^{n-1}+\ldots+a_{n-1}^\sigma x+a_n^\sigma$ от $F[x]$, който полином ще означим с $f^\sigma(x)$. Лесно се вижда, че ако $f(x)$ е неразложим над полето P, то $f^\sigma(x)$ е неразложим над полето F и, обратно, от неразложимостта на $f^\sigma(x)$ над F следва неразложимостта на $f(x)$ над P.

Теорема 7. *Нека σ е изоморфизъм на полето P върху полето F, а $f(x)$ е нормиран неразложим полином над P и $f^\sigma(x)$ е неговият образ в $F[x]$. Нека $K=P(\alpha)$ и $L=F(\beta)$ са два прости алгебрични разширения съответно на P и F, при което $f(\alpha)=0$ и $f^\sigma(\beta)=0$. Тогава изоморфизмът σ може да се продължи до изоморфизъм на K върху L, при който α се изобразява в β.*

Доказателство. Очевидно е, че $f(x)$ е минималният полином на α над P, а $f^\sigma(x)$ е минималният полином на β над F. Всеки елемент a от $K=P(\alpha)$ се записва еднозначно във вида $a=h(\alpha)$, където $h(x)$ е полином от $P[x]$ от степен, по-малка от степента на $f(x)$. Затова изображението ψ, което се определя с равенството $a^\psi=h^\sigma(\beta)$, е коректно дефинирано и продължава σ, т. е. за $a\in P$ имаме $a^\psi=a^\sigma$. Освен това очевидно е, че $\alpha^\psi=\beta$.

Всеки елемент b от $F(\beta)$ се записва във вида $b=c_0+c_1\beta+\ldots+c_{n-1}\beta^{n-1}$ $(c_i\in F)$, където $n=\deg f^\sigma(x)=\deg f(x)$. Тъй като σ е изоморфизъм на P върху F, то съществуват такива елементи $p_0, p_1, \ldots, p_{n-1}$ от P, че $p_i^\sigma=c_i$ за всяко $i=0, 1, \ldots, n-1$. Тогава елементът $a=p_0+p_1\alpha+\ldots+p_{n-1}\alpha^{n-1}$ от K се изобразява при ψ в елемента b. Следователно ψ е изображение на K върху L.

Нека $a=h(\alpha)$ и $d=g(\alpha)$ са два елемента от K, където $h(x)$ и $g(x)$ са полиноми от $P[x]$ от степени, по-малки от n. Полиномът $h(x)+g(x)$ има степен, по-малка от n, и затова $(a+d)^\psi=(h+g)^\sigma(\beta)=h^\sigma(\beta)+g^\sigma(\beta)=a^\psi+b^\psi$, т. е. ψ изобразява дадена сума в сума от съответните образи на събираемите.

Нека

$$h(x)\,g(x)=q(x)\,f(x)+r(x),\ \deg r(x)<n.$$

Тогава $h^\sigma(x)\,g^\sigma(x)=q^\sigma(x)\,f^\sigma(x)+r^\sigma(x)$, тъй като изображението

на $P[x]$ в $F[x]$, което продължава σ, е изоморфизъм на $P[x]$ вър-
ху $F[x]$. Освен това $\deg r^\sigma(x)=\deg r(x)<n$. Следователно според твърдение 8 ще имаме $(ad)^\psi=r^\psi(\alpha)=r^\sigma(\beta)=h^\sigma(\beta)g^\sigma(\beta)=a^\psi d^\psi$, т. е. ψ изобразява дадено произведение в произведение от образите на съответните множители. С това доказахме, че изображението ψ е изоморфизъм на полето K върху полето L, който продължава σ и изобразява α в β.

Доказаната теорема при $P=F$ и тъждественото изображение σ показва, че устройството на разширението на P, получено чрез присъединяване на корен на един неразложим полином, съвсем не зависи от конкретното построяване на този корен. В частност от тази теорема следва единствеността на полето **C** на комплексните числа: *както и да разширяваме полето* **R** *от реалните числа чрез присъединяване на корен на полинома* x^2+1, *с точност до изоморфизъм получаваме едно и също поле.*

§ 6. Поле на разлагане

Нека $g(x)$ е полином над полето P, а K е разширение на P, над което полиномът $g(x)$ се разлага в произведение на линейни множители, т. е.

$$g(x)=a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_m),$$

където $a(a\in P)$ е старшият коефициент на $g(x)$, а $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$. Най-малкото междинно поле, над което $g(x)$ може да се разложи на линейни множители, е алгебрично породеното разширение $P(\alpha_1, \alpha_2, \ldots, \alpha_m)$ и това поле се нарича *поле на разлагане* на полинома $g(x)$ над полето P.

Ако L е друго разширение на полето P, над което $g(x)$ се разлага във вида $g(x)=a(x-\beta_1)(x-\beta_2)\ldots(x-\beta_m)$, то $P(\beta_1, \beta_2, \ldots, \beta_m)$ ще бъде друго поле на разлагане на полинома $g(x)$. Ще покажем, че двете полета на разлагане на $g(x)$ над P с точност до изоморфизъм са едно и също разширение на полето P.

Трябва да подчертаем, че понятието поле на разлагане на даден полином $g(x)$ съществено зависи от това, над кое поле се разглежда този полином. Например полето на разлагане на полинома x^2+1 над полето **Q** е полето $\mathbf{Q}(i)$ на гаусовите числа, а полето на разлагане на същия полином над **R** е полето **C** на комплексните числа.

Съществуването на поле на разлагане за всеки полином се установява по следния начин. Нека $g(x)$ е произволен полином от положителна степен и с коефициенти от полето P. Съгласно теорема 6 съществува разширение L_1 на полето P, което съдържа корен α_1 на $g(x)$. Над полето L_1 полиномът $g(x)$ се разлага във вида $g(x)=(x-\alpha_1)g_1(x)$. Разширяваме полето L_1 до поле L_2, което съдържа корен α_2 на полинома $g_1(x)$. Над L_2 полиномът $g(x)$ се разлага във вида $g(x)=(x-\alpha_1)(x-\alpha_2)g_2(x)$. По същия начин разширяваме полето L_2 до полето L_3, което съдържа корен α_3 на $g_2(x)$ и т. е. Степента на всеки от полиномите $g(x), g_1(x), g_2(x), \ldots$

е с единица то-малка от степента на предхо-ждащия го и затова посоченият процес ще завърши след краен брой стъпки, т. е. ще стигнем до полином от нулева степен, а за $g(x)$ получаваме поле, над което той се разлага на линейни множители. Същите разсъждения показват, че всеки ненулев полином от n-та степен има в едно поле L не повече от n на брой корена и този брой е равен на n точно тогава, когато L съдържа поле на разлагане на дадения полином. Така установихме следната

Теорема 8. *За всеки полином $g(x)$ над едно поле P съществува поле на разлагане. Във всяко разширение K на P ненулевият полином $g(x)$ от n-та степен има не повече от n на брой корена и K съдържа поле на разлагане на $g(x)$ над P точно тогава, когато $g(x)$ има n корена в K (броени с техните кратности).*

Да преминем сега към въпроса за единствеността на полето на разлагане на един полином над дадено поле. Този въпрос се решава от следната

Теорема 9. *Нека σ е изоморфизъм на полето P върху полето F, а $g(x)$ е полином от $P[x]$ и $g^\sigma(x)$ е съответният му полином от $F[x]$. Нека E е поле на разлагане на $g(x)$ над P, а G е поле на разлагане на $g^\sigma(x)$ над F. Тогава съществува изоморфизъм ψ на полето E върху полето G, който разширява изоморфизма σ, т. е. ограничението на ψ върху подполето P на E съвпада със σ.*

Доказателство. Нека

$$g(x)=a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_m)$$

е разлагането на $g(x)$ на линейни множители над E. Тъй като E е поле на разлагане на $g(x)$, то $E=P(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

Ако $\alpha_1, \alpha_2, \ldots, \alpha_m$ се съдържат в P, то $E=P$ и тогава, като приложим изоморфизма σ направо към написаното разлагане на $g(x)$, ще получим

$$g^\sigma(x)=a^\sigma(x-\alpha_1^\sigma)(x-\alpha_2^\sigma)\ldots(x-\alpha_m^\sigma),$$

което е разлагане на $g^\sigma(x)$ на линейни множители над полето F. Затова $G=F$ и в разглеждания частен случай $\psi=\sigma$ и теоремата е доказана.

Нека k е броят на корените на $g(x)$, които лежат вън от полето P. Видяхме, че ако $k=0$, твърдението на теоремата е вярно.

Нека $k\geqq 1$. Да допуснем, че теоремата е доказана за всички случаи, когато имаме $l(l<k)$ корена вън от P. Нека например коренът α_1 не лежи в P, а $f(x)$ е минималният полином на α_1 над P. Тогава $g(x)=f(x)\,h(x)$, където $h(x)\in P[x]$. Като приложим σ към написаното разлагане на $g(x)$, получаваме $g^\sigma(x)=f^\sigma(x)\,h^\sigma(x)$. Тъй като $f(x)$ е неразложим над P, полиномът $f^\sigma(x)$ ще бъде неразложим полином над F. Освен това полиномът $f^\sigma(x)$ има корен β_1 в G, защото неговите корени са корени и на $g^\sigma(x)$, а G е

поле на разлагане на $g^\sigma(x)$. Според теорема 7 изоморфизмът σ се продължава до изоморфизъм τ на полето $P_1=P(\alpha_1)$ върху полето $F_1=F(\beta_1)$. Разглеждаме сега полинома $g(x)$ като полином над полето P_1. Ясно е, че $g^\tau(x)=g^\sigma(x)$ и че E и G са полета на разлагане съответно на $g(x)$ и $g^\sigma(x)$ над P_1 и F_1. Сега полето P_1 съдържа в повече поне един корен α_1 на полинома $g(x)$. По предположението на индукцията изоморфизмът τ се разширява до изоморфизъм ψ на полето E върху полето G. Тъй като τ е продължение на σ, ψ е продължение на τ, то ψ е продължение на σ. Наистина нека $a\in P$. Тъй като τ продължава σ, то $a^\tau=a^\sigma$. Но $a\in P\subseteq P_1$ и ψ разширява τ. Затова $a^\psi=a^\tau$ и двете равенства ни дават $a^\psi=a^\sigma$, т. е. ограничението на ψ върху P съвпада с първоначално дадения изоморфизъм σ. Теоремата е доказана.

Следствие 8. *Нека $g(x)$ е произволен полином над полето P. Тогава всеки две полета на разлагане на полинома $g(x)$ над P са изоморфни.*

Следствието се получава директно от доказаната теорема, като се положи $P=F$ и за σ се вземе тъждественият изомофизъм, т. е. $a^\sigma=a$ за всяко $a\in P$.

Ще завършим този параграф с няколко бележки, които се отнасят до понятията производна и многократен корен на даден полином.

Въз основа на последното следствие можем просто да казваме „поле на разлагане на полинома $g(x)$ над полето P“, без да конкретизираме за кое поле на разлагане на $g(x)$ над P става дума, тъй като всеки две такива полета на разлагане са изоморфни.

Ако P е произволно поле, а

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$$

е произволен полином над P, то полиномът

$$na_0x^{n-1}+(n-1)\,a_1x^{n-2}+\ldots+2a_{n-2}x+a_{n-1}$$

се нарича първа производна на полинома $f(x)$ и се означава с $f'(x)$. Производната на полинома с числови коефициенти определихме по същия начин в § 4 на глава II. Там често използувахме факта, че производната на полином с числови коефициенти и от положителна степен е ненулев полином. Ако полето P има положителна характеристика p, може да се случи производната на ненулев полином от положителна степен да е равна на нула. Например полиномът x^p+1 над поле с характеристика p има първа производна $px^{p-1}=(p\cdot 1)\,x^{p-1}=0\cdot x^{p-1}=0$. Обаче в случая на полета с нулева характеристика връзката между многократните корени и производната на даден полином си остава същата. Не е трудно да се повторят разсъжденията от § 4 на глава II и да се получат съответните твърдения за полином над произволно поле с характеристика, равна на нула.

Твърдение 9. *Нека P е произволно поле с характеристика 0, а $f(x)$ е неразложим полином над P. Тогава $f(x)$ няма многократни корени.*

Доказателство. Нека $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ ($a_i \in P$). Понеже $f(x)$ е неразложим над P, то $n>0$. Тъй като $a_0\neq 0$, $n\neq 0$ и полето P има характеристика нула, то $na_0\neq 0$. Следователно производната $f'(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\ldots+2a_{n-2}x+a_{n-1}$ е ненулев полином от степен $n-1$.

Неразложимият полином $f(x)$ има степен, по-висока от степента на ненулевия полином $f'(x)$, и затова $f(x)$ и $f'(x)$ са взаимно прости. Следователно съществуват такива полиноми $u(x)$ и $v(x)$ от $P[x]$, че е изпълнено равенството

$$u(x)f(x)+v(x)f'(x)=1.$$

Ако сега α е корен на $f(x)$ от някое разширение L на P като заместим x с α в горното равенство, получаваме

$$1=u(\alpha)f(\alpha)+v(\alpha)f'(\alpha)$$
$$=u(\alpha).0+v(\alpha)f'(\alpha)=v(\alpha)f'(\alpha),$$

т. е. $f'(\alpha)\neq 0$. Затова никой корен на $f(x)$ не може да бъде корен на производната му $f'(x)$.

Да допуснем сега, че α е многократен корен на $f(x)$. Тогава $f(x)=(x-\alpha)^k g(x)$, където $k>1$ и $g(x)$ е полином над L. За производната на $f(x)$ получаваме

$$f'(x)=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^k g'(x)$$
$$=(x-a)^{k-1}[kg(x)+(x-\alpha)g'(x)],$$

тъдето $k-1>0$. Така α се оказва корен и на $f'(x)$, което противоречи на доказаното по-горе. Следователно всичките корени на $f(x)$ са еднократни (прости). Твърдението е доказано.

Задача. Ако $f(x)$ е полином над полето P и $f'(\alpha)\neq 0$ ($\alpha \in P$) то α не е многократен корен на $f(x)$.

§ 7. Крайни полета

Ако K е крайно поле, то неговата характеристика е равна на някое просто число p, а съгласно твърдение 3 броят $|K|$ на елементите на K е равен на p^n за някое естествено число n.

По такъв начин възниква въпросът, дали за всяко просто число p и за всяко естествено число n съществува крайно поле с p^n елемента. За $n=1$ положителен отговор на този въпрос дава полето Z_p на класовете остатъци по модул простото число p. Интересно е също да се установи дали две крайни полета с еднакъв брой елементи могат да бъдат неизоморфни. В този параграф ще дадем отговор на тези два въпроса.

Теорема 10. *Нека p е просто число, а n е произволно естествено число. Тогава полето на разлагане на полинома $f(x)=x^{p^n}-x$ над полето Z_p на класовете остатъци по модул p е крайно поле с $q=p^n$ елемента и е съставено само от корените на $f(x)$.*

Доказателство. Нека L е полето на разлагане на $f(x)$ над Z_p. Да означим с P множеството от корените на $f(x)$. Тъй като $f'(x)=qx^{q-1}-1=-1$, то $f(x)$ има само прости (еднократни) корени и P е подмножество на L с q различни елемента. Ще покажем, че P е подполе на L. Нека $\alpha\in P$ и $\beta\in P$. Понеже L е поле с характеристика p, то $(\alpha-\beta)^p=\alpha^p-\beta^p$. Затова $(\alpha-\beta)^q=(\alpha-\beta)^{p^n}=\alpha^q-\beta^q$. Тогава

$$f(\alpha-\beta)=(\alpha-\beta)^q-(\alpha-\beta)=\alpha^q-\beta^q-\alpha+\beta=$$
$$=f(\alpha)-f(\beta)=0-0=0,$$

т. е. $\alpha-\beta\in P$. Освен това ако $\beta\neq 0$, то $f(\alpha\beta^{-1})=(\alpha\beta^{-1})^q-\alpha\beta^{-1}=\alpha^q(\beta^q)^{-1}-\alpha\beta^{-1}=\alpha^q\beta^{-1}-\alpha\beta^{-1}=f(\alpha)\,\beta^{-1}=0\,.\beta^{-1}=0$, т. е. $\alpha\beta^{-1}\in P$. Съгласно твърдение 1 подмножеството P на L е подполе в L. Тъй като Z_p е простото подполе на L, $Z_p\subseteq P$. Подполето P на L съдържа Z_p и всички корени на полинома $f(x)$, а L е полето на разлагане на $f(x)$. Следователно $L=P$, с което теоремата е доказана.

Като обединим доказаните резултати, получаваме следното пълно описание на крайните полета.

Теорема 11. *Крайно поле с q елемента съществува тогава и само тогава, когато естественото число q е степен на някое просто число. Всеки две крайни полета с еднакъв брой елементи са изоморфни помежду си.*

Наистина от твърдение 3 и теорема 10 следва първата част на теоремата. Ако K и L са две крайни полета с $q=p^n$ елемента, то $p=\operatorname{char} K=\operatorname{char} L$. Нека P е простото подполе на K, а S е простото подполе на L. Тогава P и S са изоморфни на полето Z_p на класовете остатъци по модул p. Нека $\sigma: P\to S$ е изоморфизъм на P върху S. По теорема 10 K е полето на разлагане на $f(x)=x^q-x$ над P, а L е полето на разлагане на $f^\sigma(x)=x^q-x$ над S. По теорема 9 съществува изоморфизъм ψ на полето K върху полето L, който продължава изоморфизма σ. Следователно K и L са изоморфни.

§ 8. Теорема за примитивния елемент

В § 4 споменахме, че в общия случай с простите алгебрични разширения не се изчерпва класът на всички съставни алгебрични разширения на дадено поле. Но ако основното поле P има характеристика нула, класът на простите алгебрични разширения на P съвпада с класа на съставните алгебрични разширения на P. Тук целта ни е да докажем това твърдение, което е прието да се нарича теорема за примитивния елемент.

Теорема 12. *Ако полето P има характеристика нула, то всяко съставно алгебрично разширение на P е просто алгебрично разширение на P.*

Доказателство. Нека $K=P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$ е произволно съставно алгебрично разширение на P. От твърдение 7 и от тео-

рема 4 следва, че всеки елемент от K е алгебричен над P. Трябва да докажем, че в K има такъв елемент θ, че $K=P(\theta)$, т. е. че K е просто алгебрично разширение на P, получено с присъединяването на θ към P.

Ако $s=1$, то $K=P(\alpha_1)$ и можем да положим $\theta=\alpha_1$.

Да разгледаме случая, когато $s=2$, т. е. $K=P(\alpha_1)(\alpha_2)$. Нека $f(x)$ е минималният полином на α_1 над P, а $g(x)$ е минималният полином на α_2 над P. Тъй като $f(x)$ и $g(x)$ са неразложими над P, а полето P има характеристика нула; то от твърдение 9 следва, че $f(x)$ и $g(x)$ имат само еднократни корени. Нека L е полето на разлагане на полинома $f(x)g(x)$ над K. Тогава L ще съдържа както корените на $f(x)$, така и корените на $g(x)$. Нека $\beta_1=\alpha_1, \beta_2, \beta_3, \ldots, \beta_n$ $(n=\deg f(x))$ са корените в L на полинома $f(x)$, а $\gamma_1=\alpha_2, \gamma_2, \ldots, \gamma_m$ $(m=\deg g(x))$ са корените в L на полинома $g(x)$. Между елементите $\gamma_1, \gamma_2, \ldots, \gamma_m$ няма съвпадащи, защото $g(x)$ няма многократни корени. Затова можем да образуваме елементите

$$(\beta_i-\beta_1)(\gamma_1-\gamma_j)^{-1} \quad (i=1, 2, \ldots, n;\ j=2, 3, \ldots, m).$$

Тези елементи са $1+(n-1)(m-1)$ на брой. Полето P има характеристика нула и затова то съдържа безбройно много елементи. Следователно в P можем да намерим елемент c, който не съвпада с никой от посочените $1+(n-1)(m-1)$ на брой елементи, т. е.

$$c\neq\frac{\beta_i-\beta_1}{\gamma_1-\gamma_j} \quad (i=1, 2, \ldots, n;\ j=2, 3, \ldots, m).$$

Нека $\theta=\alpha_1+c\alpha_2=\beta_1+c\gamma_1$. Тъй като $c\in P$, а $\alpha_1, \alpha_2\in K$, то θ е елемент от K. Освен това θ не съвпада с никой от елементите $\beta_i+c\gamma_j$ $(i=1, 2, \ldots, n;\ j=2, 3, \ldots, m)$. Наистина, ако $\theta=\beta_i+c\gamma_j$ за някои i и j $(1\leqq i\leqq n,\ 2\leqq j\leqq m)$, получаваме

$$\beta_1+c\gamma_1=\beta_i+c\gamma_j,$$

т. е. $c=(\beta_i-\beta_1)(\gamma_1-\gamma_j)^{-1}$, което противоречи на избора на c.

Простото алгебрично разширение $P(\theta)$ е подполе на K. Ще покажем, че $K=P(\theta)$. За целта в полинома $f(x)$ заместваме x с $\theta-cx$ и получаваме полинома $h(x)=f(\theta-cx)$, който е с коефициенти от полето $P(\theta)$. Полиномът $g(x)$ има коефициенти от P, а P е подполе на $P(\theta)$. Следователно $g(x)$ и $h(x)$ са два полинома с коефициенти от полето $P(\theta)$. Елементът α_2 е корен на $g(x)$, защото $g(x)$ е минималният полином на α_2 над P. От друга страна, имаме $h(\alpha_2)=f(\theta-c\alpha_2)=f(\alpha_1)=0$, т. е. α_2 е общ корен на $h(x)$ и $g(x)$.

Нека $d(x)=(g(x), h(x))$ е най-големият общ делител на $g(x)$ и $h(x)$. Полиномът $d(x)$ е нормиран и коефициентите му са от $P(\theta)$. Ясно е, че общите корени на $g(x)$ и $h(x)$ и само те са корени на $d(x)$. Но $g(x)$ и $h(x)$ нямат други общи корени освен $\alpha_2=\gamma_1$. Наистина другите корени на $g(x)$ са $\gamma_2, \gamma_3, \ldots, \gamma_m$ и ако $h(\gamma_j)=0$ за някое j $(2\leqq j\leqq m)$, то

$$h(\gamma_j)=f(\theta-c\gamma_j)=0.$$

Тогава ще имаме $\theta-c\gamma_j=\beta_i$ за някое i. Отново получаваме, че $c=(\beta_i-\beta_1)(\gamma_1-\gamma_j)^{-1}$, което не е вярно. Следователно $d(x)$ има само един корен α_2, а понеже α_2 е еднократен корен на $g(x)$ и $d(x)/g(x)$, то нормираният полином $d(x)$ ще бъде равен на полинома $x-\alpha_2$. Полиномът $d(x)=x-\alpha_2$ е с коефициенти от $P(\theta)$ и затова $\alpha_2\in P(\theta)$. Тогава и $\alpha_1=\theta-c\alpha_2$ е също елемент от $P(\theta)$.

Дотук показахме, че елементите α_1 и α_2 се съдържат в полето $P(\theta)$ на K. Понеже $P\subseteq P(\theta)$ и $P(\alpha_1)$ е най-малкото подполе на K, което съдържа P и α_1, то $P(\alpha_1)$ е подполе на $P(\theta)$. По аналогични причини полето $P(\alpha_1)(\alpha_2)$ ще бъде подполе на $P(\theta)$, т. е. подполето $P(\theta)$ на полето K съдържа всеки елемент от полето $P(\alpha_1)(\alpha_2)=K$ и затова $K=P(\theta)$. С това теоремата е доказана за случая, когато $s=2$.

Нека $s>2$. Да допуснем, че теоремата е доказана за всяко съставно алгебрично разширение на полето P с нулева характеристика, което е получено от P с по-малко от s последователно взети прости алгебрични разширения.

Да означим с L_{s-1} подполето $P(\alpha_1)(\alpha_2)\ldots(\alpha_{s-1})$ на полето $K=P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$. По предположението на индукцията разширението L_{s-1} е просто алгебрично разширение на P, т. е. $L_{s-1}=P(\tau)$ за някой елемент τ от L_{s-1}. Тогава $K=L_{s-1}(\alpha_s)=P(\tau)(\alpha_s)$ и от доказаното по-горе следва, че съществува елемент θ от K такъв, че $K=P(\theta)$. Следователно полето $K=P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$ е просто алгебрично разширение на P. Теоремата е доказана.

§ 9. Квадратични радикални разширения

Ще казваме, че разширението L на полето P е *квадратично разширение* на P, ако $L=P$ или $L\neq P$, но степента $[L:P]$ на L над P е равна на 2.

Твърдение 10. *Нека P е произволно поле с характеристика, различна от 2. Разширението L на полето P е квадратично разширение на P тогава и само тогава, когато съществува такъв елемент θ от L, че $L=P(\theta)$ и θ^2 е от полето P.*

Доказателство. Ако $L=P(\theta)$, където $\theta^2\in P$, то θ е корен на полинома $x^2-\theta^2$ от $P[x]$. Затова минималният полином на θ над P ще бъде от степен, не по-голяма от 2, т. е. или $L=P$ (когато $\theta\in P$), или $[L:P]=2$, т. е. L е квадратично разширение на P.

Нека L е квадратично разширение на P. Ако $L=P$, то можем да положим θ да бъде кой да е елемент от P. Затова да разгледаме случая, когато $[L:P]=2$. Нека β е елемент от L, който не се съдържа в P. Тогава простото алгебрично разширение $P(\beta)$ е подполе на L, което не съвпада с P. Затова $[P(\beta):P]>1$. Но степента $[P(\beta):P]$ е делител на степента $[L:P]=2$ и затова $[P(\beta):P]=2=[L:P]$. Според следствие 4 ще бъде изпълнено ра-

венството $L=P(\beta)$. Минималният полином $p(x)$ на β над P ще има степен 2 и затова ще имаме $p(x)=x^2+bx+c$ ($b, c\in P$). Понеже β е корен на $p(x)$, то $c=-\beta^2-b\beta$. Нека $\theta=2\beta+b$. Тъй като $\beta\in L$ и $b\in P\subset L$, то θ е елемент от L. Елементът θ не се съдържа в P, защото характеристиката на P е различна от 2 и β не е елемент от P. От разсъжденията, които проведохме по-горе, следва, че $L=P(\theta)$. Остава ни да проверим, че $\theta^2\in P$. Но

$$\theta^2=(2\beta+b)^2=4(\beta^2+b\beta)+b^2=-4c+b^2$$

е елемент от P, с което твърдението е доказано.

Определение 4: Разширението K на полето P се нарича *квадратично радикално разширение* на P, ако съществува такава редица

$$P=L_0\subseteq L_1\subseteq L_2\subseteq \ldots \subseteq L_{m-1}\subseteq L_m=K$$

от краен брой подполета, последователно вложени едно в друго, че всяко подполе L_i е квадратично разширение на предхождащото го поле L_{i-1} ($i=1, 2, \ldots, m$).

Твърдение 11. *Ако K е квадратично разширение на полето P, то K е крайномерно разширение на P и неговата степен над P е равна на някоя степен на числото 2.*

Наистина от P до K има крайна редица

$$P=L_0\subseteq L_1\subseteq \ldots \subseteq L_m=K$$

от подполета, където L_i е квадратично разширение на L_{i-1} ($i=1, 2, \ldots, m$). Тогава $[L_i:L_{i-1}]=2^{\nu_i}$ ($\nu_i=0, 1$) и затова $[K:P]=[L_m:L_{m-1}]\cdot[L_{m-1}:L_{m-2}]\ldots[L_1:L_0]=2^{\nu}$, където $\nu=\nu_1+\nu_2+\ldots+\nu_m$

Следствие 9. *Нека K е квадратично радикално разширение на полето P. Тогава степента на алгебричност над P на всеки елемент от K е равна на степен на числото 2.*

Действително по предишното твърдение имаме $[K:P]=2^{\nu}$, $\nu\geqq 0$. Числото 2^{ν} се дели само на степени на 2. Тъй като степента на алгебричност над P на всеки елемент от K е делител на $[K:P]=2^{\nu}$, то тази степен е равна на степен на числото 2.

Следствие 10. *Нека $f(x)$ е нормиран неразложим над полето P полином от n-та степен. Тогава ако числото n не е степен на 2, то никое квадратично радикално разширение на P не може да съдържа корен на полинома $f(x)$.*

Наистина ако някое квадратично радикално разширение на полето P съдържа корен α на полинома $f(x)$, то α по предишното следствие ще има степен на алгебричност над P, равна на някоя степен на числото 2. Тъй като $f(\alpha)=0$ и $f(x)$ е нормиран неразложим над P полином, то $f(x)$ е минималният полином над P на елемента α, т. е. степента на алгебричност на α над P е равна на n и n не е степен на 2. Полученото противоречие показва, че никой корен на $f(x)$ не се съдържа в квадратично радикално разширение на P.

Твърдение 11. *Нека L е квадратично радикално разшире-*

ние на полето P, а K е квадратично радикално разширение на полето L. Тогава K е квадратично радикално разширение на полето P.

Доказателство. По условие съществуват редиците

$$P=N_0\subseteq N_1\subseteq \ldots \subseteq N_m=L,\ L=M_0\subseteq M_1\subseteq \ldots \subseteq M_n=K, \quad (1)$$

където N_i е квадратично разширение на N_{i-1}, а M_j е квадратично разширение на M_{j-1} ($i=1, \ldots, m$; $j=1, \ldots, n$). Тогава от P до K имаме редица от подполета

$$P=N_0\subseteq N_1\subseteq \ldots \subseteq N_m=M_0\subseteq M_1\subseteq \ldots \subseteq M_n=K,$$

където всяко подполе е квадратично разширение на предхождащото го. Следователно K е квадратично радикално разширение на полето P.

§ 10. Алгебрически затворени полета

Твърдение 12. *Нека P е подполе на полето L, а L е подполе на полето K. За да бъде полето K алгебрично разширение на полето P, е необходимо и достатъчно L да е алгебрично разширение на P, а K да е алгебрично разширение на L.*

Доказателство. Необходимост. Нека K е алгебрично разширение на P. Тъй като всеки елемент от K е алгебричен над P и $L\subseteq K$, то L е алгебрично разширение на P. Освен това според твърдение 5 всеки елемент от K е алгебричен и над L, т. е. K е алгебрично разширение на L.

Достатъчност. Нека K е алгебрично разширение на L, а L е алгебрично разширение на P. Нека α е произволен елемент от K и $p(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ ($a_i\in L$) е минималният полином на α над L. Коефициентите $a_1, a_2, \ldots, a_n$ на $p(x)$ са от L и затова са алгебрични елементи над P. Следователно можем да образуваме съставното алгебрично разширение $M=P(a_1)(a_2)\ldots(a_n)$. Тъй като $p(x)\in M[x]$, то α е алгебричен елемент над полето M и $M(\alpha)$ е просто алгебрично разширение. Полето $M(\alpha)$ е съставно алгебрично разширение на P, понеже $M(\alpha)=P(a_1)(a_2)\ldots(a_n)(\alpha)$; и затова съгласно теорема 4 $M(\alpha)$ е крайномерно разширение на P. Но тогава според твърдение 7 полето $M(\alpha)$ е алгебрично разширение на P и понеже $\alpha\in M(\alpha)$, то α е алгебричен елемент над P.

Твърдение 13. *Ако K е произволно поле, то следните четири свойства са еквивалентни:*

a) всеки полином от пръстена $K[x]$, степента на който е положителна, се разлага в произведение на полиноми от $K[x]$, степените на които са равни на единица;

b) всеки полином от положителна степен от пръстена $K[x]$ има поне един корен в полето K;

c) всеки неразложим полином над полето K е полином от първа степен;

d) всяко алгебрично разширение на K съвпада с K.

Доказателство. Нека $f(x)$ е полином от $K[x]$ и $n=\deg f(x)>0$. *a)⇒b).* Наистина ако полето K има свойството *a)*, то $f(x)=p_1(x)p_2(x)\ldots p_n(x)$, където $p_i(x)=a_ix+b_i$ $(a_i, b_i\in K)$ и $a_i\neq 0$ $(i=1, 2, \ldots, n)$. Елементите $-a_i^{-1}b_i$ $(i=1, 2, \ldots, n)$ са от полето K и са корени на полинома $f(x)$. Следователно полето K има свойството *b)*.

b) ⇒c). Нека полето K е със свойство *b)* и $p(x)$ е произволен неразложим над K полином. Тъй като степента на неразложимия полином $p(x)$ е положителна, то в K ще съществува поне един корен α на $p(x)$. Но тогава $x-\alpha$ е полином от $K[x]$ и $x-\alpha$ ще дели $p(x)$, т. е. $p(x)=(x-\alpha)q(x)$, където $q(x)$ е полином от $K[x]$. Тъй като $p(x)$ е неразложим над полето K, то $\deg q(x)=0$, т. е. $q(x)=\beta\in K$ и $p(x)=\beta(x-\alpha)$ е полином от първа степен.

c)⇒a). Нека полето K е със свойство *c)*. Пръстенът $K[x]$ е област на главни идеали (виж глава VI, § 2, пример 3 и твърдение 3), а простите елементи в този пръстен са неразложимите над K полиноми. Тогава според теорема 6 от глава VI всеки полином от положителна степен и с коефициенти от K се разлага в произведение на неразложими над K полиноми. Но полето K е със свойството *c)* и затова множителите от това разлагане са полиноми от първа степен. Следователно полето K е със свойство *a)*.

c)⇒d). Нека L е алгебрично разширение на K и K е със свойство *c)*. Ако $\alpha\in L$, то α е алгебричен над K и неговият минимален полином $p(x)$ над K е нормиран и неразложим над K. Понеже K е със свойството *c)*, полиномът $p(x)$ е от първа степен и затова $p(x)=x-\alpha$. Следователно елементът α като коефициент на $p(x)$ от $K[x]$ е от K. С това показахме, че всеки елемент от разширението L на полето K е елемент от K, т. е. $L=K$.

d)⇒c). Нека K е със свойството *d)*, а $p(x)$ е неразложим полином над K. Тъй като $\deg p(x)>0$, то според теорема 6 съществува разширение L на полето K, което съдържа корен α на полинома $p(x)$. Можем да считаме, че полето L съвпада с простото алгебрично разширение $K(\alpha)$. Тъй като $L=K(\alpha)$ е алгебрично разширение на K (виж следствие 6), а K е със свойството *d)*, то $L=K$ и затова $\alpha\in K$. Понеже α е корен на $p(x)$, то $p(x)=(x-\alpha)q(x)$, където $q(x)\in K[x]$. От неразложимостта на $p(x)$ над K следва, че $\deg q(x)=0$ и затова $\deg p(x)=1$, т. е. полето K е със свойство *c)*. Твърдението е доказано.

Определение 5. Полето K се нарича *алгебрически затворено*, ако то притежава едно от еквивалентните свойства *a)*, *b)*, *c)*, *d)*, формулирани в твърдение 13.

Примери

1. От теоремата на Даламбер за съществуване на корен на полином с числови коефициенти, която вече многократно използувахме и която ще докажем в следващия параграф, следва, че полето $\mathbf{C}$ на комплексните числа е алгебрически затворено.

2. Полето $\mathbf{Q}$ на рационалните числа и полето $\mathbf{R}$ на реалните числа не са алгебрически затворени полета.

3. Крайните полета не са алгебрически затворени. Наистина ако M е крайно поле и $a_1, a_2, \ldots, a_n$ са всичките му елементи то полиномът

$$f(x)=\prod_{i=1}^{n}(x-a_i)+1$$

е с коефициенти от M и $f(x)$ няма корен в M. От твърдение 13 следва, че полето M не е алгебрически затворено.

Теорема 13. *Ако P е подполе на алгебрически затвореното поле K, то множеството L от всички елементи на K, които са алгебрични над P, е алгебрически затворено поле.*

Доказателство. От теорема 5 знаем, че множеството L е подполе на K и че L съдържа всеки елемент от K, който е алгебричен над L. Нека $f(x)$ е произволен полином от положителна степен и с коефициенти от полето L. Тъй като $L \subseteq K$ и K е алгебрически затворено поле, то полиномът $f(x)$ има корен α в полето K. Но $f(x)$ е с коефициентите от полето L и затова α е алгебричен над L. Следователно елементът α се съдържа в L, т. е. $f(x)$ има корен в L и L е алгебрически затворено поле. Теоремата е доказана.

В теорията на полетата твърде важен е следният въпрос: ако P е произволно поле, съществува ли такова разширение K на полето P, което да е алгебрически затворено? Положителен отговор на този въпрос е получен от Щайниц. Теоремата на Щайниц ще приведем без доказателетво.

Теорема 14. *За всяко поле P съществува разширение K, което е алгебрически затворено поле.*

Доказателството на тази теорема може да се намери например в книгата на С. Ленг [16] (теорема 1, стр. 194).

Следствие 11. *За всяко поле P съществува алгебрично разширение L, което е алгебрически затворено.*

Действително съгласно теорема 14 съществува разширение K на P, което е алгебрически затворено поле. Ако с L означим множеството от всички елементи на K, които са алгебрични над P, то според теорема 13 L е алгебрически затворено поле. Очевидно е освен това, че L е алгебрично разширение на P.

Може да се докаже, че всеки две алгебрични разширения на едно поле P, които са алгебрически затворени полета, са изоморфни помежду си над полето P, т. е. между тези разширения на P има такъв изоморфизъм, който оставя елементите на P неподвижни. Този резултат, както и теоремата на Щайниц, се доказва с помощта на лемата на Цорн или на нейни еквивалентни твърдения (вж. [16], стр. 196).

§ 11. Доказателство на теоремата на Даламбер за съществуване на корен на полином с числови коефициенти

В § 5 на глава II вече се запознахме с теоремата на Даламбер и изведохме редица нейни следствия. Дотук неведнъж имахме възможност да се убедим във важността на тази теорема. В този параграф ще приведем едно от многото известни нейни доказателства. Всяко от тези доказателства в една или друга степен използува неалгебрични факти. Единствената причина, поради която излагаме доказателството така късно, е да сведем неалгебричната му част до минимум.

Лема 1. *Нека*

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\ (a_0\neq 0) \tag{1}$$

е произволен полином с реални коефициенти. Тогава — при всички достатъчно големи по абсолютна стойност реални стойности на x — знакът на полинома $f(x)$ съвпада със знака на неговия старши член a_0x^n.

Доказателство. Лемата ще бъде доказана, ако установим, че за всички достатъчно големи по абсолютна стойност реални значения на x е изпълнено неравенството

$$|a_0x^n|>|a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n|. \tag{2}$$

Нека $b=\max\{|a_1|, |a_2|,\ldots,|a_n|\}$. Тогава при всяка стойност на x, за която $|x|>1$, ще имаме

$$|a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n|\leqq|a_1||x|^{n-1}+\ldots+|a_n|$$
$$\leqq b(|x|^{n-1}+|x|^{n-2}+\ldots+|x|+1)\leqq b\frac{|x|^n-1}{|x|-1}<b\frac{|x^n|}{|x|-1}.$$

Неравенството (2) ще бъде изпълнено, ако

$$b\frac{|x|^n}{|x|-1}\leqq|a_0x^n|=|a_0||x|^n,$$

т. е. ако стойностите на x удовлетворяват условието

$$|x|\geqq\frac{b}{|a_0|}+1, \tag{3}$$

с което лемата е доказана.

От доказателството на тази лема се вижда, че неравенството (2) остава в сила и за комплексни коефициенти $a_0, a_1,\ldots,a_n$, при условие че комплексното число x удовлетворява неравенството (3). Следователно при горните означения получаваме следното

Следствие 12. *Всички комплексни корени на полинома $f(x)$ с комплексни коефициенти се намират в кръга*

$$|x|<\frac{b}{|a_0|}+1.$$

Преминаваме към разглеждането на лема, която по своя ректер се отнася към математическия анализ.

Лема 2. *Всеки полином от нечетна степен с реални коефициенти притежава поне един реален корен.*

Доказателство. Нека полиномът (1) е от нечетна степен и коефициентите му са реални числа. Старшият член a_0x^n на $f(x)$ при положителни и отрицателни стойности на x ще има различни знаци. Затова съгласно лема 1 при всички достатъчно големи по абсолютна стойност положителни и отрицателни реални стойности на x полиномът $f(x)$ също ще приема стойности с различни знаци. Следователно съществуват такива реални числа a и b $(a<b)$, че $f(a)$ и $f(b)$ са числа с различни знаци.

От курса по математичен анализ е известно, че полиномът $f(x)$ е непрекъсната функция и по едно от основните свойства на непрекъснатите функции, когато x се изменя между a и b, $f(x)$ ще приема поне по веднъж всички стойности, заключени между $f(a)$ и $f(b)$. Следователно съществува такова реално число c $(a<c<b)$, за което $f(c)=0$. Лемата е доказана.

Като използуваме понятията и резултатите от предишния параграф, можем да формулираме тооремата на Даламбер и по следния начин.

Теорема 15 (теорема на Даламбер). *Полето* **C** *на комплексните числа е алгебрически затворено.*

Доказателство. Трябва да докажем, че всеки полином с комплексни коефициенти от положителна степен притежава поне един комплексен корен. Доказателството ще разделим на две части — най-напред ще разгледаме полиноми с реални коефициенти, а след това — полиноми с комплексни коефициенти.

Нека $f(x)$ е произволен полином с реални коефициенти и неговата степен е $n=2^kq$, където q е нечетно число. Доказателството ще извършим по метода на пълната математична индукция по числото k. Ако $k=0$, то $f(x)$ е от нечетна степен и по предишната лема $f(x)$ има поне един реален корен.

Нека $k>0$. Да допуснем, че теоремата е доказана за всички полиноми с реални коефициенти, чиято степен се дели на 2^{k-1}, но не се дели на 2^k. Да означим с K полето на разлагане на полинома $f(x)$ над полето **C** на комплексните числа. Нека $\alpha_1, \alpha_2, \ldots, \alpha_n$ са корените на $f(x)$ в полето K. Ясно е, че $K=\mathbf{C}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Ще покажем, че поне един от елементите $\alpha_1, \alpha_2, \ldots, \alpha_n$ се съдържа в полето **C**. Нека r е произволно реално число. Образуваме всевъзможните елементи от вида

$$\beta_{ij}=\alpha_i\alpha_j+r(\alpha_i+\alpha_j),\ 1\leqq i<j\leqq n. \tag{3}$$

Ясно е, че β_{ij} са елементи от полето K и техният брой е равен на

$$\left(\frac{n}{2}\right)=\frac{n(n-1)}{2}=\frac{2^kq(2^kq-1)}{2}=2^{k-1}q_1,$$

където $q_1=q(2^kq-1)$ е нечетно число. Разглеждаме полинома

$$g(x)=\prod_{1\leqq i<j\leqq n}(x-\beta_{ij})$$

от степен $n_1=2^{k-1}q_1$, корените на който са елементите β_{ij} $(1\leqq \leqq i<j\leqq n)$ от K и следователно неговите коефициенти принадлежат на полето K. Коефициентите на g $x)$ са с точност до знак елементарните симетрични полиноми на елементите β_{ij}. Не е трудно да се види, че произволно разместване на корените $\alpha_1, \alpha_2, \ldots, \alpha_n$ води само до някакво разместване между елементите β_{ij}. Следователно коефициентите на $g(x)$ са симетрични полиноми на $\alpha_1, \alpha_2, \ldots, \alpha_n$ над полето R на реалните числа (понеже r е реално число). Съгласно основната теорема за симетричните полиноми коефициентите на $g(x)$ са полиноми с реални коефициенти на коефициентите на $f(x)$ и затова $g(x)$ е полином с реални коефициенти. Но степента на $g(x)$ се дели на 2^{k-1} и не се дели на 2^k. Следователно по индуктивното предположение полиномът $g(x)$ ще притежава поне един комплексен корен. По този начин при всеки избор на реалното число r може да се посочи такава двойка от индекси i и $j(1\leqq i<j\leqq n)$, която зависи от r, така че елементът $\alpha_i\alpha_j+r(\alpha_i+\alpha_j)$ е комплексно число. Понеже различните двойки индекси i, j са само краен брой, а реалните числа са безбройно много, то ще съществуват две различни реални числа r_1 и r_2, на които ще съответствува една и съща двойка индекси i и j, за които елементите

$$c=\alpha_i\alpha_j+r_1(\alpha_i+\alpha_j),\ d=\alpha_i\alpha_j+r_2(\alpha_i+\alpha_j)$$

са едновременно комплексни числа. От тези две равенства намираме, че

$$\alpha_i+\alpha_j=\frac{c-d}{r_1-r_2},\ \alpha_i\alpha_j=\frac{dr_1-cr_2}{r_1-r_2}\ (r_1\neq r_2).$$

Това означава, че α_i и α_j са корени на квадратното уравнение

$$(r_1-r_2)x^2+(d-c)x+(dr_1-cr_2)=0$$

с комплексни коефициенти. Но от формулите за корените на квадратното уравнение следва, че елементите α_i и α_j от K са комплексни числа. Така установихме, че разглежданият полином $f(x)$ с реални коефициенти има даже два комплексни корена и теоремата е доказана за полиномите от $R[x]$.

Нека полиномът (1) от положителна степен е с произволни комплексни коефициенти. Да означим с

$$\bar{f}(x)=\bar{a}_0x^n+\bar{a}_1x^{n-1}+\ldots+\bar{a}_{n-1}x+\bar{a}_n$$

полинома, получен от $f(x)$ чрез замяна на коефициентите му със съответните им комплексно спрегнати. Произведението

$$F(x)=f(x)\bar{f}(x)=b_0x^{2n}+b_1x^{2n-1}+\ldots+b_{2n-1}x+b_{2n},$$

където

$$b_k=\sum_{i+j=k} a_i\bar{a}_j\ (k=0,\ 1,\ 2,\ldots,\ 2n),$$

е полином с реални коефициенти, тъй като $\bar{b}_k=b_k$ за всяко k. Съгласно току-що доказаното полиномът $F(x)$ ще притежава комплексен корен β. Но от

$$F(\beta)=f(\beta)\,\bar{f}(\beta)=0$$

следва, че $f(\beta)=0$ или $\bar{f}(\beta)=0$. В първия случай β е комплексен корен на $f(x)$ и теоремата е доказана. Ако е изпълнено второто равенство, т. е.

$$\bar{f}(\beta)=\bar{a}_0\beta^n+\bar{a}_1\beta^{n-1}+\ldots+\bar{a}_{n-1}\beta+\bar{a}_n=0,$$

то като заменим в двете страни на последното равенство всяко число с неговото комплексно спрегнато, получаваме

$$a_0\bar{\beta}^n+a_1\bar{\beta}^{n-1}+\ldots+a_{n-1}\bar{\beta}+a_n=0,$$

т. е. $\bar{\beta}$ е комплексен корен на полинома $f(x)$. С това теоремата е доказана.

Нека подчертаем, че изложеното доказателство на теоремата на Даламбер не използува разглежданите по-рано следствия от нея.

§ 12. Алгебрични числа

Комплексните числа, които са алгебрични над полето $\mathbf{Q}$ на рационалните числа, е прието да се наричат *алгебрични числа*, т. е. едно комплексно число α се нарича алгебрично, ако то е корен на ненулев полином с рационални коефициенти. Числата, които не са алгебрични, се наричат трансцендентни, т. е. трансцендентните елементи на полето $\mathbf{C}$ над полето $\mathbf{Q}$ се наричат *трансцендентни числа*. Ако алгебричното число α е корен на нормиран полином с цели коефициенти, то α се нарича *цяло алгебрично число*.

Примери

1. Всяко рационално число q е алгебрично, тъй като то е корен на полинома $f(x)=x-q\in\mathbf{Q}[x]$.

2. Целите числа $n\in Z$ са в същото време и цели алгебрични.

3. Алгебрично число е всеки радикал от вида $\sqrt[n]{q}$, където n е произволно естествено число и q е рационално число, защото то е корен на полинома $f(x)=x^n-q\in\mathbf{Q}[x]$.

4. Числото $\sqrt{2}$ не е рационално, но е цяло алгебрично, тъй като е корен на нормирания полином x^2-2 с цели коефициенти.

Задача. Докажете, че всяко рационално цяло алгебрично число е цяло число.

5. От твърдението на задачата следва например, че алгебричното число $\frac{1}{2}$ не е цяло алгебрично.

6. Цели алгебрични са комплексните числа i, $-i$, $1+i$, $1-i$.

В 1873 г. Ермит е установил, че неперовото число e е трансцендентно, а малко по-късно Линдеман е доказал трансцендентността на лудолфовото число π. През 1936 г. съветският математик Гелфонд е установил трансцендетността на всички числа от вида α^β, където α е положително алгебрично число, различно от единица, а β е ирационално алгебрично число. В този параграф ще покажем, че трансцендентните числа са в известен смисъл много повече от алгебричните.

От теоремата на Даламбер и от теорема 13 директно се получава следната теорема.

Теорема 16. *Множеството A на всички алгебрични числа е алгебрически затворено подполе на полето $\mathbf{C}$ на комплексните числа.*

Задача. Докажете, че полето A на алгебричните числа е безкрайномерно разширение на полето $\mathbf{Q}$ на рационалните числа.

Полето A на алгебричните числа е пример на алгебрично разширение на $\mathbf{Q}$, което не е крайномерно, т. е. този пример показва, че в общия случай класът на алгебричните разширения не съвпада с класа на крайномерните разширения на дадено поле.

Минималният полином на алгебричното число α над полето Q се нарича просто минимален полином на α. Две алгебрични числа, които имат един и същ минимален полином, се наричат *спрегнати*.

Ясно е, че алгебричното число α се съдържа в $\mathbf{Q}$ тогава и само тогава, когато то е спрегнато само със себе си.

Минималният полином на имагинерната единица i е полиномът x^2+1 и затова i и $-i$ са спрегнати алгебрични числа (те са спрегнати и като комплексни числа, защото $\bar{i}=-i$).

Минималният полином на $\sqrt[n]{p}$, където p е произволно просто число, а n е естествено число, е полиномът x^n-p, тъй като този полином съгласно критерия на Айзенщайн — Шонеман е неразложим над $\mathbf{Q}$ и $\sqrt[n]{p}$ е негов корен. Спрегнатите на $\sqrt[n]{p}$ са всички останали n-ти корени на числото p.

Твърдение 14. *Алгебричното число α е цяло алгебрично тогава и само тогава, когато минималният полином на α е с цели коефициенти.*

Доказателство. Нека α е цяло алгебрично число и $p(x)$ е минималният му полином от степен m. Ако α е корен на нормирания полином $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ с коефициенти $a_1, a_2, \ldots, a_n \in \mathbf{Z}$, то $f(x)=p(x)q(x)$, където $q(x)\in \mathbf{Q}[x]$. Тъй като $p(x)$ и $f(x)$ са нормирани, то $q(x)=x^{n-m}+q_1x^{n-m-1}+\ldots+q_{n-m}$ ($q_i\in\mathbf{Q}$). Ако c и d са най-малките общи кратни на знаменателите съответно на $p(x)$ и $q(x)$, то $p(x)=\frac{1}{c}p_1(x)$ и $q(x)=$

$= \frac{1}{d} q_1(x)$, където $p_1(x)$ и $q_1(x)$ са примитивни полиноми. Тога ва $f(x) = \frac{1}{cd} p_1(x) q_1(x)$ и съгласно лемата на Гаус (виж § 7 на глава II) $p_1(x) q_1(x)$ е примитивен полином. Тъй като $f(x)$ е примитивен полином, то $\frac{1}{cd} = 1$, т. е. $c = 1$ и $p(x) = p_1(x)$ е примитивен полином. Затова $p(x)$ е полином с цели коефициенти. Обратната на твърдението част е очевидна.

Следствие 13. *Ако алгебричното число* β *е спрегнато с цялото алгебрично число* α, *то* β *е цяло алгебрично.*

Твърдение 15. *Множеството на целите алгебрични числа е подпръстен на полето* A *на алгебричните числа.*

Доказателство. Нека α и β са две цели алгебрични числа, а $p(x)$ и $q(x)$ са съответно техните минимални полиноми. Съгласно твърдение 14 нормираните полиноми $p(x)$ и $q(x)$ са с цели коефициенти. Нека $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ са спрегнати на α (т. е. корените на $p(x)$), а $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ — спрегнатите на β. Полиномът

$$f(x) = \prod_{i=1}^{m} \prod_{j=1}^{n} [x - (\alpha_i - \beta_j)]$$

има корен $\alpha - \beta$. Коефициентите на $f(x)$ са полиноми над Z на $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ и са симетрични поотделно спрямо $\alpha_1, \alpha_2, \ldots, \alpha_m$ и $\beta_1, \beta_2, \ldots, \beta_n$. Според теорема 3 от глава III коефициентите на $f(x)$ се изразяват като полиноми над Z на елементарните симетрични полиноми на $\alpha_1, \alpha_2, \ldots, \alpha_m$ и елементарните симетрични полиноми на $\beta_1, \beta_2, \ldots, \beta_n$. Но тези елементарни симетрични полиноми са равни с точност до знак съответно на коефициентите на $p(x)$ и $q(x)$. Следователно коефициентите на $f(x)$ са цели числа, т. е. $\alpha - \beta$ е цяло алгебрично число.

По същия начин се доказва, че и коефициентите на полинома

$$g(x) = \prod_{i=1}^{m'} \prod_{j=1}^{n} (x - \alpha_i \beta_j)$$

са цели числа, откъдето следва, че произведението $\alpha\beta$ е цяло алгебрично число. Следователно множеството на всички цели алгебрични числа е подпръстен на полето A на алгебричните числа.

Целите алгебрични числа не образуват числово поле, защото частното на цели алгебрични числа невинаги е цяло алгебрично число — 1 и 2 са цели алгебрични, но $\frac{1}{2}$ не е цяло алгебрично.

За да покажем, че съществуват твърде много трансцендентни числа, ще се наложи да използуваме някои теоретико-множествени понятия и резултати.

Едно множество се нарича *изброимо*, ако съществува взаимно еднозначно изображение на множеството $\mathbb{N}$ на естествените числа върху него, т. е. ако елементите му могат да се номерират с естествените числа. Безкрайно множество, което не е изброимо, се нарича *неизброимо*. Изброимите множества са безкрайни, защото множеството $\mathbb{N}$ има безкрайно много елементи. Да отбележим, че крайните множества са тези, елементите на които могат да се номерират само с първите няколко естествени числа.

Твърдение 16. *Обединението на две изброими множества е също изброимо множество.*

Доказателство. Нека $X=\{x_1, x_2, \ldots, x_n, \ldots\}$ и $Y=\{y_1, y_2, \ldots, y_n, \ldots\}$ са две изброими множества, а $T=X \cup Y$. Ясно е, че T е безкрайно множество и неговите елементи могат да бъдат подредени в редица например по следния начин:

$$x_1, y_1, x_2, y_2, \ldots, x_n, y_n, \ldots,$$

т. е. елементът x_j получава номер $2j-1$, а елементът y_j получава номер $2j$ ($j=1, 2, \ldots, n, \ldots$). Следователно T е изброимо множество.

Следствие 14. *Едно неизброимо множество не може да се представи като обединение на две свои изброими подмножества.*

Задача. Докажете, че всяко безкрайно подмножество на изброимо множество е изброимо.

Твърдение 17. *Множеството* $\mathbb{R}$ *на реалните числа е неизброимо множество.*

Доказателство. Ще покажем, че $\mathbb{R}$ има безкрайно неизброимо подмножество. Тогава от твърдението на предишната задача ще следва, че $\mathbb{R}$ е неизброимо. За целта да разгледаме отворения интервал $F=(0, 1)$. Известно е, че всяко реално число x от този интервал еднозначно може да се представи като правилна безкрайна десетична дроб

$$x=0, \alpha_1\alpha_2 \ldots \alpha_n \ldots,$$

където α_i са цели числа, $0 \leqq \alpha_i \leqq 9$ и не се допуска от известно място нататък да се повтаря само числото 9. Обратно, всяка такава дроб е число от интервала (0, 1). Да допуснем, че множеството F на всички числа от интервала (0, 1) е изброимо, т. е. елементите на F могат да бъдат подредени във вид на безкрайна редица

$$x_1, x_2, \ldots, x_n, \ldots \tag{1}$$

Нека числото x_i, записано като правилна безкрайна десетична дроб, има вида $x_i=0, \alpha_{i1}\alpha_{i2} \ldots \alpha_{in} \ldots$

Разглеждаме правилната десетична дроб $x=0, \beta_1\beta_2 \ldots \beta_i \ldots$, където цифрите β_i сме избрали така, че $\beta_i \neq \alpha_{ii}$ и $0 \leqq \beta_i \leqq 8$ ($i=1, 2, \ldots, n, \ldots$). Числото x е от F и не съвпада с никое от числата $x_1, x_2, \ldots$, което е противоречие. Следователно множеството F не е изброимо, а тогава и $\mathbb{R}$ е неизброимо.

Следствие 15. *Множеството* **C** *на комплексните числа не може да се представи като обединение на две свои изброими подмножества.*

Действително **C** е неизброимо, защото съдържа като подмножество неизброимото множество на реалните числа и затова твърдението се получава директно от следствие 14.

Твърдение 18. *Обединението на изброимо множество от непразни крайни непресичащи се множества е също изброимо множество.*

Доказателство. Нека $\{X_1, X_2, \ldots, X_m, \ldots,\}$ е изброимо множество от непразните крайни и непресичащи се множества: $X_m = \{x_1^{(m)}, x_2^{(m)}, \ldots, x_{n_m}^{(m)}\}$, $m = 1, 2, \ldots, n, \ldots$ Ако $Y = \bigcup_{i=1}^{\infty} X_i$ е обединението на тези множества, то неговите елементи могат да се наредят в безкрайна редица, например по следния начин:

$$x_1^{(1)}, x_2^{(1)}, \ldots, x_{n_1}^{(1)}, x_1^{(2)}, x_2^{(2)}, \ldots, x_{n_2}^{(2)}, \ldots$$
$$\ldots, x_1^{(m)}, x_2^{(m)}, \ldots, x_{n_m}^{(m)}, \ldots,$$

т. е. елементите от X_k получават номера от $n_1+n_2+\ldots+n_{k-1}+1$ до $n_1+n_2+\ldots+n_{k-1}+n_k$. Следователно Y е изброимо множество.

Ясно е, че доказаното твърдение може да се изкаже и по следния начин:

Твърдение 18′. *Ако обединението на изброимо множество от крайни множества е безкрайно, то е изброимо.*

Теорема 17. *Полето на алгебричните числа е изброимо множество.*

Доказателство. Ще използуваме, че полето A на алгебричните числа съвпада с множеството от корените на полиномите от пръстена $Z[x]$ и че последното множество е безкрайно. Най-напред ще докажем, че пръстенът $Z[x]$ на всички полиноми с цели коефициенти е изброимо множество. Наистина ако

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \quad (n \geqq 0)$$

и $f(x) \in Z[x]$, то *височина* $h(f)$ на полинома $f(x)$ наричаме числото

$$h(f) = n + |a_0| + |a_1| + \ldots + |a_n|.$$

Очевидно е, че всички полиноми от $Z[x]$, които имат височина, равна на естественото число h, образуват крайно множество M_h. Тогава

$$Z[x] = \left(\bigcup_{h=1}^{\infty} M_h\right) \cup \{0\},$$

т. е. $Z[x]$ според твърдение 18′ е изброимо множество. Тъй като всеки полином от $Z[x]$ има краен брой корени, то множеството от корените на полиномите от $Z[x]$ т. е. множеството A, ще бъде

обединение на изброимо множество от крайни множества и тъй като е безкрайно, ще бъде изброимо.

Теорема 18. *Множеството на всички трансцендентни числа е неизброимо.*

Доказателство. Ако допуснем, че множеството T на трансцендентните числа е крайно или изброимо, ще се окаже, че $C = T \cup A$ е изброимо множество, тъй като A е изброимо (виж следствие 15). Следователно множеството T е неизброимо.

13. Нерешимост на някои задачи за построение с линия и пергел

Легенди разказват, че по време на една епидемия на остров Делос в Егейско море за прекратяването на епидемията оракул е дал съвет да се увеличи два пъти кубичният жертвеник, без да се променя формата му. Така преди няколко века преди новата ера е възникнала следната задача.

Задача за удвояване на куба. Да се построи с помощта на линия и пергел страната на такъв куб, който да има два пъти по-голям обем от обема на даден куб.

Ако страната на дадения куб е равна на a, страната на новия куб би трябвало да удовлетворява уравнението $x^3 = 2a^3$. По този начин задачата се свежда до построяването на отсечка с дължина $a\sqrt[3]{2}$, където a е дължината на дадена отсечка.

От дълбока древност са известни и следните две задачи:

Задача за трисекция на ъгъл. С помощта на линия и пергел даден ъгъл да се раздели на три равни части.

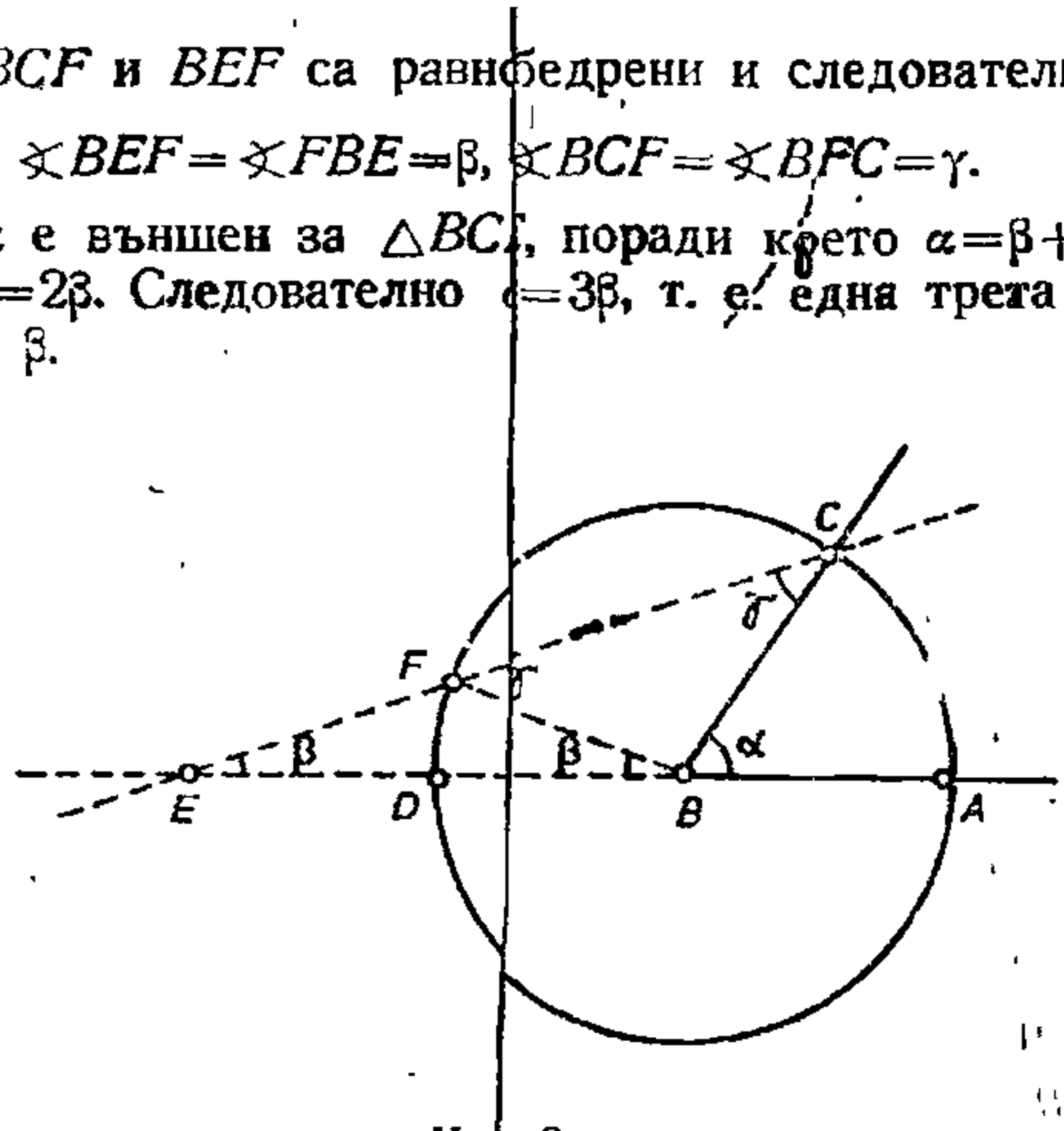
Задача за квадратура на кръга. С помощта на линия и пергел да се построи квадрат с лице, равно на лицето на даден кръг.

Повече от две хилядолетия математиците са правили безуспешни опити да решат посочените три древногръцки задачи. Тези опити са спомогнали за развитието на нови направления в математиката. През 5 в. пр. н. е. Хиократ Хеопски е свел задачата за удвояване на куб със страна x към определянето на отсечката x от пропорцията $a : x = x : y = y : 2a$. По-късно е било забелязано, че отсечката x може да се намери чрез определяне пресечните точки на две параболи или три повърхнини, или парабола и хипербола и т. н. С решаването на тази задача са се занимавали Ератостен (III в. пр. н. е.), Херон (в. пр. н. е.) и др. В съчиненията на Архимед трисекцията на ъгъла се извършва по така наречения метод на „вместването“, което се осъществява с пергел и линия с деления. Именно, ако е даден $\sphericalangle ABC = \alpha$ (черт. 2), с център точка B и произволен радиус построяваме окръжността k. След това между окръжността k и продължението на диаметъра AD „вместваме“ отсечката AB в EF така, че точките C, E и F да лежат върху една права линия. Затази цел точките E и F предварително се отбелязват върху линията с деления. Тогава три-

ъгълниците BCF и BEF са равнобедрени и следователно

$$\sphericalangle BEF = \sphericalangle FBE = \beta, \quad \sphericalangle BCF = \sphericalangle BFC = \gamma.$$

Освен това α е външен за $\triangle BCF$, поради което $\alpha = \beta + \gamma$. По същия начин $\gamma = 2\beta$. Следователно $\alpha = 3\beta$, т. е. една трета от дадения $\sphericalangle ABC$ е β.



Чер. 2

През IX и X век задачата за трисекцията на ъгъла е свеждана към решаването на непълното кубично уравнение $x^3 + px + q = 0$, корените на което са построявани с помощта на „вместването“ или с помощта на конични сечения. По такъв начин задачата за трисекцията на ъгъла е стимулирала търсенето на формули за определяне корените на кубичните уравнения.

През 1637 г. френският учен Рене Декарт пръв е изказал предположението, че в общия случай трите знаменити древногръцки задачи са нерешими с линия и пергел. Неуспешните многобройни опити (които отделни любители напразно продължават и днес) са подтикнали Парижката академия на науките в 1775 г., а след това и други академии да се откажат да разглеждат работи, посветени на тези задачи. Научна обосновка на този отказ донася едва XIX век. Строго доказателство за невъзможността в общия случай произволен ъгъл да бъде разделен на три равни части и да се удвои куб с помощта на линия и пергел е дал през 1837 г. френският математик П. Ванцел. Нека подчертаем, че при посочената по-горе трисекция на Архимед се използува линия с деления. Окончателното изясняване на въпроса за квадратурата на кръга е свързано с изясняване аритметичното естество на лудолфовото число π. В края на XVIII век И. Ламберт и А. Льожандър са доказали, че π е ирационално число. Едва в 1882 г. немският математик Ф. Линдеман е установил, че числото π е трансцендентно. Тази теорема слага край на опитите за решаване задачата за квадратурата на кръга с линия и пергел.

Нашата цел е да разгледаме някои от алгебричните аспекти

на теорията на геометричните построения с линия и пергел, които довеждат до доказателството на невъзможността за решаване на редица геометрични задачи за построения, между които се оказват и споменатите три древногръцки задачи. Най-напред трябва да отговорим на следните три въроса:

а) какви средства можем да използуваме за решаването на дадена геометрична задача за построение с линия и пергел;

b) какви са изходните данни;

с) какво имаме да построим.

Отговорът на първия въпос е, че на наше разположение са само „идеална“ едностранна линия и „идеален“ пергел.

Ако разгледаме задачите за построение с линия и пергел, то ще се убедим, че (с малки изключения) изходните данни на всяка от тях се свеждат до това, че в равнината е дадено крайно множество от точки. При това даденото множество от точки съдържа най-малко две точки — в противен случай задачата съдържа или тривиален, или нееднозначен отговор, а от такива задачи няма да се интересуваме. Наистина, за да бъде зададен ъгъл, е достатъчно да знаем три точки—върха му и по една точка от рамената му; отсечката се определя от двата й края; триъгълникът се задава с три точки — върховете му; въобще многоъгълникът се определя от върховете си (при условие че е казано допълнително кои отсечки, съединяващи върховете, са негови страни); за да бъде зададена окръжност, е достатъчно да се зададат три нейни точки или центърът й и една нейна точка и т. н. Често пъти изходните данни могат да бъдат сведени до задаване само на единичната отсечка, т. е. отсечка, чиято дължина се приема за единица. В този случай отново имаме дадени две точки, а именно краищата на единичната отсечка. По този начин на втория въпрос даваме следния отговор: За първоначални данни се взема в равнината крайно множество от поне две точки.

Разбира се, при този отговор се губи част от геометричния смисъл на задачата — кои от дадените точки и как точно определят една или друга отнапред дадена геометрична фигура. Например едни и същи точки могат да се съединяват по различен начин и така те да определят различни многоъгълници. Обаче тази загуба ни дава възможност да се абстрахираме от дадената конкретна задача и да изследваме въпроса за решимост едновременно за всички геометрични задачи за построение с линия и пергел.

По същия начин не е трудно да се провери, че почти всички задачи за построение се свеждат до построяването на краен брой точки в равнината. Например задачата за трисекцията на ъгъла се свежда до намирането на две точки, през които трябва да се прекарат правите, разделящи ъгъла на три равни части. Задачата за удвояване на куба също се свежда до намирането на две точки — краищата на отсечката, равна на страната на търсения куб. Намирането на някоя окръжност се свежда до построяването на центъра й и една от нейните точки. Задачата за построяване на многоъгълник (в частност на квадрата с лице, равно на

лицето на даден кръг) се свежда до построяването на върховете му, но допълнително трябва да се посочи кои отсечки, съединяващи двойките точки, са страни на търсения многоъгълник.

Забележка. Всъщност съществуват задачи за построение, в които се изисква построяването на безбройно много точки, например построяването на елипса по дадени полуоси. Но ако задачата не може да се сведе до намирането на краен брой точки, то няма да я разглеждаме, като я считаме за нерешима с линия и пергел.

След тези бележки даваме следния отговор на третия въпрос: крайната цел на всяка задача за построение с линия и пергел е построяването в равнината на краен брой точки.

Средствата, с които разполагаме при решаване на геометричните задачи за построение, са идеална линия (без деления) и пергел. С тях се извършват следните построения: (*i*) намират се пресечните точки на прави и окръжности, при което всяка от правите минава през две дадени или получени вече в процеса на построяването) точки и всяка от окръжностите е с даден (или получен вече) център и минава през дадена (или получена вече) точка; (*ii*) прекарват се помощни окръжности с център дадена (получена вече) точка и произволен радиус.

Нека точките в равнината, които представляват изходните данни на задачата, са M_1, M_2, ..., M_n ($n \geqq 2$). Ще казваме, че една точка M от равнината е построима въз основа (на базата) на дадените точки M_1, M_2, ..., M_n, ако тя може да се получи след краен брой построения от вида (*i*) и (*ii*). Естествено точките M_1, M_2, ..., M_n се считат за построими. В дадената равнина избираме правоъгълна координатна система Oxy така, че $M_1=(1, 0)$ и $M_2=(0, 1)$ (с това фактически се въвежда и единичната отсечка, т. е. отсечка с дължина единица). Сега вече всяка точка M от равнината се определя еднозначно от своите координати (x, y). Очевидно е, че точката $M=(x, y)$ е построима тогава и само тогава, когато са построими точките $(x, 0)$ и $(0, y)$. Като отъждествим реалните числа със съответните точки на абцисната ос Ox на координатната система, вместо да говорим за построимост на точката $M=(x, y)$, ще говорим за построимост на реалните числа x и y, а за построенията с линия и пергел ще покажем, че са еквивалентни на редица действия с реални числа. В по-нататъшните разглеждания ще използуваме неизменно следните означения: $A=\{x_1, x_2 \ldots, x_n; y_1, y_2, \ldots, y_n\}$, където x_i и y_i са координатите на изходната точка M_i ($i=1, 2, \ldots, n$); $\mathbf{Q}(A)=\mathbf{Q}(x_1, x_2, \ldots, x_n, y_1, \ldots, y_n)$ — разширение на полето $\mathbf{Q}$ на рационалните числа, получено от $\mathbf{Q}$ чрез присъединяване на числата x_1, x_2, ..., x_n, y_1, ..., y_n. Ако изходните точки M_1, M_2, ..., M_n са само две, т. е. ако $n=2$, просто ще говорим за построимост с линия и пергел на точката $M(x, y)$ или на числата x и y, а ако $n>2$ — за построимост (с линия и пергел) на тази точка и тези числа въз основа (на базата) на множеството A.

Построението (*ii*) съдържа известен произвол и се среща при някои елементарногеометрични задачи, например при прекарване на ъглополовяща на даден ъгъл; на права, перпендикулярна на друга права, и т. н. За определеност обаче ще се условим при построението (*ii*) радиусът на окръжността, който избираме, да бъде с рационална дължина (спрямо избраната вече единична отсечка). Очевидно това ограничение не изменя метода на построение.

Лема 3. *Всяко рационално число е построимо с линия и пергел.*

Наистина цялото положително число n се построява като n-кратно на единицата. Положителното рационално число $\frac{m}{n}$ се построява по познатия начин като „четвърта пропорционална“ $x=\frac{m.1}{n}$, т. е. всички неотрицателни рационални числа са построими. Отрицателното рационално число $-\frac{m}{n}$ е пресечна точка на абсцисната ос с окръжност с център началото на координатната система, която минава през построимата точка $\frac{m}{n}$, т. е. $-\frac{m}{n}$ е построимо число.

Определение 6. Действията събиране, изваждане, умножение деление с ненулево число и извличане на квадратен корен наричаме *квадратични действия.* Под *квадратични действия* върху елементите на числовото множество B (върху множеството B или над множеството B, $B\subseteq R$) ще разбираме прилагане краен брой пъти на квадратични действия върху елементите на B и върху получени по този начин числа.

Лема 4. *Ако множеството B от реални числа съдържа поне едно ненулево число, то множеството K_B от всички числа, които се получават чрез квадратични действия върху елементите на B, е подполе на полето R на реалните числа.*

Наистина K_B е затворено относно изваждането и умножението, които са квадратични действия, т. е. K_B е подпръстен на R. Тъй като $B\subseteq K_B$, в числовия пръстен K_B има поне два елемента. Но K_B е затворено относно делението на ненулево число, т. е. K_B е подполе на R.

Лема 5. *Квадратичните действия върху елементите на множеството A и само те се извършват с помощта на линия и пергел.*

Доказателство. Всяко квадратично действие може да се извърши с линия и пергел. Наистина ако a и b са две дадени числа, то $a+b$ и $a-b$ се построяват по очевиден начин върху абсцисната ос. Числата ab и $\frac{a}{b}$ $(b\neq 0)$, когато a и b са положителни, се построяват като дължини на отсечки, които са четвърти пропорционални на отсечки с дължини 1, a и b, след като се представят във вида $x=\frac{ab}{1}$ и $y=\frac{a.1}{b}$. Ако a или b не е положи-

телно, то числата $|a|.|b|$ и $\frac{|a|}{|b|}$ са построими, а тогава и ab и $\frac{a}{b}$ също могат да се построят с линия и пергел. Числото $x=\sqrt{a}=\sqrt{a.1}$ $(a>0)$ се построява по познатия начин като височина към хипотенузата на правоъгълен триъгълник, проекциите на катетите върху хипотенузата на който имат дължини съответно a и 1.

За да установим, че само квадратичните действия се извършват с линия и пергел, ще анализираме построенията (i) и (ii). За построението (i) ще покажем, че пресечните точки на съответните прави и окръжности имат координати, които се получават чрез квадратични действия върху елементите на A. Наистина уравнението на права g през две построени вече точки $M_1=(x_1, y_1)$ и $M_2=(x_2, y_2)$ (за координатите на които предполагаме, че са получени чрез квадратични действия върху елементите на A) има вида

$$(y_2-y_1)(x-x_1)-(x_2-x_1)(y-y_1)=0.$$

Затова g има уравнение от вида $ax+by+c=0$, в което a, b и c са числа, получени чрез квадратични действия над A. Ако k е окръжност с център (u, v) и радиус r (където за u, v, r се предполага, че са получени чрез квадратични действия над A), то уравнението на k е

$$(x-u)^2+(y-v)^2=r^2.$$

Нека g_1 е друга права с уравнение $a_1x+b_1y+c_1=0$, а k_1 е друг окръжност с уравнение $(x-u_1)^2+(y-v_1)^2=r_1^2$. Очевидно координатите на пресечните точки на g и g_1, g и k, k и k_1 се изразяват чрез квадратични действия върху числата a, b, c, a_1, b_1, c_1, u, v, r, u_1, v_1 и r_1, т. е. координатите на пресечните точки също се изразяват чрез квадратични действия върху елементите на A.

При построението (ii) е направеното по-горе уточнение се получава: окръжност $(x-u)^2+(y-v)^2=r^2$, където r е рационално число, а u и v са построени вече числа, т. е. u, v, r се изразяват чрез квадратични действия върху A и по-нататъшните построения се свеждат към построенията от вида (i), за които видяхме, че водят само до числа, получени чрез квадратични действия върху A. Лемата е доказана.

Следствие 16. *Точката $M=(x, y)$ е построима с линия и пергел въз основа на множеството A тогава и само тогава, когато нейните координати x и y се получават чрез квадратични действия върху елементите на A, т. е. точно тогава, когато x и y се съдържат в полето K_A.*

Следствие 17. *Реалното число α е построимо въз основа на множеството A тогава и само тогава, когато α се получава чрез квадратични действия върху елементите на разширението $Q(A)$.*

Наистина според лема 5 α е построимо въз основа на A точно тогава, когато $\alpha \in K_A=K_{Q(A)}$ (докажете последното равенство!).

Теорема 19. *Реалното число α се получава чрез квадратични действия върху елементите на подполето P на полето на реалните числа тогава и само тогава, когато α принадлежи на квадратично радикално разширение на P.*

Доказателство. Нека α се съдържа в квадратичното радикално разширение K на P. Тогава съществува редица от подполета

$$P=L_0\subseteq L_1\subseteq L_2\subseteq \ldots\subseteq L_s=K,$$

където L_i е квадратично разширение на L_{i-1} $(i=1, 2, \ldots, s)$. Можем да считаме, че в тази редица от подполета няма повторения, т. е. $L_{i-1}\neq L_i$ $(i=1, 2, \ldots, s)$. Тогава $L_i=L_{i-1}(\alpha_i)$, където $\alpha_i=\sqrt{\beta_i}$ и $\beta_i\in L_{i-1}$ (твърдение 10).

Ако $s=0$, то $\alpha\in K=P$ и α се получава чрез квадратични действия върху P. Нека $s>0$ и да допуснем, че за елементите от L_{s-1} сме доказали, че се получават чрез квадратични действия върху елементите на P. Тогава $K=L_{s-1}(\sqrt{\beta_s})$ и $1, \sqrt{\beta_s}$ образуват базис на K над L_{s-1}. Затова $\alpha=a+b\sqrt{\beta_s}$, където $a, b\in L_{s-1}$, т. е. α се получава чрез квадратични действия върху елементите на P.

Обратно, нека α се получава чрез квадратични действия върху елементите на P и нека тези квадратични действия са n на брой. Ако $n=1$, то α има един от следните видове: $a+b$, $a-b$, ab, $\frac{a}{b}$ $(b\neq 0)$, $\sqrt{a}$ $(a>0)$, където $a, b\in P$. Очевидно в първите четири случая $\alpha\in P$ и затова α се съдържа в квадратично радикално разширение на P (самото P). Ако $\alpha=\sqrt{a}$ $(a>0, a\in P)$, то $P(\alpha)$ е квадратично разширение на P и $\alpha\in P(\alpha)$, т. е. при $n=1$ е вярно, че α се съдържа в квадратично радикално разширение на P. Нека $n>1$. Да допуснем, че за числата, които се получават с помалко от n квадратични действия, твърдението е вярно. Числото α има един от следните пет вида: $a+b$, $a-b$, ab, $\frac{a}{b}$ $(b\neq 0)$ и $\sqrt{a}$ $(a>0)$, където a и b се получават с по-малко от n квадратични действия над елементите на P. По предположението на индукцията и съгласно твърдение 10 $a\in K_1=P(\sqrt{\alpha_1})(\sqrt{\alpha_2})\ldots(\sqrt{\alpha_r})$, $b\in P(\sqrt{\beta_1})(\sqrt{\beta_2})\ldots(\sqrt{\beta_t})$, където $\alpha_i\in P(\sqrt{\alpha_1})\ldots(\sqrt{\alpha_{i-1}})$, $\beta_j\in P(\sqrt{\beta_1})\ldots(\sqrt{\beta_{j-1}})$, $i=1, 2, \ldots, r$; $j=1, 2, \ldots, t$. Очевидно подполето $M=P(\sqrt{\alpha_1})\ldots(\sqrt{\alpha_r})(\sqrt{\beta_1})\ldots(\sqrt{\beta_s})=K_1(\sqrt{\beta_1})\ldots(\sqrt{\beta_t})$ е квадратично разширение, което съдържа a и b, т. е. то съдържа $a+b$, $a-b$ $\frac{a}{b}$ и ab. Следователно, когато α има един от първите четири вида, то α се съдържа в квадратично радикално разширение на P. Ако пък $\alpha=\sqrt{a}$, то $\alpha\in K_1(\sqrt{a})=P(\sqrt{\alpha_1})\ldots(\sqrt{\alpha_r})(\sqrt{a})$, което е квадратично радикално разширение на P. Теоремата е доказана.

От предишните две твърдения директно се получава следният важен критерий за построимост.

Следствие 18. *Точката* $M=(x, y)$ *е построима въз основа на множеството* A *тогава и само тогава, когато* x *и* y *се съдържат в квадратични радикални разширения на полето* $\mathbf{Q}(A)$.

Следствие 19. *Ако реалното число* α *е построимо с линия и пергел въз основа на множеството* A, *то* α *е алгебричен елемент над полето* $\mathbf{Q}(A)$ *и степента на минималния му полином над* $\mathbf{Q}(A)$ *е равна на някоя степен* 2^s $(s\geqq 0)$ *на числото* 2.

Наистина по предишните две твърдения α се съдържа в квадратично радикално разширение на полето $\mathbf{Q}(A)$, а съгласно следствие 9 α ще бъде алгебричен елемент над $\mathbf{Q}(A)$ със степен на алгебричност, равна на 2^s за някое $s\geqq 0$.

Ако $n=2$, т. е. ако $A=\{0, 1\}$, то въз основа на горните условия следствието може да се изкаже по следния начин:

Следствие 20. *Ако реалното число* α *е построимо с линия и пергел, то* α *е алгебрично число и степента на минималния му полином над* $\mathbf{Q}$ *е от вида* 2^s $(s\geqq 0)$.

Вече можем да покажем, че споменатите три древногръцки задачи за построение са нерешими с линия и пергел.

1. *Задача за трисекция на ъгъла.* Да се докаже, че с помощта на линия и пергел произволен ъгъл φ не може да се раздели на три равни части.

Както бе вече посочено, даден ъгъл φ може да бъде напълно определен с три точки от равнината — върха O на ъгъла и по една точка M_1 и M_2 от рамената му. Без ограничение на общността можем да считаме, че M_1 и M_2 са на едно и също разстояние от точката O. Върхът O на дадения ъгъл φ избираме за начало на координатна система, а едното му рамо — за абсцисна ос. При това абсцисната ос избираме така, че в посока, обратна на часовниковата стрелка, другото рамо на ъгъла да сключва с тази ос ъгъл φ. За определеност нека $M_1=(1, 0)$. Да допуснем, че трисекцията на ъгъл φ е възможна. Тогава е построима точката $\left(\cos\frac{\varphi}{3}, 0\right)$. От тригонометрията е известно, че $\cos\varphi=4\cos^3\frac{\varphi}{3}-3\cos\frac{\varphi}{3}$. Следователно числото $\cos\frac{\varphi}{3}$ е корен на уравнението $4x^3-3x-\cos\varphi=0$. Нека $\varphi=\frac{\pi}{3}$. Понеже точката M_2 е построима с линия и пергел тогава и само тогава, когато е построима ортогоналната проекция $P=\left(\frac{1}{2}, 0\right)$ на M_2 върху абсцисната ос, то можем да считаме, че изходното множество е $A=\left\{0, 1, \frac{1}{2}\right\}$, т. е. че $\mathbf{Q}(A)=Q$. Тогава $\cos\frac{\varphi}{3}=\cos\frac{\pi}{9}$ е корен на полинома $f(x)=8x^3-6x-1$, който няма рационални корени и следователно е неразложим над полето $\mathbf{Q}$ на рационалните числа.

По такъв начин минималният полином на $\cos\frac{\varphi}{3}=\cos\frac{\pi}{9}$ над Q е от степен 3 и съгласно следствие 19 числото $\cos\frac{\pi}{9}$ няма да бъде построимо с линия и пергел, което е противоречие. Това означава, че трисекцията на конкретния ъгъл $\varphi=\frac{\pi}{3}$ е невъзможна с линия и пергел. Обаче не е трудно да се види, че например ъглите $\varphi=\frac{\pi}{2}$, $\varphi=\frac{\pi}{4}$ могат да се разделят с линия и пергел на три равни части.

2. *Задача за удвояване на куба.* Да се докаже, че с помощта на линия и пергел не може да бъде построена страната на куб, на който обемът е два пъти по-голям от обема на даден куб.

Страната на дадения куб е определена от две различни точки в равнината. Едната от точките избираме за начало O на координатната система, а другата приемаме да съвпада с единичната точка 1. В такъв случай $A=\{0, 1\}$. Задачата се свежда до построяването на такова реално число α, което да удовлетворява уравнението $x^3-2=0$. Тъй като x^3-2 е минималният полином на числото α над Q и неговата степен не е степен на числото 2, то α не е построимо с линийка и пергел.

3. *Задача за квадратурата на кръга.* Да се докаже, че с помощта на линия и пергел не може да се построи квадрат, на който лицето е равно на лицето на даден кръг.

Даденият кръг е напълно определен от две точки — центъра O и една точка M от ограждащата го окръжност. Точката O приемаме за начало на координатна система, а точката M — единичната точка 1. По такъв начин лицето на кръга е равно на числото π, а първоначално даденото множество от точки е $A=\{0, 1\}$. Така задачата се свежда до построяване на числото $\sqrt{\pi}$, което е равносилно на построимостта на π с линия и пергел. Ако обаче π е построимо с линия и пергел, то съгласно следствие 19 π ще бъде алгебрично число, което противоречи на резултата на Линдеман за трансцендентността на π ([3], стр. 269).

ГЛАВА IX

МОДУЛИ

§ 1. Определение на модул над комутативен пръстен с единица

Линейните пространства над едно поле P са адитивно записани абелеви групи, в които има допълнителната възможност да умножаваме елементите им с елементи от P и са в сила редица аксиоми за това умножение. От друга страна, елементите на всяка абелева (адитивно записана) група можем да умножаваме с цели числа, т. е. с елементите на пръстена Z на целите числа, и за това умножение са в сила аналогични аксиоми на тези за линейните пространства. От такава гледна точка редица от резултатите за линейни пространства се оказват аналози на съответни твърдения за абелеви групи. В математиката често се срещат абелеви групи, в които можем да действуваме на (да умножаваме) елементите им с елементи от някой пръстен. В това отношение е естествена необходимостта да се изгради обща теория за изучаването на този тип обекти. Тази теория е теорията на модулите, като понятието модул е едно естествено обобщение на понятията линейно пространство и абелева група.

Определение 1. Нека K е произволен комутативен пръстен с единица 1. Адитивно записаната абелева група M се нарича *модул* над пръстена K или K-модул, ако за всеки елемент a от M и за всеки елемент λ от K е дефинирано тяхното произведение λa — еднозначно определен елемент от M, като при това за произволни λ и μ от K и a, b от M са в сила следните равенства (аксиоми):

1. $(\lambda+\mu)\,a=\lambda a+\mu a$;
2. $\lambda\,(a+b)=\lambda a+\lambda b$;
3. $(\lambda\mu)\,a\ \ =\lambda\,(\mu a)$;
4. $1\,.a\ \ \ =a$.

Примери

1. Модулите над поле са линейните пространства над това поле.

2. Всяка абелева група е модул над пръстена Z на целите числа. Действително ако M е произволна абелева група (адитивно записана), то за всеки неин елемент a и за всяко $n\in Z$ е определено n-кратното na, което приемаме за резултат от умножението на числото n с елемента a. При такова определение, както знаем, аксиомите 1—4 са изпълнени.

3. Адитивната група на всеки комутативен пръстен K с единица можем да разглеждаме като модул над същия пръстен K с

определеното в K умножение. По-общо всеки идеал в K може да се разглежда като модул над K. Аксиомите 1—4 са следствия от съответните аксиоми за пръстен.

4. Нулевата група $M=\{0\}$, която съдържа само един нулев елемент, може да бъде разглеждана като модул над всеки пръстен. Този модул ще наричаме *нулев модул*.

Ще изведем някои елементарни следствия от аксиомите за модул M над комутативен пръстен K с единица.

I. *За всяко* $\lambda \in K$ *е изпълнено равенството* $\lambda . 0 = 0$, *където* 0 *е нулевият елемент на* M.

Действително $\lambda 0 = \lambda (0+0) = \lambda 0 + \lambda 0$ и затова $\lambda 0 = 0$.

II. *За всяко* $a \in M$ *имаме* $0a = 0$, *където* 0 *в лявата страна на равенството е нулевият елемент на* K, *а вдясно — нулата на* M.

Това твърдение следва от равенствата $0a = (0+0)\, a = 0a + 0a$.

III. *За всяко* $\lambda \in K$ *и за всяко* $a \in M$ *имаме* $(-\lambda)\, a = -\lambda a$.

Наистина

$$\lambda a + (-\lambda)\, a = [\lambda + (-\lambda)]\, a = 0a = 0$$

и затова $(-\lambda)\, a = -(\lambda a)$.

IV. $\lambda (-a) = -\lambda a$ *за* $\lambda \in K$ *и* $a \in M$.

Равенството се доказва по същия начин както III.

За линейни пространства знаем, че от равенството $\lambda a = 0$ следва, че $\lambda = 0$ или $a = 0$. За модули в общия случай това твърдение не е вярно. Например нека $M = \langle g \rangle$ е циклична група от ред 2. M е модул над пръстена Z на целите числа, но $2g = 0$, въпреки че $2 \neq 0$ и $g \neq 0$.

V. $$\left(\sum_{i=1}^{n} \lambda_i\right) a = \sum_{i=1}^{n} \lambda_i a \quad (\lambda_i \in K,\ a \in M).$$

За $n = 2$ горното равенство е изпълнено съгласно аксиома 2 за модул. Да допуснем, че за $n-1$ събираеми равенството е вярно. Тогава

$$\left(\sum_{i=1}^{n} \lambda_i\right) a = \left(\sum_{i=1}^{n-1} \lambda_i + \lambda_n\right) a = \left(\sum_{i=1}^{n-1} \lambda_i\right) a + \lambda_n a =$$

$$= \sum_{i=1}^{n-1} \lambda_i a + \lambda_n a = \sum_{i=1}^{n} \lambda_i a,$$

т. е. равенството е вярно за всяко n.

VI. $$\lambda \left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} \lambda a_i.$$

Равенството се доказва с индукция спрямо n.

VII. $(\lambda-\mu)\,a=\lambda a-\mu a$ $(\lambda,\ \mu\in K,\ a\in M)$.

Ще покажем, че $(\lambda-\mu)\,a$ е решение на уравнението $\mu a+x=\lambda a$, с което дистрибутивният закон за разлика на елементи от K ще бъде доказан. Наистина

$$\mu a+(\lambda-\mu)\,a=[\mu+(\lambda-\mu)]\,a=\lambda a.$$

VIII. $\lambda\,(a-b)=\lambda a-\lambda b$.

Доказва се по същия начин както VII.

Определение 2. Изображението φ на K-модула M в K-модула N се нарича *модулен хомоморфизъм*, ако за всяко $\lambda\in K$ и за всеки два елемента a и b от M са изпълнени условията

$$(i)\qquad \varphi(\lambda a)=\lambda\varphi(a),$$

$$(ii)\qquad \varphi(a+b)=\varphi(a)+\varphi(b).$$

Очевидно модулният хомоморфизъм φ: $M\to N$ е такъв хомоморфизъм на абелевата група M в абелевата група N, който удовлетворява условие (i).

Ако хомоморфизмът φ на модула M в модула N е такъв, че за всеки елемент $c\in N$ съществува първообраз a от M при φ (т. е. $\varphi(a)=c$), то ще казваме, че φ е хомоморфизъм на модула M *върху* модула N. Ако хомоморфизмът φ на модула M върху модула N изобразява различни елементи от M в различни елементи от N, то φ се нарича *изоморфизъм*. Ако съществува изоморфизъм на M върху N, то модулите M и N се наричат *изоморфни* и пишем $M\cong N$.

§ 2. Подмодули. Директни суми на модули

Определение 3. Непразното подмножество S на модула M над пръстена K се нарича *подмодул* на M, ако S е модул над K спрямо дефинираните в M операции събиране и умножение на елементи от K.

Твърдение 1. *Непразното подмножество S на модула M над пръстена K е подмодул тогава и само тогава, когато са изпълнени следните две условия:*

(i) за всеки два елемента x и y от S тяхната сума $x+y$ е също елемент на S;

(ii) за всяко $\lambda\in K$ и за всяко $x\in S$ елементът λx принадлежи на S.

Доказателство. Ако S е подмодул, то от определението на подмодул условията (i) и (ii) са изпълнени.

Нека за S са изпълнени условията (i) и (ii). Тъй като $(-1)\,x=-x$ за всяко x, то S заедно с всеки елемент съдържа и неговия противоположен. Следователно S е абелева група с определено в нея умножение на елементи от K, което съвпада с умножението в модула M. Аксиомите 1—4 са изпълнени в S, тъй като те са изпълнени за елементите на модула M, а S е подмножество на M. Твърдението е доказано.

Нека $S_1, S_2, \ldots, S_n$ са произволни подмодули на модула M над K. Подмножеството на M, съставено от всички елементи x от вида $x=x_1+x_2+\ldots+x_n$ $(x_i \in S_i, i=1, 2, \ldots, n)$, се нарича сума на подмодулите $S_1, S_2, \ldots, S_n$ и се означава с $S_1+S_2+\ldots+S_n$, т. е. $S_1+S_2+\ldots+S_n=\{x \mid x \in M, \quad x=x_1+x_2+\ldots+x_n, x_i \in S_i\}$.

Сумата на подмодули е подмодул. Действително нека x и y са от $S_1+S_2+\ldots+S_n$ и $\lambda \in K$. Тогава $x=x_1+x_2+\ldots+x_n$ и $y=y_1+y_2+\ldots+y_n$ за някои x_i и y_i от S_i $(i=1, 2, \ldots, n)$. Тъй като S_i е подмодул на M, то $x_i+y_i \in S_i$ и $\lambda x_i \in S_i$. Затова $x+y=(x_1+y_1)+\ldots+(x_n+y_n)$ и $\lambda x=\lambda x_1+\lambda x_2+\ldots+\lambda x_n$ са също елементи от $S_1+S_2+\ldots+S_n$. От твърдение 1 следва, че сумата $S_1+S_2+\ldots+S_n$ е подмодул на M. Очевидно $S_1+S_2+\ldots+S_n$ съдържа всеки от подмодулите S_i.

Определение 4. *Нека $S_1, S_2, \ldots, S_n$ са подмодули на модула M над пръстена K. Ако всеки елемент x от сумата $S_1+S_2+\ldots+S_n$ има единствено представяне във вида*

$$x=x_1+x_2+\ldots+x_n \quad (x_i \in S_i, \quad i=1, 2, \ldots, n),$$

то сумата на подмодулите ще наричаме директна и ще я означаваме с $S_1 \oplus S_2 \oplus \ldots \oplus S_n$. Ако $M=S_1 \oplus S_2 \oplus \ldots \oplus S_n$, то ще казваме, че модулът M се разлага в директна сума на своите подмодули $S_1, S_2, S_3, \ldots, S_n$.

Твърдение 2. *Нека M_1 и M_2 са два подмодула на модула M. Сумата M_1+M_2 е директна тогава и само тогава, когато $M_1 \cap M_2=(0)$, т. е. когато сечението на двата подмодула е ненулевият подмодул.*

Доказателство. 1. Нека $M_1+M_2=M_1 \oplus M_2$.

Да допуснем, че $M_1 \cap M_2 \neq (0)$ и нека $x \in M_1 \cap M_2$, $x \neq 0$. Тъй като сечението $M_1 \cap M_2$ се съдържа в сумата $M_1 \oplus M_2$, то $x \in M_1 \oplus M_2$. Но елемента x можем да запишем по два различни начина $x=0+x=x+0$ като елемент от сумата. Това противоречи на директността на сумата $M_1 \oplus M_2$. Следователно $M_1 \cap M_2=(0)$.

2. Нека $M_1 \cap M_2=(0)$ и $x=x_1+x_2=y_1+y_2$ са две представяния на елемента x от M_1+M_2 като сума на елементи, взети съответно от M_1 и M_2. Тогава елементът $z=x_1-y_1=y_2-x_2$ е от сечението $M_1 \cap M_2=(0)$ и затова е нулевият елемент, т. е. $x_1=x_2$ и $y_1=y_2$. Така показахме, че всеки елемент от сумата M_1+M_2 има единствено представяне като сума на елемент от M_1 и елемент от M_2, т. е. сумата е директна.

Теорема 1 (транзитивност на разлагането). *Нека $M=M_1 \oplus M_2 \oplus \ldots \oplus M_n$ е произволно разлагане на модула M в директна сума на своите подмодули $M_1, M_2, \ldots, M_n$. Ако всеки от подмодулите M_i е разложен в директна сума на някои свои подмодули, т. е. $M_i=M_{i1} \oplus M_{i2} \oplus \ldots \oplus M_{ik_i}$ $(i=1, 2, \ldots, n)$, то модулът M се разлага в директна сума на подмодулите M_{ij}, където $j=1, 2, \ldots, k_i$ и $i=1, 2, \ldots, n$.*

Доказателство. Нека x е произволен елемент от M. Тогава

$$x=\sum_{i=1}^{n} x_i \quad (x_i \in M_i),$$

$$x_i=\sum_{j=1}^{k_i} x_{ij} \quad (x_{ij} \in M_{ij}).$$

Заместваме x_i с техните равни и получаваме $x=\sum_{i=1}^{n}\sum_{j=1}^{k_i} x_{ij}$, т. е. модулът M съвпада със сумата на модулите M_{ij}. Да допуснем, че $x=\sum_{i=1}^{n}\sum_{j=1}^{k_i} y_{ij}$ е второто представяне на x като сума на елементи от M_{ij}. Тъй като $M=M_1\oplus M_2\oplus \ldots \oplus M_n$, то сумите $\sum_{j=1}^{k_i} x_{ij}$ и $\sum_{j=1}^{k_i} y_{ij}$ съвпадат, т. е.

$$\sum_{j=1}^{k_i} x_{ij}=\sum_{j=1}^{k_i} y_{ij} \qquad (i=1, 2, \ldots, n).$$

Но за всяко i сумата $M_i=M_{i1}\oplus \ldots \oplus M_{ik_i}$ е директна и затова $x_{ij}=y_{ij}$ за всяко i и j. С това доказахме, че сумата на подмодулите M_{ij} е директна.

Задача. Докажете, че модулът M е директна сума на своите подмодули $M_1, \ldots, M_n$ тогава и само тогава, когато $M=M_1+M_2+\ldots+M_n$ и за всяко i е изпълнено равенството

$$M_i \cap (M_1+\ldots+M_{i-1}+M_{i+1}+\ldots+M_n)=(0).$$

По аналогичен начин, както в теорията на пръстените, може да се разглеждат и директни суми на модули. Действително нека $M_1, M_2, \ldots, M_n$ са n (не обезателно различни) K-модули и M е множеството от всички наредени n-торки от вида $(a_1, a_2, \ldots, a_n)$, където $a_i \in M_i$ $(i=1, 2, \ldots, n)$. Две n-торки са равни тогава и само тогава, когато съвпадат съответните им компоненти. За всеки два елемента $a=(a_1, a_2, \ldots, a_n)$ и $b=(b_1, b_2, \ldots, b_n)$ от M дефинираме сума $a+b=(a_1+b_1, a_2+b_2, \ldots, a_n+b_n)$ и произведение $\alpha a=(\alpha a_1, \alpha a_2, \ldots, \alpha a_n)$, където $\alpha \in K$. Лесно се проверява, че по отношение на така въведените действия множеството M се превръща в K-модул, който се нарича *директна сума* на модулите $M_1, M_2, \ldots, M_n$ и се означава $M=M_1\oplus M_2\oplus \ldots \oplus M_n$.

Задача. Нека M е директна сума на K-модулите M_1, M_2

..., M_n. Докажете, че M съдържа такива подмодули M_1, M_2, ..., M_n, че M е тяхната директна сума и $M_i \cong M_i$ $(i = 1, 2, \ldots, n)$.

Тъй като всяка абелева група G е модул над пръстена $\mathbf{Z}$ на целите числа, то можем да говорим и за *директна сума* $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ на подгрупите G_i на групата G. Тогава доказаните по-горе твърдения остават верни и за директни суми на абелеви групи. Ако операцията в G е мултипликативна, то говорим за *директно произведение* $G_1 \times G_2 \times \ldots \times G_n$ на групите $G_1, G_2, \ldots, G_n$.

§ 3. Фактор-модули. Теорема за хомоморфизмите

Нека M и N са два модула над комутативния пръстен K и $\varphi: M \to N$ е произволен хомоморфизъм на M в N. С $\ker\varphi$ ще означаваме множеството от всички елементи на модула M, които чрез φ се изобразяват в нулевия елемент на модула N, и ще го наричаме ядро на хомоморфизма φ, т. е.

$$\ker\varphi = \{a \mid a \in M,\ \varphi(a) = 0\}.$$

С $\operatorname{Im}\varphi$ или с $\varphi(M)$ ще означаваме подмножеството на N, което се състои от всички елементи на N, които имат първообраз при φ, т. е.

$$\operatorname{Im}\varphi = \varphi(M) = \{\varphi(a) \mid a \in M\}.$$

Задача. Да се докаже, че ядрото на всеки хомоморфизъм на модула M в кой да е модул N е подмодул на M, а образът на този хомоморфизъм е подмодул на N.

Нека S е произволен подмодул на модула M. Тъй като S е подгрупа на адитивната група M, то можем да образуваме фактор-групата M/S. Можем ли да определим умножение на елементите от пръстена K с елементите на фактор-групата M/S така, че последната да се превърне в модул над K? Оказва се, че това е възможно благодарение на факта, че S е подмодул в M. Нека λ е произволен елемент от пръстена K и $a+S$ — произволен съседен клас от M/S. По определение полагаме $\lambda(a+S) = \lambda a + S$, като дясната страна на равенството определя лявата.

Да проверим коректността на определението. Нека $a+S = a_1+S$, т. е. a_1 е друг представител на съседния клас $a+S$. Трябва да покажем, че $\lambda a + S = \lambda a_1 + S$, т. е. че λa и λa_1 са представители на един и същ съседен клас по S. Но $\lambda a - \lambda a_1 = \lambda(a - a_1) \in S$, тъй като $a - a_1 \in S$ и S е подмодул на M. С това коректността на определението е проверена.

Като се използува определението съвършено лесно се проверява, че фактор-групата M/S е модул над K. Така определеният модул се нарича *фактор-модул* на модула M по неговия подмодул S и се означава също с M/S.

Да дефинираме изображението η на модула M във фактор-модула M/S, като положим $\eta(a) = a + S$ за всеки елемент a от M

От глава IV знаем, че η е групов хомоморфизъм на групата M върху фактор-групата M/S. Но

$$\eta(\lambda a)=\lambda a+S=\lambda(a+S)=\lambda\eta(a),$$

т. е. η е модулен хомоморфизъм на M върху фактор-модула M/S. Този хомоморфизъм наричаме *естествен хомоморфизъм* на модула M върху неговия фактор-модул M/S. Да намерим ядрото $\ker\eta$ на този естествен хомоморфизъм. Нулевият елемент на M/S е класът $S=0+S$, а

$$\ker\eta=\{a\mid a\in M,\ \eta(a)=S\}.$$

Нека $a\in\ker\eta$. Тогава $\eta(a)=S$. Но $\eta(a)=a+S$, т. е. $a+S=S$ и затова $a\in S$. Показахме, че $\ker\eta$ се съдържа в подмодула S. Тъй като всеки елемент от S при η се изобразява в нулевия елемент S на фактор-модула M/S, то ядрото на естествения хомоморфизъм η съвпада с подмодула S, по който сме факторизирали M.

Ако съществува поне един хомоморфизъм на модула M върху модула N, ще казваме, че N е хомоморфен образ на модула M.

Вече видяхме, че всеки фактор-модул на модула M е негов хомоморфен образ.

Връзката между фактор-модулите на даден модул и неговите хомоморфни образи се дава от следната теорема.

Теорема 2 (теорема за хомоморфизмите). *Нека M и N са модули над комутативния пръстен K, φ е произволен хомоморфизъм на модула M върху модула N, а S е ядрото на φ. Тогава модулът N е изоморфен на фактор-модула M/S. При това съществува такъв изоморфизъм σ на M/S върху N, че произведението $\sigma\eta$ на изоморфизма σ и естествения хомоморфизъм η съвпада с хомоморфизма φ.*

Доказателство. Тъй като M, N и M/S са групи, а φ и η са групови хомоморфизми, то от теоремата за хомоморфизмите на групи следва, че съществува групов изоморфизъм σ на M/S върху N, при което е изпълнено равенството $\varphi=\sigma\eta$. Остава само да проверим, че σ е модулен хомоморфизъм. Нека $b\in M/S$ и $\lambda\in K$. Тъй като η е хомоморфизъм на M върху M/S, то елементът b има поне един първообраз от M при η. Ако $a\in M$ е един от тези първообрази, т. е. $\eta(a)=b$, то $\sigma(\lambda b)=\sigma[\lambda\eta(a)]=\sigma[\eta(\lambda a)]=\sigma\eta(\lambda a)=\varphi(\lambda a)=\lambda\varphi(a)=\lambda\sigma\eta(a)=\lambda\sigma(b)$. Последните равенства показват, че груповият изоморфизъм σ е и модулен изоморфизъм. Теоремата е доказана.

Трябва да забележим, че горната теорема можеше да докажем и без да се опираме на съответната теорема за групи, при това схемата на доказателството би била напълно аналогична на доказателството на последната.

Нека I е произволен идеал на пръстена K и M е модул над K. С IM ще означаваме множеството от всички елементи на M, които могат да се представят като крайни суми на елементи от вида μa, където $\mu\in I$ и a е елемент от M, т. е.

$$IM=\left\{\sum_i \mu_i\, a_i \mid \mu_i \in I,\ a_i \in M\right\}.$$

Подмножеството IM е подмодул на M.

Действително нека $x=\sum_i \mu_i\, a_i$, $y=\sum_j \nu_j b_j$ са два елемента от IM. Очевидно $x+y$ е също крайна сума на елементи от вида $\mu a\,(\mu \in I,\ a \in M)$ и затова $x+y \in IM$. Ако $\lambda \in K$ е произволен елемент на пръстена, то $\lambda x=\sum(\lambda\mu_i)\,a_i$. Тъй като $\mu_i \in I$ и I е идеал, то $\lambda\mu_i \in I$, т. е. $\lambda x \in IM$.

Доказахме, че IM е подмодул на M. Да образуваме фактор-модула M/IM. Този фактор-модул е модул над пръстена K, но той може да се разглежда още и като модул над фактор-пръстена K/I. И наистина нека $\lambda+I$ е произволен елемент от фактор-пръстена K/I и $a+IM$ е произволен елемент от M/IM. По определение полагаме

$$(\lambda+I)\,(a+IM)=\lambda a+IM.$$

За да проверим коректността на определението, нека $\lambda+I=\lambda_1+I$ и $a+IM=a_1+IM$, т. е. $\lambda-\lambda_1=\mu \in I$ и $a-a_1 \in IM$. Тогава $\lambda a-\lambda_1 a_1=(\lambda_1+\mu)a-\lambda_1 a_1=\lambda_1(a-a_1)+\mu a$. Тъй като $\mu \in I$, то $\mu a \in IM$. Понеже IM е подмодул и $a-a_1 \in IM$, то $\lambda_1(a-a_1) \in IM$. Следователно $\lambda a-\lambda_1 a_1 \in IM$, т. е. $\lambda a+IM=\lambda_1 a_1+IM$. С това коректността на определението е проверена.

Проверката на съответните закони за модул се провежда тривиално.

Знаем (виж последната задача от § 4 на глава V), че ако I е максимален идеал в комутативния пръстен K с единица, то фактор-пръстенът K/I е поле. От тази забележка и от горните разглеждания получаваме следния резултат.

Твърдение 3. *Нека I е максимален идеал в комутативния пръстен K с единица, а M е произволен модул над K. Тогава фактор-модулът M/IM е линейно пространство над полето K/I.*

Задача 3. Да се докаже, че ако модулът M е директна сума на своите подмодули N и S, т. е. $M=N\oplus S$, то фактор-модулът M/S е изоморфен на модула N.

§ 4. Анулатор на елемент на модул

Нека K е комутативен пръстен с единица, а M е произволен модул над K. Ако a е елемент на M, то множеството от всички елементи $\lambda \in K$, за които е в сила равенството $\lambda a=0$, ще означаваме с $\mathrm{Ann}(a)$ и ще го наричаме *анулатор* на елемента a, т. е.

$$\mathrm{Ann}(a)=\{\lambda \mid \lambda \in K,\ \ \lambda a=0\}.$$

Например анулаторът $\mathrm{Ann}(0)$ на нулевия елемент на модула M съвпада с целия пръстен K, т. е. $\mathrm{Ann}(0)=K$.

Твърдение 4. *Анулаторът* $\mathrm{Ann}(a)$ *на всеки елемент* a *на модула* M *е идеал в пръстена* K.

Доказателство. Нека λ и μ са два произволни елемента от $\mathrm{Ann}(a)$, а ν е елемент от K. Тогава $(\lambda \pm \mu)a = \lambda a \pm \mu a = 0 \pm 0 = 0$, $(\nu\lambda)a = \nu(\lambda a) = \nu 0 = 0$ и затова $\lambda \pm \mu \in \mathrm{Ann}(a)$ и $\nu\lambda \in \mathrm{Ann}(a)$. Твърдението е доказано.

Определение 5. Модулът M над пръстена K се нарича *цикличен*, ако в M съществува такъв елемент a, че всеки елемент x от M има вида $x = \lambda a$ за някое $\lambda \in K$. Елементът a с посоченото свойство се нарича *образуващ* (*пораждащ*) *елемент* на цикличния модул M и записваме $M = (a)$.

Примери

1. Цикличните модули над дадено поле P са нулевото пространство и едномерните линейни пространства над P.

2. Всяка циклична група е цикличен модул над пръстена Z на целите числа.

3. Адитивната група на пръстена K, разглеждана като модул над K, е цикличен модул с пораждащ елемент единицата 1 на пръстена.

4. Всеки главен идеал на пръстена K е цикличен модул над K и неговият образуващ елемент съвпада с пораждащия елемент на самия главен идеал.

5. Нулевият модул е цикличен модул.

Теорема 3. *Анулаторите на различните образуващи елементи на даден цикличен модул* M *съвпадат.*

Доказателство. Нека a и b са два образуващи елемента на M. Тогава $a = \lambda b$ и $b = \mu a$ за някои елементи λ и μ от K. Ако $\nu \in \mathrm{Ann}(a)$, то $\nu b = \nu(\mu a) = (\nu\mu)a = (\mu\nu)a = \mu(\nu a) = \mu 0 = 0$, т. е. $\nu \in \mathrm{Ann}(b)$. Получихме включването $\mathrm{Ann}(a) \subseteq \mathrm{Ann}(b)$. По същия начин се доказва и обратното включване. Следователно $\mathrm{Ann}(a) = \mathrm{Ann}(b)$.

Определение 6. Цикличният модул M над пръстена K се нарича *свободен цикличен модул*, ако анулаторът на пораждащия елемент на M съвпада с нулевия идеал на K.

Например безкрайните циклични групи и само те са свободни циклични Z-модули. Също така едномерните линейни пространства над поле и само те са свободни циклични модули над това поле.

Задача. Да се докаже, че ако (a) е цикличен модул над пръстена K, то K-модулите $K/\mathrm{Ann}(a)$ и (a) са изоморфни.

Упътване. Разгледайте модулния хомоморфизъм $\varphi : K \to (a)$, дефиниран чрез $\varphi(\alpha) = \alpha a$, и докажете, че $\ker\varphi = \mathrm{Ann}(a)$.

Теорема 4. *Цикличният модул* M *над пръстена* K *е свободен точно тогава, когато* M *е изоморфен на* K*-модула* K.

Доказателство. Ако $M = (a)$ е свободен цикличен K-модул, то $\mathrm{Ann}(a) = (0)$. Следователно според предишната задача е изпълнено $K/(0) \cong (a)$, т. е. в сила е модулният изоморфизъм $M \cong K$.

Обратно, нека $M \cong K$ и $\varphi : K \to M$ е модулен изоморфизъм на K-модулите K и M. Ще докажем, че $\varphi(1) = b$ е образуващ

елемент на модула M. Наистина, ако $c \in M$, за c съществува първообраз λ от K при φ, т. е. $c = \varphi(\lambda) = \varphi(\lambda . 1) = \lambda\varphi(1) = \lambda b$. Ако $\mu \in \mathrm{Ann}\,(b)$, то $0 = \mu b = \mu\varphi(1) = \varphi(\mu)$ и тъй като φ е изоморфизъм, то $\mu = 0$, т. е. $\mathrm{Ann}(b) = (0)$ и следователно M е свободен циклични модул. Теоремата е доказана.

§ 5. Неразложими циклични модули над област на главни идеали

Нека K е област на главни идеали. Ако M е модул над K и a е произволен елемент на M, то $\mathrm{Ann}(a)$ е главен идеал в K, т. е. $\mathrm{Ann}(a) = (\alpha)$ за някой елемент $\alpha \in K$. Елементът α, както знаем, е определен с точност до асоциираност. Под ред на елемента a ще разбираме елемента α или кой да е асоцииран с α.

Пример. Ако M е модул над пръстена Z на целите числа, то M е абелева група. Тогава $\mathrm{Ann}(a) = nZ = (n)$ и за ред на елемента a се приема числа n или $-n$. Ако приемем за ред на a положителното от двете числа n и $-n$, то понятието ред на елемент от модул над Z съвпада с обичайното понятие ред на елемент от абелева група. Изключение прави само елемент a за който $\mathrm{Ann}(a) = (0)$, т. е. елемент от безкраен ред.

Определение 7. Ако K е област на главни идеали, а M е такъв цикличен модул, че редът на образуващия елемент на M е равен (асоцииран) на степен на прост елемент p от K, то M се нарича *примарен цикличен модул* спрямо простия елемент p или *p-примарен цикличен модул.*

Ясно е, че цикличният модул $M = (a)$ е p-примарен точно тогава, когато $\mathrm{Ann}(a)$ се поражда от някоя степен на p.

Примери

1. Ако K е поле, то над K не съществуват примарни циклични модули, тъй като в K няма прости елементи.

2. Ако $K = Z$, то цикличната абелева група M е примарен цикличен Z-модул тогава и само тогава, когато редът ѝ е равен на степен на някое просто число p, т. е. когато M е циклична p-група.

Определение 8. Ще казваме, че модулът M над пръстена K е *неразложим* (*в директна сума*), ако за всяко разлагане $M = M_1 \oplus M_2$ на M в директна сума на негови подмодули M_1 и M_2 следва, че $M_1 = (0)$ или $M_2 = (0)$.

Примери

1. Нулевият модул е неразложим.

2. Всяко едномерно линейно пространство над дадено поле P е неразложим модул над P.°

3. Всяка абелева група от прост ред е неразложим модул над Z.

Твърдение 5. *Ако K е област на главни идеали, то всеки свободен цикличен модул над K е неразложим.*

Доказателство. Нека $M = (a)$ е свободен цикличен мо-

дул над K и a е негов образуващ елемент. Да допуснем, че $M=M_1\oplus M_2$, където $M_1\neq(0)$ и $M_2\neq(0)$. Нека $0\neq b_1\in M_1$ и $0\neq b_2\in M_2$. Тогава $b_1=\lambda a\neq 0$ и $b_2=\mu a\neq 0$ за някои елементи λ и μ от K. Тъй като $\lambda\neq 0$ и $\mu\neq 0$, и в пръстена K няма делители на нулата, то $\lambda\mu\neq 0$. Елементът $b=(\lambda\mu)a$ не е нулев, понеже $\mathrm{Ann}(a)=(0)$ (виж теорема 4). Но $b=\mu b_1=\lambda b_2$ и затова $0\neq b\in M_1\cap M_2$. Последното съгласно твърдение 2 противоречи на това, че сумата $M_1\oplus M_2$ е директна. Следователно $M_1=(0)$ или $M_2=(0)$. Твърдението е доказано.

Твърдение 6. *Всеки примарен цикличен модул над областта K на главни идеали е неразложим.*

Доказателство. Нека M е примарен цикличен модул спрямо простия елемент p на K, a е негов образуващ елемент и $\mathrm{Ann}(a)=(p^n)$. Ако N е ненулев подмодул на M, то елементът $b=p^{n-1}a\neq 0$ се съдържа в N. Наистина нека $x=\lambda a\neq 0$ е произволен ненулев елемент на N. Елементът λ не се дели на p^n, тъй като $x\neq 0$. Затова ако p^l/λ, но p^{l+1} не дели λ, то $l<n$. Тогава $\lambda=p^l\lambda_1$, където НОД $(p, \lambda_1)=1$. Тъй като K е пръстен на главни идеали и НОД $(\lambda, p^n)=p^l$, то $p^l=u\lambda+vp^n$ за някои елементи u и v от K. Тогава

$$b=p^{n-1}a=p^{n-l-1}(u\lambda+vp^n)a=p^{n-l-1}(u\lambda)a=(p^{n-l-1}u)x\in N,$$

понеже $x\in N$. Така доказахме, че всеки ненулев подмодул на M съдържа ненулевия елемент $b=p^{n-1}a$.

Да допуснем сега, че $M=M_1\oplus M_2$, където M_1 и M_2 са два ненулеви подмодула на M. Тогава $0\neq b\in M_1\cap M_2$, а това противоречи на предположението, че сумата $M_1\oplus M_2$ е директна. Следователно M е неразложим модул.

Твърдение 7. *Ако цикличният модул M над областта K на главни идеали не е нулев, не е свободен и не е примарен, то M се разлага в директна сума на примарни циклични модули спрямо различни неасоциирани прости елементи.*

Доказателство. Нека a е образуващ елемент на M, а $\mathrm{Ann}(a)=(\alpha)$. Елементът α не е обратим, защото M не е нулевият модул; α не е нула, защото M не е свободен цикличен модул; α не е асоцииран със степен на прост елемент, защото M не е примарен. Следователно елементът α е асоцииран с елемент от вида $p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, където $k_i\geqq 1$, $s\geqq 2$, а $p_1, p_2, \ldots, p_s$ са различни (неасоциирани) прости елементи, които делят α.

Можем да считаме, че $\alpha=p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, тъй като асоциираните елементи пораждат един и същ идеал $\mathrm{Ann}(a)$. Да означим с α_i елемента $p_1^{k_1}\ldots p_{i-1}^{k_{i-1}}p_{i+1}^{k_{i+1}}\ldots p_s^{k_s}$. Нека M_i е цикличният подмодул на M, породен от елемента $b_i=\alpha_i a$ $(i=1, 2, \ldots, s)$, т. е. $M_i=\{\lambda b_i \mid \lambda\in K\}$, $\mathrm{Ann}(b_i)=(p_i^{k_i})$.

Не е трудно да се види, че НОД на елементите $\alpha_1, \alpha_2, \ldots, \alpha_s$ е единица. Затова съществуват такива $\lambda_1, \lambda_2, \ldots, \lambda_s$ от K, че

$$1=\lambda_1\alpha_1+\lambda_2\alpha_2+\ldots+\lambda_s\alpha_s,$$

и затова

$$a = 1a = \lambda_1(\alpha_1 a) + \lambda_2(\alpha_2 a) + \ldots + \lambda_s(\alpha_s a) = \\ = \lambda_1 b_1 + \lambda_2 b_2 + \ldots + \lambda_s b_s.$$

т. е. a се съдържа в сумата $M_1 + M_2 + \ldots + M_s$. Тъй като a поражда целия модул M, то от $a \in M_1 + M_2 + \ldots + M_s$ следва равенството $M = M_1 + M_2 + \ldots + M_s$. Ще докажем, че тази сума е директна. Нека

$$x = \sum_{i=1}^{s} \mu_i b_i = \sum_{i=1}^{s} \nu_i b_i \quad (\mu_i b_i,\ \nu_i b_i \in M_i).$$

Тогава

$$0 = \sum_{i=1}^{s} (\mu_i - \nu_i) b_i = \sum_{i=1}^{s} (\mu_i - \nu_i)\alpha_i\, a = \left[\sum_{i=1}^{s} (\mu_i - \nu_i)\alpha_i\right] a.$$

Следователно сумата $\sum_{i=1}^{s} (\mu_i - \nu_i)\alpha_i$ се съдържа в $\mathrm{Ann}(a) = (\alpha)$ и затова $\alpha / \sum_{i=1}^{s} (\mu_i - \nu_i)\alpha_i$. Тъй като $p_j^{k_j} / \alpha$, $p_j^{k_j} / \alpha_i$ при $i \neq j$ и НОД $(\alpha_j, p_j) = 1$, то $p_j^{k_j} / (\mu_j - \nu_j)$, $1 \leqq j \leqq s$. Но $\mathrm{Ann}(b_j) = (p_j^{k_j})$ и затова $\mu_j b_j = \nu_j b_j$ за всяко $j = 1, 2, \ldots, s$, т. е. $M = M_1 \oplus M_2 \oplus \ldots \oplus M_s$. Твърдението е доказано.

Последните три твърдения се обединяват в следната

Теорема 5. ***Цикличният модул M над областта K на главни идеали е неразложим в директна сума тогава и само тогава, когато M е или нулев, или свободен, или примарен.***

Твърдение 8. *Нека модулът M над пръстена K на главни идеали се разлага в директна сума на своите примарни циклични подмодули $M_1, M_2, \ldots, M_n$, които се отнасят към различни неасоциирани прости елементи на пръстена K. Тогава модулът M е цикличен.*

Доказателство. Нека b_i е образуващ елемент на примарния модул M_i и $\mathrm{Ann}(b_i) = (p_i^{k_i})$, където p_i е прост елемент от K $(i = 1, 2, \ldots, n)$. По условие $M = M_1 \oplus M_2 \oplus \ldots \oplus M_n$ и $p_i \nmid p_j$ при $i \neq j$ $(i, j = 1, 2, \ldots, n)$. Да положим

$$\alpha_i = p_1^{k_1} \ldots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \ldots p_n^{k_n} \quad (i = 1, 2, \ldots, n).$$

Очевидно $\alpha_i \in \mathrm{Ann}(b_j)$ при $j \neq i$. Тъй като НОД на елементите $\alpha_1, \alpha_2, \ldots, \alpha_n$ е 1, съществуват такива елементи $\lambda_1, \lambda_2, \ldots, \lambda_n$ от K, че

$$1 = \lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \ldots + \lambda_n \alpha_n.$$

Ще докажем, че цикличният подмодул (a), където $a=\lambda_1 b_1+\lambda_2 b_2+\ldots+\lambda_n b_n$, съвпада с модула M. Затова е достатъчно да покажем, че $b_i \in (a)$ за всяко $i=1, 2, \ldots, n$. Но

$$\alpha_i a=\lambda_1(\alpha_i b_1)+\ldots+\lambda_{i-1}(\alpha_i b_{i-1})+\lambda_i(\alpha_i b_i)+\lambda_{i+1}(\alpha_i b_{i+1})+$$
$$+\ldots+\lambda_n(\alpha_i b_n)=\lambda_1 0+\ldots+\lambda_{i-1}0+\lambda_i \alpha_i b_i+\lambda_{i+1}0+\ldots+$$
$$+\lambda_n 0=(\lambda_i \alpha_i)b_i=\left(1-\sum_{j\neq i}\lambda_j\alpha_j\right)b_i=1b_i-0=b_i,$$

т. е. $b_i=\alpha_i a\in(a)$. Твърдението е доказано.

§ 6. Структурна теорема за крайно породените модули над област на главни идеали

Да припомним, че комутативният пръстен K с единица се нарича *ньотеров*, ако всяка растяща редица от идеали на K се стабилизира на крайно място (глава VI, определение 4).

Нека S е непразно множество от идеали на K. Идеалът $I\in S$ се нарича *максимален елемент в* S, ако за всеки идеал $J\in S$ от $I\subseteq J$ следва $I=J$.

Лема 1. *Всяко непразно множество S от идеали на ньотеровия пръстен K съдържа максимален елемент.*

Доказателство. Да допуснем, че в S няма максимален елемент. Тогава ако I_1 е произволен елемент от S, то I_1 не е максимален в S и затова в S съществува такъв друг елемент I_2, че $I_1\subsetneq I_2$. Понеже I_2 не е максимален в S, то съществува такъв идеал $I_3\in S$, че $I_2\subsetneq I_3$ и т. н. Така се получава безкрайна строго растяща верига $I_1\subsetneq I_2\subsetneq\ldots\subsetneq I_n\subsetneq\ldots$ от идеали в ньотеровия пръстен K, което е невъзможно. Следователно множеството S има максимален елемент. Лемата е доказана.

Тъй като всяка област на главни идеали е ньотеров пръстен, то от предната лема се получава следното твърдение.

Следствие 1. *Всяко непразно множество от идеали на област на главни идеали притежава поне един максимален елемент.*

Определение 9. Ще казваме, че модулът M над пръстена K е *крайно породен*, ако съществуват такива краен брой елементи $x_1, x_2, \ldots, x_n\in M$, че всеки елемент $x\in M$ може да се представи във вида

$$x=\lambda_1 x_1+\lambda_2 x_2+\ldots+\lambda_n x_n \qquad (\lambda_i\in K).$$

В този случай казваме, че елементите на M *се изразяват линейно* (като *линейни комбинации*) чрез $x_1, x_2, \ldots, x_n$. Елементите $x_1, x_2, \ldots, x_n$ се наричат система *образуващи* (или *пораждащи*) на модула M; и записваме $M=(x_1, x_2, \ldots, x_n)$.

Ясно е, че елементите $x_1, x_2, \ldots, x_n$ пораждат модула M точно тогава, когато $M=(x_1)+(x_2)+\ldots+(x_n)$, където (x_i) е цикличният подмодул на M, породен от елемента x_i $(i=1, 2, \ldots, n)$.

Примери

1. Всеки цикличен K-модул е крайно породен и има едноелементна система образуващи.

2. Крайномерните линейни пространства над полето K и само те са крайно породени K-модули над K.

3. Всяка крайна абелева група е крайно породен Z-модул.

Задача. Докажете, че директната сума на краен брой крайно породени модули е крайно породен модул.

Нетривиално съотношение между образуващите $x_1, x_2, \ldots, x_n$ на модула M се нарича всяко равенство в M от вида $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0 (\alpha_i \in K)$, където не всички от коефициентите $\alpha_1, \alpha_2, \ldots, \alpha_n$ са равни на нула. Съотношението $0x_1 + 0x_2 + \ldots + 0x_n = 0$ се нарича *тривиално.*

Твърдение 9. *Ако между образуващите $x_1, x_2, \ldots, x_n$ на модула M няма нетривиално съотношение, то $(x_1), (x_2), \ldots, (x_n)$ са свободни циклични подмодули на M и*

$$M = (x_1) \oplus (x_2) \oplus \ldots \oplus (x_n).$$

Доказателство. Ако $\alpha \in \text{Апп}(x_1)$, то $\alpha x_1 = 0$ и $\alpha x_1 + 0x_2 + \ldots + 0x_n = 0$ е съотношение между $x_1, x_2, \ldots, x_n$. Тъй като по условие между образуващите $x_1, x_2, \ldots, x_n$ няма нетривиално съотношение, то $\alpha = 0$. Следователно $\text{Апп}(x_1) = (0)$ и затова подмодулът (x_1) е свободен цикличен подмодул. По същия начин се доказва, че $\text{Апп}(x_i) = (0)$ и (x_i) е свободен цикличен подмодул на M за $i = 2, 3, \ldots, n$. Ще покажем, че сумата $M = (x_1) + (x_2) + \ldots + (x_n)$ е директна. Наистина нека $x \in M$ и

$$x = y_1 + y_2 + \ldots + y_n = z_1 + z_2 + \ldots + z_n,$$

където $y_i, z_i \in (x_i)$ за $i = 1, 2, \ldots, n$. Тогава $y_i = \lambda_i x_i$ и $z_i = \mu_i x_i$, където $\lambda_i, \mu_i \in K$, а

$$x = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = \mu_1 z_1 + \mu_2 z_2 + \ldots + \mu_n z_n.$$

Оттук получаваме съотношението

$$(\lambda_1 - \mu_1) x_1 + (\lambda_2 - \mu_2) x_2 + \ldots + (\lambda_n - \mu_n) x_n = 0.$$

Следователно $\lambda_1 - \mu_1 = \lambda_2 - \mu_2 = \ldots = \lambda_n - \mu_n = 0$, т. е. $\lambda_1 = \mu_1$, $\lambda_2 = \mu_2, \ldots, \lambda_n = \mu_n$. Така всеки елемент x от M се представя еднозначно като сума на елементи от подмодулите $(x_1), (x_2), \ldots, (x_n)$, т. е. M е тяхна директна сума. Твърдението е доказано.

Ако M е крайно породен модул, то сред крайните системи образуващи на M има такива с най-малък брой елементи, който ще наричаме минимален брой образуващи на модула M. Ако n е минималният брой образуващи на M, то N има поне една система пораждащи с n елемента и M не може да се породи от някоя своя система с по-малък от n на брой елемента. Всяка такава система се нарича *минимална пораждаща система* на M.

Нека n е минималният брой образуващи на крайно породения модул M над областта K на главни идеали. Да означим с

$S(M)$ множеството на всички ненулеви главни идеали на пръстена K, породени от ненулеви елементи на K, които участвуват като коефициенти в нетривиално съотношение на някоя минимална пораждаща система от образуващи на M. С други думи, идеалът $I=(\alpha)$ принадлежи на $S(M)$ точно тогава, когато съществува такава минимална система от образуващи елементи $x_1, x_2, \ldots, x_n$ на M с нетривиално съотношение

$$\alpha_1 x_1+\alpha_2 x_2+\ldots+\alpha_n x_n=0 \quad (\alpha_i \in K), \tag{1}$$

в което $\alpha_1=\alpha$. Ако $S(M)$ не е празното множество $\emptyset$, то съгласно следствие I $S(M)$ притежава поне един максимален елемент.

Да предположим, че $S(M)\neq\emptyset$, идеалът $I_1=(\alpha_1)$ е максимален елемент на $S(M)$ и нека (1) е съответното му нетривиално съотношение на някоя фиксирана минимална система образуващи $x_1, x_2, \ldots, x_n$.

Лема 2. *При горните предположения ако*

$$\beta_1 x_1+\beta_2 x_2+\ldots+\beta_n x_n=0 \quad (\beta_i \in K) \tag{2}$$

е произволно друго нетривиално съотношение за избраната система образуващи $x_1, x_2, \ldots, x_n$, *то* α_1/β_1.

Доказателство. Нека $d=(\alpha_1, \beta_1)=u\alpha_1+v\beta_1$ е най-голям общ делител на α_1 и β_1, където $u, v \in K$. Като умножим (1) с u, а (2) — с v и новополучените равенства съберем, ще получим нетривиалното съотношение

$$dx_1+(u\alpha_2+v\beta_2)x_2+\ldots+(u\alpha_n+v\beta_n)x_n=0.$$

Следователно $(d) \in S(M)$. Понеже d/α_1, то $(d) \supseteq (\alpha_1)$. Оттук поради избора на идеала $I_1=(\alpha_1)$ следва равенството $(d)=(\alpha_1)$. Но тъй като K е област на цялостност, то последното равенство означава, че d и α_1 са асоциирани, т. е $\alpha_1=d\varepsilon$ $(\varepsilon \in K^*)$. Тогава от d/β_1 и $\alpha_1=d\varepsilon$ следва, че α_1/β_1.

Лема 3. *Нека* $y_1, y_2, \ldots, y_n$ *е произволна минимална система образуващи на модула* M, *която притежава нетривиално съотношение*

$$\gamma_1 y_1+\gamma_2 y_2+\ldots+\gamma_n y_n=0 \quad (\gamma_i \in K), \tag{3}$$

където $\gamma_1=\alpha_1$ *и* $I_1=(\alpha_1)$ *е избраният максимален идеал от* $S(M)$. *Тогава* α_1/γ_i *за всяко* $i=2, 3, \ldots, n$.

Доказателство. Нека $d=(\alpha_1, \gamma_2)$ и $\alpha_1=d\alpha_1'$, $\gamma_2=d\gamma_2'$. Тогава елементите $\alpha_1', \gamma_2' \in K$ са взаимно прости и нека $u\alpha_1'+v\gamma_2'=1$ $(u, v \in K)$. Полагаме

$$z_1=\alpha_1' y_1+\gamma_2' y_2,\ z_2=-vy_1+uy_2,\ z_s=y_s \ (s=3, 4, \ldots, n). \tag{4}$$

Тъй като $y_1, y_2, \ldots, y_n$ пораждат модула M, а от (4) и условието $u\alpha_1'+v\gamma_2'=1 \in K$ следва, че те се изразяват линейно чрез $z_1, z_2, \ldots, z_n$, то $M=(z_1, z_2, \ldots, z_n)$. Освен това лесно се проверява, че

$$dz_1+0z_2+\gamma_3 z_3+\ldots+\gamma_n' z_n=0,$$

което е нетривиално съотношение за пораждащите елементи $z_1, z_2, \ldots, z_n$, понеже $d \neq 0$. Следователно $(d) \in S(M)$. Тъй като d/α_1, то $(d) \supseteq (\alpha_1$, и от избора на идеала $I_1=(\alpha_1)$ следва, че $(d)=(\alpha_1)$. Оттук се получава, че $d \sim \alpha_1$, и понеже d/γ_2, то α_1/γ_2. По същия начин се доказва, че α_1 дели $\gamma_3, \gamma_4, \ldots, \gamma_n$. Лемата е доказана.

Следствие 2. *Ако $I_1=(\alpha_1)$ е максимален елемент в $S(M)$ и (1) е съответното му нетривиално съотношение, то α_1 дели $\alpha_2, \alpha_3, \ldots, \alpha_n$.*

Теорема 6 (структурна теорема за крайно породените модули). *Всеки крайно породен модул M над област K на главни идеали се разлага в директна сума на краен брой циклични модули. По-точно ако n е минималният брой образуващи на M, то*

$$M=(y_1) \oplus (y_2) \oplus \ldots \oplus (y_n),$$

където $y_1, y_2, \ldots, y_n$ е такава система образуващи на M, че редът β_i на елемента y_i дели реда β_{i+1} на y_{i+1} за $i=1, 2, \ldots, n-1$.

Доказателство. Нека n е минималният брой образуващи на крайно породения модул M. Теоремата ще докажем с индукция по n. При $n=1$ твърдението на теоремата е очевидно. Нека $n>1$. Ако $S(M)=\emptyset$, то твърдението на първата част на теоремата следва от твърдение 9. Втората й част следва от факта, че анулаторите на свободните циклични модули съвпадат с нулевия идеал $O=(0)$ и 0/0. Нека $S(M) \neq \emptyset$ и $I_1=(\alpha_1)$ е максимален елемент в $S(M)$ със съответно нетривиално съотношение (1). От следствие 2 получаваме, че $\alpha_i=\alpha_1 q_i$ за $i=2, 3, \ldots, n$, където $q_i \in K$. Полагаме $y_1=x_1+q_2x_2+\ldots+q_nx_n$. Тогава от (1) следва, че $\alpha_1 y_1=0$, т. е. $\alpha_1 \in \operatorname{Ann}(y_1)=(\beta_1)$ и $(\alpha_1) \subseteq (\beta_1)$. Понеже $M=(y_1, x_2, \ldots, x_n)$ и $\beta_1 y_1+0x_2+\ldots+0x_n=0$ е нетривиално съотношение, то $(\beta_1) \in S(M)$ и от избора на α_1 следва, че $(\alpha_1)=(\beta_1)$, т. е. $\operatorname{Ann}(y_1)=(\alpha_1)$. Ще докажем, че $M=(y_1) \oplus (x_2, x_3, \ldots, x_n)$.

Действително $M=(y_1)+(x_2, x_3, \ldots, x_n)$. Остава да се покаже, че всеки елемент $m \in M$ по единствен начин се представя във вида $m=\beta' y_1+m'$, където $\beta' \in K$, а $m' \in (x_2, \ldots, x_n)$. Да допуснем, че елементът $m \in M$ има и второ представяне $m=\beta'' y_1+m''$ с $\beta'' \in K$ и $m'' \in (x_2, \ldots, x_n)$. Тогава от равенството

$$(\beta'-\beta'')y_1+(m'-m'')=0$$

ще получим едно съотношение за пораждащите елементи $x_1, x_2, \ldots, x_n$ с коефициент пред x_1, равен на $\beta'-\beta''$. От лема 2 следва, че $\alpha_1/(\beta'-\beta'')$, т. е. $\beta'-\beta''=\alpha_1\alpha_1'$ $(\alpha_1' \in K)$. Тъй като $\alpha_1 y_1=0$, то $(\beta'-\beta'')y_1=0$ и $m'-m''=0$. Следователно $\beta' y_1=\beta'' y_1$ и $m'=m''$, с което еднозначността на представянето на m е установена.

Като приложим индукция по n, за подмодула $(x_2, x_3, \ldots, x_n$ получаваме разлагането

$$(x_2, x_3, \ldots, x_n)=(y_2) \oplus (y_3) \oplus \ldots \oplus (y_n),$$

където редът β_i на елемента y_i дели реда β_{i+1} на елемента y_{i+1} за $i=2, 3, \ldots, n-1$. Тогава $M=(y_1)\oplus(y_2)\oplus\ldots\oplus y_n$. Понеже бе показано, че $(\alpha_1)=(\beta_1)=\mathrm{Ann}(y_1)$, то остава да поверим, че α_1/β_2. Но това се получава от очевидното нетривиално съотношение $\alpha_1 y_1 + \beta_2 y_2 + \ldots + \beta_n y_n = 0$ и следствие 2. Теоремата е доказана.

Ако модулът M е разложен в директна сума $M=M_1\oplus M_2\oplus\ldots\oplus M_s$ и $M_{r+1}=M_{r+2}=\ldots=M_s=(0)$, то $M=M_1\oplus M_2\oplus\ldots\oplus M_r$. С други думи, от произволна директна сума можем да отстраняваме нулевите директни събираеми. Ще отбележим, че ако M е ненулев модул, то полученото в предната теорема разлагане на M в директна сума на циклични подмодули няма нулеви директни събираеми. Тук възниква въпросът за еднозначност на това разлагане. Отговор на този въпрос дава следната теорема, която ще приведем без доказателство.

Теорема 7. *Ако ненулевият крайно породен модул M над областта K на главни идеали е разложен по два начина на ненулеви циклични модули* $M=(v_1)\oplus(v_2)\oplus\ldots\oplus(v_n)=(w_1)\oplus(w_2)\oplus\ldots\oplus(w_m)$ *и редът* β_i *на* v_i *дели реда* β_{i+1} *на* v_{i+1} *за* $i=1, 2, \ldots, n-1$, *редът* γ_j *на* w_j *дели реда* γ_{j+1} *на* w_{j+1} *за* $j=1, 2, \ldots, m-1$, то $n=m$ и β_i *е асоциран с* γ_j *за* $i=1, 2, \ldots, n$.

По този начин елементите $\beta_1, \beta_2, \ldots, \beta_n$ еднозначно определят разлагането на модула M, дадено в теорема 6. Те се наричат инвариантни множители на модула M.

От теорема 6 и твърдение 7 се получава следната теорема:

Теорема 8. *Всеки ненулев крайно породен модул M над област K на главни идеали се разлага в директна сума на краен брой свободни циклични и примарни модули, т. е. M се разлага в крайна директна сума на неразложими ненулеви циклични подмодули.*

Наистина съгласно теорема 6 M се разлага в директна сума на ненулеви циклични подмодули. Тези циклични подмодули са или свободни, циклични, или примарни, или ако не са от тези два вида, съгласно твърдение 7 те ще се разлагат в директна сума на краен брой примарни циклични подмодули. След заместването на последните с техните разлагания в разлагането на модула M прилагаме теоремата за транзитивността на разлагането (теорема 1) и получаваме твърдението на теоремата.

За разлагането на крайно породен модул в директна сума на неразложими циклични подмодули е в сила следната теорема.

Теорема 9 (теорема за единственост на разлагането). *Ако M е произволен крайно породен модул над областта K на главни идеали, то във всяко разлагане на модула M в директна сума на неразложими ненулеви циклични модули броят на свободните циклични събираеми и броят на примарните циклични събираеми с образуващи от даден ред са постоянни, независещи от самото разлагане.*

Доказателството на тази теорема не привеждаме, но ще отбележим, че тя е еквивалентна на теорема 7, т. е. всяка една от тях може да се получи от другата.

§ 7. Едно приложение на структурната теорема за крайните абелеви групи

Особено важна е структурната теорема за крайно породените модули, когато основният пръстен е пръстенът Z на целите числа. В този случай структурната теорема дава пълна характеризация на крайно породените абелеви групи, а именно крайните директни суми на неразложими циклични групи и само те са крайно породени абелеви групи. Ако G е крайна абелева група, то в G няма безкрайна циклични подгрупи (свободни циклични Z-модули) и затова от структурната теорема следва, че G е директна сума на циклични p_i-групи за краен брой прости числа p_i (простите делители на реда $|G|$ на G). В този параграф ще изложим едно приложение на структурната теорема за крайните абелеви групи.

Лема 4. *Адитивно записаната крайна абелева група G е циклична тогава и само тогава, когато е изпълнено следното условие:*

(i) за всяко цяло положително число n уравнението $nx=0$ (вдясно е нулата на групата G) има не повече от n различни решения в групата G.

Доказателство. Нека G е крайна циклична група, а G_n е подмножеството на G, съставено от решенията на уравнението $nx=0$, т. е.

$$G_n=\{g|g\in G,\ ng=0\}.$$

Очевидно G_n е подгрупа на цикличната група G. Но всяка подгрупа на цикличната група е циклична и затова G_n е циклична подгрупа. Нека a е образуващ елемент на G_n. Тъй като $a\in G_n$, то $na=0$, т. е. редът на a дели числото n. Но редът на a е равен на реда на цикличната група, породена от a, т. е. редът на a е равен на реда $|G_n|$ на подгрупата G_n. Следователно $|G_n|$ дели числото n и затова $|G_n|\leqq n$.

Нека за адитивно записаната крайна абелева група G е изпълнено условието (i). Да допуснем, че G не е циклична група. Според структурната теорема крайната абелева група G се разлага в директна сума на примарни циклични подгрупи. В това разлагане ще съществуват поне две директни примарни събираеми, които имат редове, равни на степени на едно и също просто число p. В противен случай съгласно твърдение 8 групата G би била циклична. Следователно в групата G имаме подгрупа от вида $G_1\oplus G_2$, където G_i е циклична група от ред p^{s_i} $(i=1, 2)$. Нека a_i е образуващ елемент на цикличната група G_i $(i=1, 2)$. Елементите от вида $kp^{s_1-1}a_1+lp^{s_2-1}a_2$, $0\leqq k<p$, $0\leqq l<p$ са различни и образуват множество от p^2 на брой елементи. Но всеки елемент от вида $kp^{s_1-1}a_1+lp^{s_2-1}a_2$ е решение на уравнението $px=0$, т. е. последното уравнение има в G поне p^2 решения. Достигнахме до противоречие, което се дължи на допускането, че G не е циклична. Лемата е доказана.

Всяка адитивно записана абелева група е изоморфна на мултипликативно записана абелева група. Затова лема 4 може да бъде формулирана и за мултипликативно записани крайни абелеви групи по следния начин.

Лема 5. *Мултипликативно записаната крайна абелева група G е циклична тогава и само тогава, когато за всяко естествено число n уравнението $x^n=1$ (вдясно е единицата на групата G) има не повече от n различни решения в G.*

Теорема 10. *Нека A е произволна област на цялостност. Всяка крайна подгрупа на мултипликативната група A^* на пръстена A е циклична.*

Доказателство. Областта A на цялостност е подпръстен на своето поле $\bar{A}$ от частни (виж § 10 от глава V). Нека G е произволна крайна подгрупа на групата A^*. За всяко цяло положително число n уравнението $x^n=1$ има не повече от n решения в полето $\bar{A}$ (виж теорема 8 от глава VIII) и затова има не повече от n решения и в групата G. Тогава съгласно лема 5 групата G е циклична.

Следствие 3. *Ако P е произволно крайно поле, то мултипликативната му група P^* е циклична.*

Следствие 4. *Корените на полинома x^n-1, които се съдържат в полето P, образуват циклична подгрупа на мултипликативната му група P^*.*

Доказателство. Множеството $P(n)$ от корените на полинома $f(x)=x^n-1$, които се съдържат в полето P, има не повече от n елемента. Понеже нулата на P не принадлежи на $P(n)$, то $P(n)\subseteq P^*$. Ако α и β са два произволни елемента на $P(n)$, то

$$f(\alpha\beta^{-1})=(\alpha\beta^{-1})^n-1=\frac{\alpha^n}{\beta^n}-1=1-1=0,$$

т. е. $\alpha\beta^{-1}\in P(n)$ и затова $P(n)$ е подгрупа на P^*, при това крайна. От теорема 10 следва, че $P(n)$ е циклична подгрупа на P^*. Следствието е доказано.

В частност отново получихме, че мултипликативната група $\mathbf{C}(n)$ на корените на единицата от степен n в полето $\mathbf{C}$ на комплексните числа е циклична. Естествено последният факт се доказва просто, ако се използува формулата на Моавър.

Нека отбележим, че полето P не е задължено да съдържа всичките корени на полинома x^n-1. Например полиномът x^4-1 има два корена ± 1 в полето $\mathbf{R}$ на реалните числа, но 4 корена ± 1, $\pm i$ в полето $\mathbf{C}$ на комплексните числа.

ГЛАВА X

НОРМАЛНА ФОРМА НА ЛИНЕЙНИТЕ ПРЕОБРАЗУВАНИЯ

В настоящата глава ще се спрем на някои въпроси, които се отнасят към линейната алгебра. Основното поле ще бъде полето на комплексните числа и ще разглеждаме само крайномерни комплексни линейни пространства.

Да припомним някои резултати от общия курс по линейна алгебра, които ще ни бъдат необходими в бъдеще.

Нека V е произволно комплексно линейно пространство с размерност n и φ е произволно линейно преобразуване на V. Ако системата вектори $e_1, e_2, \ldots, e_n$ е базис на пространството V и

$$
\begin{aligned}
\varphi(e_1) &= \alpha_{11} e_1 + \alpha_{21} e_2 + \ldots + \alpha_{n1} e_n, \\
\varphi(e_2) &= \alpha_{12} e_1 + \alpha_{22} e_2 + \ldots + \alpha_{n2} e_n, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\varphi(e_n) &= \alpha_{1n} e_1 + \alpha_{2n} e_2 + \ldots + \alpha_{nn} e_n,
\end{aligned} \tag{1}
$$

то квадратната матрица $A=(\alpha_{ij})$ се нарича *матрица на линейното преобразуване* φ относно базиса $e_1, e_2, \ldots, e_n$. Обратно, ако $A=(\alpha_{ij})$ е произволна комплексна матрица от ред n, то равенствата (1) определят напълно линейното преобразуване φ на V. Нека $f_1, f_2, \ldots, f_n$ е друг базис на пространството V и

$$
\begin{aligned}
f_1 &= \tau_{11} e_1 + \tau_{21} e_2 + \ldots + \tau_{n1} e_n, \\
f_2 &= \tau_{12} e_1 + \tau_{22} e_2 + \ldots + \tau_{n2} e_n, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
f_n &= \tau_{1n} e_1 + \tau_{2n} e_2 + \ldots + \tau_{nn} e_n.
\end{aligned} \tag{2}
$$

Матрицата $T=(\tau_{ij})$ се нарича *матрица на прехода* от базиса $e_1, e_2, \ldots, e_n$ към базиса $f_1, f_2, \ldots, f_n$. Ако $B=(\beta_{ij})$ е матрица на линейното преобразуване φ в базиса $f_1, f_2, \ldots, f_n$, то матриците A и B са свързани с равенствата $A=TBT^{-1}$ и $B=T^{-1}AT$, т. е. матриците на едно и също линейно преобразуване в два базиса на пространството са подобни. Обратно, ако матриците $A=(\alpha_{ij})$ и $B=(\beta_{ij})$ са подобни и $A=TBT^{-1}$, те задават едно и също преобразуване в два базиса на пространството, а именно ако A задава φ в базиса $e_1, e_2, \ldots, e_n$, то B ще задава същото преобразуване в базиса $f_1, f_2, \ldots, f_n$, определен с равенствата (2).

Матрицата $A-\lambda E$, където λ е неизвестно и E — единичната матрица от ред n, се нарича *характеристична матрица* на матрицата A; детерминантата $|A-\lambda E|$ на характеристичната матрица се нарича *характеристичен полином* на A (на линейното преобразуване φ), а корените на характеристичния полином — *характеристични корени* на A (на φ).

Ненулевият вектор v на пространството V се нарича *собствен вектор* на преобразуването φ, който съответствува на собствената стойност λ_0 от C, ако е изпълнено равенството $\varphi(v)=\lambda_0 v$. Характеристичните корени на преобразуването φ и само те са собствени стойности на φ. Подобните матрици имат един и същ характеристичен полином и затова — едни и същи характеристични корени.

Казваме, че линейното преобразуване φ е с *прост спектър*, ако характеристичните му корени са два по два различни. Ако φ е преобразуване с прост спектър, в пространството V съществува базис, съставен от собстени вектори на φ, т. е. базис, в който матрицата на φ е диагонална.

Във връзка с приведените по-горе резултати възникват следните въпроси, които имат особено важно значение както за теоретическите изследвания, така и за практическите приложения на линейната алгебра.

1. Може ли за всяко линейно преобразуване φ на комплексното линейно пространство V да се намери такъв базис, че в този базис φ да има възможно най-просто записване, т. е. матрицата му в този базис да има възможно най-прост вид?

2. Възможно ли е да се намери критерий, кога две произволни комплексни матрици от ред n са подобни?

3. Ако отговорът на горните въпроси е утвърдителен, може ли да се намери ефективен метод за решаването им?

Именно тези въпроси ще разгледаме в настоящата глава.

На първия въпрос засега можем да отговорим само в частния случай, когато преобразуването φ има прост спектър. Пълният отговор на този въпрос ще получим като едно естествено приложение на структурната теорема за крайно породените модули над област на главни идеали, а отговорите на другите два въпроса — след като развием теорията на λ-матриците.

§ 1. Построяване на модул над пръстен на полиноми с помощта на линейно пространство с фиксирано линейно преобразуване

С $C[\lambda]$ ще означим пръстена на полиномите с комплексни коефициенти на променливата λ.

Твърдение 1. *Пръстенът* $C[\lambda]$ *е пръстен на главни идеали, а простите му елементи са полиномите от вида* $p(\lambda)=\lambda-\lambda_0$ $(\lambda_0 \in C)$ *и техните асоциирани.*

Доказателство. Първото твърдение следва от пример 4 на § 2 и твърдение 3 на глава VI.

Очевидно е, че всички полиноми от вида $\lambda-\lambda_0$ $(\lambda_0 \in C)$ и асоциираните с тях са прости елементи в $C[\lambda]$ (т. е. неразложими полиноми в $C[\lambda]$).

Обратно, нека $p(\lambda)$ е произволен прост елемент на пръстена $C[\lambda]$, т. е. $p(\lambda)\neq 0$ и $p(\lambda)$ не допуска истинско разлагане. Сте-

лента на полинома $p(\lambda)$ не е нула, тъй като $p(\lambda)$ е необратим елемент в $C[\lambda]$. По теоремата на Даламбер за съществуване на корен полономът $p(\lambda)$ има поне един комплексен корен λ_0. Но тогава полиномът $\lambda-\lambda_0$ дели $p(\lambda)$, т. е.

$$p(\lambda)=(\lambda-\lambda_0)q(\lambda),$$

където $q(\lambda)$ е полином от $C[\lambda]$. Степента на $q(\lambda)$ не може да бъде различна от нула, защото в противен случай равлагането $p(\lambda)=(\lambda-\lambda_0)q(\lambda)$ би било истинско в противоречие с простотата на $p(\lambda)$. Следователно $\deg q(\lambda)=0$ и затова $q(\lambda)$ е различно от нула комплексно число, т. е. обратим елемент в $C[\lambda]$. С това показахме, че $p(\lambda)$ е асоцииран с полинома $\lambda-\lambda_0$. Твърдението е доказано.

Да напомним, че пръстенът $C[\lambda]$ може да се разглежда като линейно пространство над полето C с базис

$$\lambda^0=1,\ \lambda,\ \lambda^2,\ldots,\ \lambda^n,\ldots,$$

т. е. $C[\lambda]$ е безкрайномерно линейно пространство над полето C.

Нека M е произволен модул над пръстена $C[\lambda]$. Тъй като полето C на комплексните числа е подпръстен на пръстена $C[\lambda]$, то M е линейно пространство над полето C. Наистина умножението на комплексните числа с елементи на модула M е напълно определено, защото комплексните числа са едновременно и полиноми, а аксиомите за линейно пространство автоматически следват от аксиомите за модул. Тази двояка възможност да разглеждаме комплексните числа и като полиноми ни позволява да твърдим, че *ако* $\varphi: M\to N$ *е модулен изоморфизъм на* M *върху модула* N *над.* $C[\lambda]$, *то* φ *е изоморфизъм на комплексното пространство* M *върху комплексното пространство* N. В частност свободният цикличен $C[\lambda]$-модул M е изоморфен на $C[\lambda]$-модула $C[\lambda]$ (виж теорема 4 на глава IX), който е безкрайномерно линейно пространство над C. Следователно M е безкрайномерно пространство над полето C. Така получихме следното твърдение.

Твърдение 2. *Всеки свободен цикличен модул над пръстена* $C[\lambda]$ *е безкрайномерно линейно пространство над полето* C *на комплексните числа.*

Нека V е произволно крайномерно линейно пространство над полето C с размерност n. Да означим с $\mathrm{Hom}(V, V)$ множеството от всички линейни преобразувания на пространството V. От курса по линейна алгебра знаем, че в множеството $\mathrm{Hom}(V, V)$ може да се дефинират следните операции:

1) умножение на комплексно число с линейно преобразуване;

2) събиране на линейни преобразувания;

3) умножение на линейни преобразувания.

При това произведението на число с линейно преобразувание, сумата и произведението на две линейни преобразувания са линейни преобразувания.

Задача. Докажете, че множеството $\mathrm{Hom}(V, V)$ с операциите умножение на линейни преобразувания с комплексни числа и събиране на линейни преобразувания е линейно пространство над полето C.

Задача. Докажете, че множеството $\mathrm{Hom}(V, V)$ с операциите събиране и умножение на линейни преобразувания е пръстен.

Задача. Нека $e_1, e_2, \ldots, e_n$ е произволен базис на пространството V. Докажете, че съответствието, което съпоставя на всяко преобразуване неговата матрица в базиса $e_1, e_2, \ldots, e_n$, е изоморфизъм на пръстена $\mathrm{Hom}(V, V)$ върху пръстена $M(n, \mathbf{C})$ на всички квадратни матрици от ред n с комплексни елементи. Покажете още, че това съответствие е изоморфизъм на линейните пространства $\mathrm{Hom}(V, V)$ и $M(n, \mathbf{C})$.

Определение 1. Нека V е произволно комплексно пространство, а φ — линейно преобразуване на V. Подпространството W на пространството V се нарича *инвариантно подпространство* спрямо преобразуването φ, ако за всеки вектор w от подпространството W векторът $\varphi(w)$ се съдържа в W.

Примери

1. Нулевото подпространство и цялото пространство са инвариантни подпространства спрямо всяко линейно преобразуване.

2. Знаем, че $\mathbf{C}[\lambda]$ е безкрайномерно комплексно пространство. Нека φ е преобразуването, което съпоставя на всеки полином $f(\lambda)=a_n\lambda^n+a_{n-1}\lambda^{n-1}+\ldots+a_1\lambda+a_0$ неговата производна $f'(\lambda)=na_n\lambda^{n-1}+(n-1)a_{n-1}\lambda^{n-2}+\ldots+2a_2\lambda+a_1$, т. е.

$$\varphi[f(\lambda)]=f'(\lambda).$$

Очевидно е, че преобразуването φ е линейно. Да означим с P_n подпространството на пространството $\mathbf{C}[\lambda]$, съставено от всички полиноми от степен, която не надминава n. Тъй като производната на всеки полином има степен, по-малка от степента на полинома, то P_n е инвариантно подпространство относно φ. От друга страна, подпространството $(\lambda)=\{a\lambda \mid a\in\mathbf{C}\}$, породено от полинома λ, не е инвариантно спрямо φ, тъй като $\varphi(\lambda)=1$ и 1 не се съдържа в това подпространство.

Задача. Докажете, че освен подпространствата P_n $(n=0, 1, 2, \ldots)$ в примера 2 няма други инвариантни подпространства.

В бъдеще с ε ще означаваме тъждественото преобразуване на пространството V, т. е. $\varepsilon(v)=v$ за всяко $v\in V$, а единичната матрица — с E или с E_n, когато се налага да посочим, че редът ѝ е n.

Нека V е крайномерно комплексно пространство с размерност n, а φ — линейно преобразуване в пространството V. Ако

$$f(\lambda)=a_m\lambda^m+a_{m-1}\lambda^{m-1}+\ldots+a_1\lambda+a_0$$

е произволен полином от $\mathbf{C}[\lambda]$, то

$$f(\varphi)=a_m\varphi^m+a_{m-1}\varphi^{m-1}+\ldots+a_1\varphi+a_0\varepsilon$$

е линейно преобразуване в пространството V. Това ни дава възможност да определим произведение на полинома $f(\lambda)$ с вектор v от V, като положим

$$f(\lambda)v = f(\varphi)(v),$$

т. е. $f(\lambda)v$ е образът на вектора v при линейното преобразуване $f(\varphi)$.

Не е трудно да се провери, че линейното пространство V с операцията събиране на вектори и с така определеното умножение на елементи от V с елементи от пръстена $C[\lambda]$ се превръща в модул над $C[\lambda]$, т. е. че за всеки два полинома $f(\lambda)$ и $g(\lambda)$ от $C[\lambda]$ и за всеки два вектора u и v от V са изпълнени равенствата:

1) $[f(\lambda)+g(\lambda)]u = f(\lambda)u + g(\lambda)u$;
2) $f(\lambda)(u+v) = f(\lambda)u + f(\lambda)v$;
3) $[f(\lambda)g(\lambda)]u = f(\lambda)[g(\lambda)u]$;
4) $1 \cdot u = u$.

Ще казваме, че линейното пространство V *е превърнато в модул над* $C[\lambda]$ посредством линейното преобразуване φ.

Ще отбележим някои от свойствата на така построения модул.

Твърдение 3. *Инвариантните подпространства на V спрямо линейното преобразуване φ и само те са подмодули на V, превърнато в модул над $C[\lambda]$ посредством φ.*

Доказателство. Нека M е инвариантно подпространство на V. Ако u, v са два вектора от M, а c е произволно комплексно число, то векторите $u+v$ и cu принадлежат на M, тъй като M е подпространство. За всяко цяло положително число m векторът $\varphi^m(u)$ принадлежи на M. При $m=1$ това е така, защото M е инвариантно относно φ. Да предположим, че за $m-1$ твърдението е доказано, т. е. $\varphi^{m-1}(u) \in M$. Тогава $\varphi^m(u) = \varphi[\varphi^{m-1}(u)]$ и поради инвариантността на M спрямо φ векторът $\varphi^m(u)$ ще бъде от M. Нека

$$f(\lambda) = a_m\lambda^m + a_{m-1}\lambda^{m-1} + \ldots + a_1\lambda + a_0$$

е произволен полином от $C[\lambda]$. Тогава

$$f(\lambda)u = f(\varphi)(u) = a_m\varphi^m(u) + a_{m-1}\varphi^{m-1}(u) + \ldots + a_1\varphi(u) + a_0u,$$

т. е. векторът $f(\lambda)u$ е сума на вектори от M и затова той се съдържа в M. Съгласно твърдение 1 от глава IX инвариантното подпространство M е подмодул на V.

Обратно, нека M е подмодул на пространството V, превърнато в модул над $C[\lambda]$ посредством φ. Ако u и v са два вектора от M, а c — произволно комплексно число, то $u+v$ и cu са вектори от M, защото M е подмодул. Но това означава, че M е подпространство на подпространството V. По същите причини векторът $\lambda u = \varphi(u)$ е елемент от M, т. е. M е инвариантно подпространство на V. Твърдението е доказано.

Твърдение 4. *Крайномерното комплексно линейно про-*

странство V, превърнато в $\mathbf{C}[\lambda]$-модул над пръстен $\mathbf{C}[\lambda]$ посредством линейното преобразуване φ, е крайно породен модул, който се разлага в директна сума на краен брой примарни циклични подмодули.

Доказателство. Ако $e_1, e_2, \ldots, e_n$ е един базис в пространството V, то всеки вектор от V е линейна комбинация на векторите $e_1, e_2, \ldots, e_n$ с коефициенти от полето $\mathbf{C}$, т. е. с коефициенти от пръстена $\mathbf{C}[\lambda]$. Затова $e_1, e_2, \ldots, e_n$ е една система образуващи на модула V над $\mathbf{C}[\lambda]$, т. е. V е крайно породен модул. $\mathbf{C}[\lambda]$-модулът V не може да съдържа свободен цикличен подмодул L, тъй като L съгласно твърдение 3 ще бъде безкрайномерно линейно пространство над $\mathbf{C}$, т. е. пространството V над $\mathbf{C}$ би било безкрайномерно.

Пръстенът $\mathbf{C}[\lambda]$ е пръстен на главни идеали, а модулът V — краен породен модул над $\mathbf{C}[\lambda]$. По структурната теорема за крайно породените модули над област на главни идеали модулът V се разлага в директна сума на краен брой свободни циклични и примарни циклични подмодули. Но модулът V не съдържа свободни циклични подмодули. Следователно модулът V се разлага в директна сума на краен брой примарни циклични подмодули.

Забележка. Лесно се вижда, че всички резултати от този параграф с изключение само на твърдение 1 остават в сила и ако заменим полето $\mathbf{C}$ с произволно поле P.

§ 2. Линейни преобразувания, които имат за свои матрици жорданови клетки

Нека $e_1, e_2, \ldots, e_n$ е произволен базис на n-мерното линейно пространство V, λ_0 — произволно комплексно число, а φ — линейното преобразуване на пространството V, определено с равенствата

$$\begin{aligned}
\varphi(e_1) &= \lambda_0 e_1 + e_2,\\
\varphi(e_2) &= \lambda_0 e_2 + e_3,\\
&\cdots\cdots\cdots\\
\varphi(e_{n-1}) &= \lambda_0 e_{n-1} + e_n,\\
\varphi(e_n) &= \lambda_0 e_n.
\end{aligned} \tag{1}$$

Матрицата A на линейното преобразуване φ в дадения базис има вида

$$A = \begin{pmatrix}
\lambda_0 & 0 & 0 & \ldots & 0 & 0\\
1 & \lambda_0 & 0 & \ldots & 0 & 0\\
0 & 1 & \lambda_0 & \ldots & 0 & 0\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
0 & 0 & 0 & \ldots & \lambda_0 & 0\\
0 & 0 & 0 & \ldots & 1 & \lambda_0
\end{pmatrix}. \tag{2}$$

Всяка матрица от този вид се нарича *жорданова клетка* (с характеристичен корен λ_0).

Твърдение 5. *Собствените вектори на линейното преобразуване φ на n-мерното пространство V, което има жорданова клетка за своя матрица, са само ненулевите вектори, пропорционални на e_n.*

Доказателство. Очевидно е, че единствената собствена стойност на линейното преобразуване φ е λ_0. От линейната алгебра е известно, че координатните редове $(x_1, x_2, \ldots, x_n)$ на собствените вектори на φ (които принадлежат на собственото значение λ_0) удовлетворяват уравнението

$$(A-\lambda_0 E)\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}=0,$$

т. е. системата уравнения

$$x_1=0,\ x_2=0,\ \ldots,\ x_{n-1}=0.$$

Следователно собствените вектори $x_1e_1+x_2e_2+\ldots+x_ne_n$ на φ са пропорционални на вектора e_n.

Задача. Да се намерят всички инвариантни подпространства на V относно преобразуването φ, зададено с равенствата (1).

Твърдение 6. *Нека линейното преобразуване φ се задава в базиса $e_1, e_2, \ldots, e_n$ на комплексното пространство V с жорданова клетка с характеристичен корен λ_0. Тогава линейното пространство V, превърнато в модул над пръстена $\mathbf{C}[\lambda]$ посредством φ, е примарен цикличен модул спрямо простия елемент $p(\lambda)=\lambda-\lambda_0$ и векторът e_1 е негов образуващ елемент.*

Доказателство. Нека преобразуването φ има матрицата (2) в базиса $e_1, e_2, \ldots, e_n$. Тогава са в сила равенствата (1), които могат да се запишат в модула V по следния начин:

$$\begin{aligned} e_2&=(\lambda-\lambda_0)e_1=p(\lambda)e_1,\\ e_3&=(\lambda-\lambda_0)e_2=p(\lambda)e_2,\\ &\cdots\cdots\cdots\\ e_n&=(\lambda-\lambda_0)e_{n-1}=p(\lambda)e_{n-1},\\ 0&=(\lambda-\lambda_0)e_n=p(\lambda)e_n. \end{aligned}$$

Като заместим e_2 във второто равенство с $p(\lambda)e_1$, след това e_3 — в третото равенство с $p^2(\lambda)e_1$ и т. н., получаваме

$$e_k=(\lambda-\lambda_0)^{k-1}e_1=p^{k-1}(\lambda)e_1\ \ (k=2,\ 3,\ \ldots,\ n),$$

$$0=(\lambda-\lambda_0)^n e_1=p^n(\lambda)e_1.$$

От последното равенство следва, че полиномът $p^n(\lambda)=(\lambda-\lambda_0)^n$ е елемент от анулатора $\mathrm{Ann}(e_1)$ на вектора e_1.

Нека сега $x=\beta_1e_1+\beta_2e_2+\ldots+\beta_ne_n$ е произволен вектор от V. Тогава

$$x=\beta_1 e_1+\beta_2 p(\lambda) e_1+\beta_3 p^2(\lambda) e_1+\ldots+\beta_n p^{n-1}(\lambda) e_1=f(\lambda) c_1,$$

където с $f(\lambda)$ сме означили полинома $\beta_1+\beta_2 p(\lambda)+\ldots+\beta_n p^{n-1}(\lambda)$. Следователно пространството V е цикличен модул над областта $\mathbf{C}[\lambda]$ на главни идеали с образуващ елемент e_1. Тъй като $p^n(\lambda)\in \mathrm{Ann}(e_1)$, редът на образуващия елемент e_1 на V е степен на простия елемент $p(\lambda)=\lambda-\lambda_0$. Следователно V е примарен цикличен модул спрямо простия елемент $p(\lambda)=\lambda-\lambda_0$ на пръстена $\mathbf{C}[\lambda]$ (виж определение 7 от глава IX). Твърдението е доказано.

Задача. Докажете, че анулаторът на вектора e_1 от горното твърдение се поражда от полинома $(\lambda-\lambda_0)^n$.

Следващото твърдение е обратно на твърдение 6.

Твърдение 7. *Нека V е примарен цикличен модул над пръстена $\mathbf{C}[\lambda]$ спрямо простия елемент $\lambda-\lambda_0$. Ако e_1 е образуващ елемент на модула V и анулаторът му $\mathrm{Ann}(e_1)$ се поражда от полинома $(\lambda-\lambda_0)^n$, то векторите e_1, $e_2=(\lambda-\lambda_0)e_1$, $e_3=(\lambda-\lambda_0)^2 e_1,\ldots, e_n=(\lambda-\lambda_0)^{n-1} e_1$ образуват базис на линейното пространство V над $\mathbf{C}$ и за тях са изпълнени равенствата*

$$\begin{aligned}
\lambda e_1&=\lambda_0 e_1+e_2,\\
\lambda e_2&=\lambda_0 e_2+e_3,\\
&\ldots\ldots\\
\lambda e_{n-1}&=\lambda_0 e_{n-1}+e_n,\\
\lambda e_n&=\lambda_0 e_n.
\end{aligned}$$

Доказателство. Ще покажем най-напред, че векторите $e_1, e_2,\ldots, e_n$ са свързани с горните равенства. Наистина ако $1\leqq k\leqq n-1$, то

$$\begin{aligned}
\lambda_0 e_k+e_{k+1}&=\lambda_0(\lambda-\lambda_0)^{k-1} e_1+(\lambda-\lambda_0)^k e_1=\\
&=(\lambda-\lambda_0)^{k-1}\lambda e_1=\lambda[(\lambda-\lambda_0)^{k-1} e_1]=\lambda e_k.
\end{aligned}$$

Освен това

$$\lambda e_n-\lambda_0 e_n=(\lambda-\lambda_0)e_n=(\lambda-\lambda_0)[(\lambda-\lambda_0)^{n-1} e_1]=(\lambda-\lambda_0)^n e_1=0,$$

тъй като $(\lambda-\lambda_0)^n\in \mathrm{Ann}(e_1)$.

Нека v е произволен елемент от V. Понеже e_1 е образуващ елемент на цикличния модул V, то

$$v=f(\lambda) e_1$$

за някой полином

$$f(\lambda)=a_r\lambda^r+a_{r-1}\lambda^{r-1}+\ldots+a_1\lambda+a_0$$

от пръстена $\mathbf{C}[\lambda]$. От формулата на Тейлър следва равенството

$$f(\lambda)=b_0+b_1(\lambda-\lambda_0)+b_2(\lambda-\lambda_0)+\ldots+b_r(\lambda-\lambda_0)^r,$$

където $b_i=\frac{1}{i!} f^{(i)}(\lambda_0)$. Тогава

$$v=f(\lambda) e_1=\left[\sum_{i=0}^{r} b_i(\lambda-\lambda_0)^i\right] e_1=\sum_{i=0}^{r} b_i(\lambda-\lambda_0)^i e_1=$$

$$= \sum_{i=0}^{n-1} b_i(\lambda-\lambda_0)^i e_1 + \sum_{i=n}^{r} b_i(\lambda-\lambda_0)^i e_1 =$$

$$= \sum_{i=0}^{n-1} b_i e_{i+1} = \sum_{j=1}^{n} b_{j-1} e_j,$$

т. е. векторът v е линейна комбинация на векторите $e_1, e_2, \ldots, e_n$. Да допуснем, че системата вектори $e_1, e_2, \ldots, e_n$ е линейно зависима. В такъв случай ще съществува такава система от комплексни числа $\alpha_1, \alpha_2, \ldots, \alpha_n$, поне едно от които е различно от нула, че да бъде изпълнено равенството

$$\alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n = 0. \tag{3}$$

Като използуваме очевидната рекурентна зависимост $(\lambda-\lambda_0)e_i = e_{i+1}$ $(i=1, 2, \ldots, n-1)$ и това, че $(\lambda-\lambda_0)e_n=0$, чрез последователно умножаване на равенството (3) с $\lambda-\lambda_0$, $(\lambda-\lambda_0)^2, \ldots,$ $(\lambda-\lambda_0)^{n-1}$ получаваме равенствата

$$\begin{gathered}
\alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_{n-1} e_{n-1} + \alpha_n e_n = 0, \\
\alpha_1 e_2 + \alpha_2 e_3 + \ldots \alpha_{n-1} e_n = 0, \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha_1 e_{n-1} + \alpha_2 e_n = 0, \\
\alpha_1 e_n = 0.
\end{gathered}$$

Тъй като e_n е ненулев вектор, от последното равенство следва че $\alpha_1=0$. Но тогава от предпоследното следва $\alpha_2=0$, от предхождащото го — $\alpha_3=0$ и т. н., от първото следва $\alpha_n=0$. Следователно числата $\alpha_1, \alpha_2, \ldots, \alpha_n$ са равни на нула, което противоречи на предположението, че поне едно от тях е различно от 0. За системата вектори $e_1, e_2, \ldots, e_n$ доказахме, че е линейно независима и че всеки вектор на пространството V е тяхна линейна комбинация, т. е. тази система вектори е базис на V. Твърдението е доказано.

§ 3. Теорема на Жордан за привеждане на линейно преобразуване в нормална форма

Вече сме в състояние да дадем пълен отговор на първия въпрос, поставен в началото на настоящата глава.

За линейното преобразуване φ с прост спектър винаги може да се избере базис от собствени вектори на φ. В този базис матрицата на φ е диагонална. Но не за всяко линейно преобразуване на едно комплексно пространство може да се намери базис от собствени вектори. Естествено това може да се случи само тогава, когато линейното преобразуване φ има многократни характеристични корени.

Пример. Нека W е двумерно комплексно пространство с базис e_1, e_2, а φ е линейното преобразуване, дефинирано с равенствата

$$\varphi(e_1)=e_2,\ \varphi(e_2)=0.$$

Матрицата на φ в базиса e_1, e_2 е жордановата клетка

$$\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}.$$

Очевидно φ има един двукратен характеристичен корен $\lambda_1=\lambda_2=0$. Съгласно твърдение 5 всеки собствен вектор на φ е пропорционален на вектора e_2. Следователно в пространството W не съществува базис, съставен от собствени вектори на преобразуването φ, т. е. в никой базис на W матрицата на φ не може да бъде диагонална.

Определение 2. Всяка квадратна матрица A от вида

$$A=\begin{pmatrix}A_1 & & & 0\\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_m\end{pmatrix}, \tag{1}$$

където $A_1, A_2, \ldots, A_m$ са жорданови клетки, а останалите елементи на A са равни на нула, се нарича *жорданова матрица*.

Примери

1. Всяка жорданова клетка е жорданова матрица. В частност матрицата на преобразуването φ от приведения по-горе пример е жорданова.

2. Всяка диагонална матрица е жорданова и нейните клетки са от първи ред.

Определение 3. Ако V е крайномерно линейно пространство, а φ е линейно преобразуване на V, ще казваме, че φ *се привежда в нормална форма*, когато в пространството V има такъв базис, в който матрицата на φ е жорданова. Ако в даден базис на пространството V преобразуването φ има жорданова матрица, ще казваме, че φ има *нормална форма* в този базис.

Основен резултат на настоящата глава е следната теорема.

Теорема 1 (теорема на Жордан). *Всяко линейно преобразуване в крайномерно линейно пространство над полето* C *на комплексните числа може да се приведе в нормална форма.*

Доказателство. Нека V е комплексно линейно пространство с размерност n и φ е произволно линейно преобразуване на V. Както показахме в § 1, пространството V може да се превърне посредством φ в модул над пръстена $\mathbf{C}[\lambda]$. Според твърдение 4 този модул се разлага в директна сума на примарни циклични подмодули $V_1, V_2, \ldots, V_m$ съответно спрямо простите елементи $\lambda-\lambda_1, \lambda-\lambda_2, \ldots, \lambda-\lambda_m$. Тук следва да отбележим, че комплексните числа $\lambda_1, \lambda_2, \ldots, \lambda_m$ не са непременно различни.

Да означим с e_{i1} един от образуващите елементи на циклич-ния примарен модул V_i и да предположим, че полиномът $(\lambda-\lambda_i)^{n_i}$ поражда анулатора $\mathrm{Ann}(e_{i1})$ на елемента e_{i1} $(i=1, 2, \ldots, m)$. От твърдение 7 следва, че векторите

$$e_{i1},\ e_{i2}=(\lambda-\lambda_i)\,e_{i1},\ e_{i3}=(\lambda-\lambda_i)^2\ e_{i1},\ \ldots,\ e_{in_i}=$$
$$=(\lambda-\lambda_i)^{n_i-1}\,e_{i1}$$

образуват базис на подпространството V_i и в този базис са изпълнени равенствата

$$\begin{aligned}
\varphi(e_{i1}) &= \lambda_i e_{i1} + e_{i2},\\
\varphi(e_{i2}) &= \lambda_i e_{i2} + e_{i3},\\
&\ldots\ldots\ldots\\
\varphi(e_{i,\,n_i-1}) &= \lambda_i e_{i,\,n_i-1} + e_{in_i}\\
\varphi(e_{in_i}) &= \lambda_i e_{in_i}
\end{aligned} \tag{2}$$

при $i=1, 2, \ldots, m$. Векторите $e_{11}, e_{12}, \ldots, e_{1n}, e_{21}, e_{22}, \ldots, e_{2n_2}, \ldots, e_{m1}, e_{m2}, \ldots, e_{mn_m}$ образуват базис на пространството V. Наистина нека v е произволен вектор от V. Тъй като $V=V_1\oplus V_2\oplus \ldots \oplus V_m$, то $v=v_1+v_2+\ldots+v_m$, където $v_i\in V_i (i=1, 2, \ldots, m)$. Векторът v_i се записва като линейна комбинация на базисните вектори $e_{i1}, e_{i2}, \ldots, e_{in_i}$ на пространството V_i. Следователно векторът v е линейна комбинация на векторите e_{ij} $(i=1, 2, \ldots, m;\ j=1, 2, \ldots, n_i)$. Нека

$$\sum_{i=1}^{m}\sum_{j=1}^{n_i}\alpha_{ij}\,e_{ij}=0\ \ (\alpha_{ij}\in C) \tag{3}$$

е една линейна зависимост между векторите e_{ij}. Тъй като сумата $V=V_1\oplus V_2\oplus \ldots \oplus V_m$ е директна и $\sum_{j=1}^{n_i}\alpha_{ij}e_{ij}$ е i-тата компонента на вектора $\sum_{i=1}^{m}\sum_{j=1}^{n_i}\alpha_{ij}e_{ij}$, от равенството (3) следват равенствата

$$\sum_{j=1}^{n_i}\alpha_{ij}\,e_{ij}=0\ \ (i=1, 2, \ldots, m).$$

Но векторите $e_{i1}, e_{i2}, \ldots, e_{in_i}$ са линейно независими и затова от последните равенства получаваме $\alpha_{ij}=0$ за $j=1, 2, \ldots n_i$ и

$i=1, 2, \ldots, m$. Така доказахме, че всеки вектор v от V е линейна комбинация на векторите e_{ij} и че тези вектори са линейно независими, т. е. че векторите e_{ij} $(i=1, 2, \ldots, m;\ j=1, 2, \ldots, n_i)$ образуват базис на пространството V. От равенства (2) следва, че матрицата на преобразуването φ в базиса $e_{11}, e_{12}, \ldots, e_{1n_1}$, $e_{21}, \ldots, e_{2n_2}, e_{m1} \ldots e_{mn_m}$ е жордановата матрица (1), където

$$A_i=\begin{pmatrix} \lambda_i & 0 & 0 \ldots 0 & 0 \\ 1 & \lambda_i & 0 \ldots 0 & 0 \\ 0 & 1 & \lambda_i \ldots 0 & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 \ldots \lambda_i & 0 \\ 0 & 0 & 0 \ldots 1 & \lambda_i \end{pmatrix}$$

е жорданова клетка от ред n_i $(i=1, 2, \ldots, m)$. Затова преобразуването φ се привежда в нормална форма. Теоремата е доказана.

Следствие 1. *Всяка квадратна комлексна матрица е подобна на жорданова матрица.*

Действително всяка квадратна комплексна матрица A от ред n е матрица на определено линейно преобразуване φ на дадено комплексно n-мерно линейно пространство с фиксиран базис. Като приведем φ в нормална форма, ще получим нов базис, спрямо който матрицата B на преобразуването φ е жорданова. Известно е, че в такъв случай матриците A и B са подобни.

С последната теорема ние отговорихме утвърдително на първия от поставените в началото въпроси. По-нататък ще насочим своите усилия към създаването на ефективен метод за намиране на нормалната форма на линейното преобразуване.

Забележка. Ако P е произволно поле, то теоремата на Жордан приема следния вид: едно линейно преобразуване φ на крайномерното пространство V над P се привежда в нормална форма тогава и само тогава, когато характеристичните корени на φ се съдържат в полето P. Наистина ако φ се привежда в нормална форма, то в някой базис на V преобразуването φ ще има жорданова матрица; а на последната характеристичните корени са елементите ѝ по главния диагонал, които са от P, т. е. характеристичните корени на φ са от P. Обратното се доказва със смяна на C с P в приведеното по-горе доказателство.

§ 4. Теорема на Хамилтон—Кейли

Жордановите матрици имат по-сложен строеж от диагоналните, но и с тях могат сравнително просто да се извършат редица алгебрични операции. Ще илюстрираме това твърдение с един конкретен пример и едновременно ще получим една теорема

на Хамилтон — Кейли като следствие от теоремата на Жордан.

Нека A е произволна квадратна комплексна матрица от ред n, а $f(\lambda)=a_k\lambda^k+a_{k-1}\lambda^{k-1}+\ldots+a_1\lambda+a_0$ е произволен полином от пръстена $\mathbf{C}[\lambda]$. Тогава матрицата

$$f(A)=a_kA^k+a_{k-1}A^{k-1}+\ldots+a_1A+a_0E,$$

където $E=A^0$ е единичната матрица от ред n, се нарича стойност на полинома $f(\lambda)$ за $\lambda=A$.

Лесно се проверява, че ако

$$f(\lambda)=f_1(\lambda)+f_2(\lambda),\ g(\lambda)=f_1(\lambda)f_2(\lambda),$$

където $f_1(\lambda)\in\mathbf{C}[\lambda]$ и $f_2(\lambda)\in\mathbf{C}[\lambda]$, то

$$f(A)=f_1(A)+f_2(A),\ g(A)=f_1(A)f_2(A).$$

Ако матрицата A анулира полинома $f(\lambda)$, т. е. $f(A)=0$, то A се нарича *матричен корен* на полинома $f(\lambda)$.

Ще покажем как се пресмята стойността на произволен полином за $\lambda=J$, където J е жорданова матрица.

Лема 1. *Нека квадратните матрици A и B от ред n имат вида*

$$A=\begin{pmatrix}C & 0\\ 0 & D\end{pmatrix},\quad B=\begin{pmatrix}F & 0\\ 0 & G\end{pmatrix},$$

където $C=(c_{ij})$ и $F=(f_{ij})$ са матрици от ред p, а $D=(d_{ij})$ и $G=(g_{ij})$ са матрици от ред q и $n=p+q$.

Тогава

$$AB=\begin{pmatrix}CF & 0\\ 0 & DG\end{pmatrix}.$$

Лемата се доказва с непосредствена проверка.

Следствие 2. *Нека матрицата A има вида*

$$A=\begin{pmatrix}A_1 & & 0\\ & A_2 & \\ & \ddots & \\ 0 & & A_m\end{pmatrix},$$

където $A_1, A_2, \ldots, A_m$ са квадратни матрици, а останалите елементи на A са нули. Тогава за всяко цяло положително число k е в сила равенството

$$A^k=\begin{pmatrix}A_1^k & & 0\\ & A_2^k & \\ & \ddots & \\ 0 & & A_m^k\end{pmatrix}.$$

Доказателство. Ако $m=2$, то

$$A=\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

и твърдението се получава чрез неколкократно прилагане на предната лема.

Да допуснем, че за $m-1$ твърдението е доказано. Тъй като матрицата A има вида

$$A=\begin{pmatrix} B & 0 \\ 0 & A_m \end{pmatrix},$$

където

$$B=\begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ & \ddots & \\ 0 & & A_{m-1} \end{pmatrix},$$

то

$$A^k=\begin{pmatrix} B^k & 0 \\ 0 & A_m^k \end{pmatrix}.$$

По индуктивното предположение е в сила равенството

$$B^k=\begin{pmatrix} A_1^k & & 0 \\ & A_2^k & \\ & \ddots & \\ 0 & & A_{m-1}^k \end{pmatrix}$$

и затова A^k има посочения вид. Следствието е доказано.

Нека сега матрицата

$$J=\begin{pmatrix} J_1 & & 0 \\ & J_2 & \\ & \ddots & \\ 0 & & J_m \end{pmatrix}$$

е жорданова с жорданови клетки $J_1, J_2, \ldots, J_m$ съответно от редове $p_1, p_2, \ldots, p_m$, а $f(\lambda)$ е полином от пръстена $\mathbf{C}[\lambda]$. Като се използува следствие 2, лесно се показва, че

$$f(J)=\begin{pmatrix} f(J_1) & & 0 \\ & f(J_2) & \\ & \ddots & \\ 0 & & f(J_m) \end{pmatrix},$$

т. е. за да изчислим стойността на полинома $f(\lambda)$ за $\lambda=J$, достатъчно е да умеем да пресмятаме стойността на този полином за произволна жорданова клетка. Затова нека J_1 е жорданова клетка

от ред p, която има по диагонала си комплексното число λ_1. Тогава матрицата J_1 можем да запишем във вида $J_1=\lambda_1 E+H$, където E е единичната матрица от ред p, а

$$H=\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$

Лесно се доказва, че матриците $H^2, H^3, \ldots, H^{p-1}$ имат следния вид:

$$H^2=\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 \end{pmatrix}, \ldots, H^{p-1}=\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix},$$

т. е при всяка следваща степен единиците на H се изместват наляво, а $H^p=H^{p+1}=\ldots=0$. Нека полиномът $f(\lambda)$ е от степен n. По формулата на Тейлър имаме

$$f(\lambda)=f(\lambda_1)+\frac{f'(\lambda_1)}{1!}(\lambda-\lambda_1)+\ldots+\frac{f^{(n)}(\lambda_1)}{n!}(\lambda-\lambda_1)^n.$$

Като заместим λ с матрицата J_1, получаваме

$$f(J_1)=f(\lambda_1)E+\frac{f'(\lambda_1)}{1!}(J_1-\lambda_1 E)+\ldots+\frac{f^{(n)}(\lambda_1)}{n!}(J_1-\lambda_1 E)^n.$$

Но $J_1-\lambda_1 E=H$ и затова

$$f(J_1)=f(\lambda_1)E+\frac{f'(\lambda_1)}{1!}H+\frac{f''(\lambda_1)}{2!}H^2+\ldots+\frac{f^{(n)}(\lambda_1)}{n!}H^n.$$

Като вземем предвид вида на матриците $H, H^2, \ldots, H^{p-1}$ и това, че $H^p=H^{p+1}=\ldots=0$, ще получим

$$(1)\quad f(J_1)=\begin{pmatrix} f(\lambda_1) & 0 & 0 & \ldots & 0 \\ \frac{f'(\lambda_1)}{1!} & f(\lambda_1) & 0 & \ldots & 0 \\ \frac{f''(\lambda_1)}{2!} & \frac{f'(\lambda_1)}{1!} & f(\lambda_1) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \frac{f^{(p-1)}(\lambda_1)}{(p-1)!} & \frac{f^{(p-2)}(\lambda_1)}{(p-2)!} & \frac{f^{(p-3)}(\lambda_1)}{(p-3)!} & \ldots & f(\lambda_1) \end{pmatrix}.$$

Този резултат показва, че за да пресметнем стойността на полинома $f(\lambda)$ при λ, равно на една жорданова клетка от ред p, достатъчно е да знаем стойностите $f(\lambda_1)$, $f'(\lambda_1), \ldots, f^{(p-1)}(\lambda_1)$, където λ_1 е характеристичният корен на тази клетка.

От равенството (1) непосредствено се получава следното

Твърдение 9. *Жордановата клетка J_1 от ред p е матричен корен на полинома $f(\lambda)$ тогава и само тогава, когато характеристичният корен на J_1 е най-малко p-кратен корен на полинома $f(\lambda)$.*

Теорема 2 (теорема на Хамилтон — Кейли). *Всяка квадратна числова матрица е матричен корен на своя характеристичен полином.*

Доказателство. Нека A е произволна квадратна числова матрица, а $f(\lambda)=|A-\lambda E|$ е нейният характеристичен полином. Трябва да докажем, че $f(A)=0$. От теоремата на Жордан следва, че матрицата A е подобна на жорданова матрица J. Нека тази жорданова матрица има жорданови клетки $J_1, J_2, \ldots, J_m$ съответно от редове $n_1, n_2, \ldots, n_m$ и характеристични корени $\lambda_1, \lambda_2, \ldots, \lambda_m$. Тогава характеристичният полином на матрицата J е

$$(\lambda_1-\lambda)^{n_1}(\lambda_2-\lambda)^{n_2}\ldots(\lambda_m-\lambda)^{n_m}.$$

Тъй като подобните матрици имат един и същ характеристичен полином, то

$$f(\lambda)=(\lambda_1-\lambda)^{n_1}(\lambda_2-\lambda)^{n_2}\ldots(\lambda_m-\lambda)^{n_m}.$$

Както видяхме, стойността $f(J)$ на полинома $f(\lambda)$ за $\lambda=J$ има вида

$$f(J)=\begin{bmatrix} f(J_1) & & & 0 \\ & f(J_2) & & \\ & & \ddots & \\ 0 & & & f(J_m) \end{bmatrix}.$$

Но λ_i е най-малко n_i-кратен корен на полинома $f(\lambda)$ и затова съгласно твърдение 9 $f(J_i)=0\,(i=1, 2, \ldots, m)$. Следователно матрицата J е матричен корен на полинома $f(\lambda)$.

Тъй като A и J са подобни, то $A=T^{-1}JT$ за някоя обратима матрица T. Ако

$$f(\lambda)=a_0\lambda^n+a_1\lambda^{n-1}+\ldots+a_{n-1}\lambda+a_n,$$

то

$$\begin{aligned} f(A)&=a_0A^n+a_1A^{n-1}+\ldots+a_{n-1}A+a_nE= \\ &=a_0(T^{-1}JT)^n+a_1(T^{-1}JT)^{n-1}+\ldots+a_{n-1}(T^{-1}JT)+a_nE= \\ &=a_0T^{-1}J^nT+a_1T^{-1}J^{n-1}T+\ldots+a_{n-1}T^{-1}JT+a_nE= \\ &=T^{-1}(a_0J^n+a_1J^{n-1}+\ldots+a_{n-1}J+a_nE)\,T= \\ &=T^{-1}f(J)\,T. \end{aligned}$$

Следователно $f(A)=T^{-1}f(J)\,T$. Но $f(J)=0$ и затова $f(A)=0$. Теоремата е доказана.

Забележка. Теоремата на Хамилтон — Кейли е в сила и за квадратни матрица с елементи от произволно поле P. Наистина ако A е матрици с елементи от P, а K е полето на разлагане на характеристичния полином на A над полето P, то A е подобна на жорданова матрици J с елементи от K. Като приложим горното доказателство, което е в сила и за разглеждания случай, получаваме, че A е матричен корен на своя характеристичен полином

§ 5. Еквивалентност на λ-матрици

Всяка квадратна матрица, елементите на която са полиноми с комплексни коефициенти, ще наричаме λ-матрица, или полиномиална матрица.

Примери

1. Всяка квадратна числова матрица е λ-матрица, като нейните елементи са полиноми на λ от нулева степен или нули.

2. Характеристичната матрица $A-\lambda E$ на всяка квадратна числова матрица A е λ-матрица.

Определение 4. *Елементарни преобразувания* на λ-матрицата

$$A(\lambda)=\begin{pmatrix} a_{11}(\lambda)\, a_{12}(\lambda) & \cdots & a_{1n}(\lambda) \\ a_{21}(\lambda)\, a_{22}(\lambda) & \cdots & a_{2n}(\lambda) \\ \cdots & \cdots & \cdots \\ a_{n1}(\lambda) a_{n2}(\lambda) & \cdots & a_{nn}(\lambda) \end{pmatrix}$$

ще наричаме преобразуванията от следните четири вида:

1) *умножаване на някой от редовете на матрицата* $A(\lambda)$ *с произволно, различно от нула комплексно число;*

2) *умножаване на някой от стълбовете на матрицата* $A(\lambda)$ *с произволно, различно от нула комплексно число;*

3) *прибавяне на* j*-тия ред на матрицата* $A(\lambda)$*, умножен с произволен полином* $f(\lambda)$ *от пръстена* $\mathbf{C}[\lambda]$*, към* i*-тия й ред* $(j\neq i)$;

4) *прибавяне на* j*-тия стълб на матрицата* $A(\lambda)$*, умножен с произволен полином* $f(\lambda)$ *от пръстена* $\mathbf{C}[\lambda]$*, към* i*-тия й стълб* $(j\neq i)$.

Твърдение 10. *За всяко елементарно преобразуване на* λ*-матрица съществува обратно преобразуване, което е също елементарно.*

Доказателство. Ако елементарното преобразуване е умножаване на i-тия ред (стълб) на матрицата $A(\lambda)$ с ненулевото комплексно число α, то неговото обратно преобразуване е умножаване на i-тия ред (стълб) с числото $\alpha^{-1}\neq 0$ и затова то е също елементарно преобразуване.

Ако елементарното преобразуване на матрицата $A(\lambda)$ е прибавяне към i-тия ред (стълб) на нейния j-ти ред (стълб), умно-

жен на полинома $f(\lambda)$, където $i \neq j$, то обратното преобразуване е прибавяне към i-тия ред (стълб) на нейния j-ти ред (стълб), умножен на полинома $-f(\lambda)$, т. е. обратното преобразуване е също елементарно.

Определение 5. Ще казваме, че λ-матриците $A(\lambda)$ и $B(\lambda)$ са *еквивалентни* и ще записваме $A(\lambda) \sim B(\lambda)$, ако от матрицата $A(\lambda)$ може да се премине към матрицата $B(\lambda)$ чрез краен брой елементарни преобразувания.

Задача. Докажете, че за така въведеното отношение „еквивалентни“ в множеството от всички λ-матрици от ред n са изпълнени следните три свойства:

1) *рефлексивност* — $A(\lambda) \sim A(\lambda)$ за всяка λ-матрица $A(\lambda)$;

2) *симетричност* — ако $A(\lambda) \sim B(\lambda)$, то $B(\lambda) \sim A(\lambda)$.

3) *транзитивност* — ако $A(\lambda) \sim B(\lambda)$ и $B(\lambda) \sim C(\lambda)$, то $A(\lambda) \sim C(\lambda)$.

Упътване. Използувайте предишното твърдение.

Твърдение 11. *Ако матрицата $B(\lambda)$ се получава от матрицата $A(\lambda)$ само с разместване на редовете и стълбовете, то $A(\lambda) \sim B(\lambda)$.*

Доказателство. Нека например матрицата $B(\lambda)$ е получена от матрицата $A(\lambda)$ с разменяне на местата на i-тия и j-тия ред ($i<j$). Тогава, както показва схемата

$$A(\lambda)=\begin{pmatrix} i \\ j \end{pmatrix} \to \begin{pmatrix} i+j \\ j \end{pmatrix} \to \begin{pmatrix} i+j \\ -i \end{pmatrix} \to \begin{pmatrix} j \\ -i \end{pmatrix} \to \begin{pmatrix} j \\ i \end{pmatrix} = B(\lambda),$$

от $A(\lambda)$ към $B(\lambda)$ може да се премине чрез следните елементарни преобразувания: а) към i-тия ред е прибавен j-тият; б) от j-тия ред е изваден новият i-ти ред; в) към новия i-ти ред е прибавен новият j-ти ред; г) новият j-ти ред е умножен с -1. Аналогично се доказва твърдението и за стълбовете.

Тъй като въведеното за λ-матриците отношение „еквивалентни“ има свойствата рефлексивност, симетричност и транзитивност, то *множеството от всички λ-матрици от ред n се разпада на непресичащи се класове от еквивалентни матрици*. Във всеки един от тези класове ще намерим по една матрица, която има достатъчно прост специален вид.

Определение 6. Една λ-матрица се нарича *канонична*, ако притежава следните три свойства:

1) *тази матрица е диагонална, т. е. има вида*

$$\begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix};$$

2) *полиномът $e_i(\lambda)$ дели полинома $e_{i+1}(\lambda)$; $i=1, 2, \ldots n-1$;*

3) *ако полиномът* $e_i(\lambda)$ *е различен от нула, то неговият старши коефициент е равен на единица, т. е.* $e_i(\lambda)$ $(i=1, 2, \ldots, n)$ *е нормиран полином.*

Очевидно ако в каноничния вид на $A(\lambda)$ между полиномите $e_i(\lambda)$ има ревки на нула, то според свойство 2) те заемат последните места по главния диагонал; ако сред полиномите $e_i(\lambda)$ има полиноми от нулева степен, по свойство 3) те са равни на единицата и по свойство 2) заемат първите места по главния диагонал.

Пример. Единичната матрица и нулевата матрица са канонични λ-матрици.

Оказва се, че във всеки клас от еквивалентни λ-матрици се съдържа канонична λ-матрица, т. е. вярна е следната теорема.

Теорема 2 (теорема за съществуване на каноничен вид на λ-матриците). *Всяка* λ*-матрица е еквивалентна на някоя канонична матрица.*

Доказателство. Теоремата ще докажем с индукция спрямо реда n на разглежданите λ-матрици.

Нека $n=1$. Всяка λ-матрица $A(\lambda)$ от първия ред има вида

$$A(\lambda)=(a(\lambda)).$$

Ако $a(\lambda)=0$, то $A(\lambda)$ е канонична. Ако $a(\lambda)\neq 0$, разделяме полинома $a(\lambda)$ с коефициента пред най-високата му степен и получаваме канонична матрица. Матрицата $A(\lambda)$ е еквивалентна на получената канонична λ-матрица, защото извършеното преобразуване е елементарно.

Да допуснем, че теоремата е вече доказана за λ-матрици, на които редът е най-много $n-1$ и нека $A(\lambda)$ е произволна λ-матрица от ред n. Ако тя е нулева, тя е канонична и няма какво да доказваме. Затова ще считаме, че между елементите на $A(\lambda)$ има ненулеви полиноми. По-нататък доказателството ще проведем на няколко етапа.

а) Като разместим, ако е необходимо, редовете и стълбовете на матрицата $A(\lambda)$, може да преместим един от ненулевите елементи в горния ляв ъгъл. Съгласно твърдение 11 новополучената матрица е еквивалентна на матрицата $A(\lambda)$. Следователно между λ-матриците, които са еквивалентни на матрицата $A(\lambda)$, има такива, в горния ляв ъгъл на които стои ненулев полином. Да разгледаме всички такива матрици. Полиномите, които стоят в горните леви ъгли на тези матрици, имат неотрицателни степени. В множеството от тези степени може да се намери най-малко число m. Избираме една от матриците, които са еквивалентни на матрицата $A(\lambda)$ и имат в горния си ляв ъгъл полином от степен m. Като разделим първия ред на тази матрица със старшия коефициент на полинома от горния й ляв ъгъл, получаваме λ-матрицата

$$B(\lambda)=\begin{pmatrix} e_1(\lambda) & b_{12}(\lambda) & \cdots & b_{1n}(\lambda) \\ b_{21}(\lambda) & b_{22}(\lambda) & \cdots & b_{2n}(\lambda) \\ \cdot & \cdot & \cdots & \cdot \\ b_{n1}(\lambda) & b_{n2}(\lambda) & \cdots & b_{nn}(\lambda) \end{pmatrix},$$

където $e_1(\lambda)$ е ненулев нормиран полином от степен m и от матрицата $B(\lambda)$ с никакви елементарни преобразувания не може да се получи матрица, в горния ляв ъгъл на която стои ненулев полином от степен, по-ниска от m.

б) Ще докажем, че всички елементи от първия ред и първия стълб на матрицата $B(\lambda)$ се делят на полинома $e_1(\lambda)$. Нека например за $2 \leqq j \leqq n$ имаме

$$b_{1j}(\lambda)=q(\lambda)\,e_1(\lambda)+r(\lambda),\ \deg r(\lambda)<\deg e_1(\lambda).$$

Ако полиномът $r(\lambda)$ не е нулев, като извадим от j-тия стълб на матрицата $B(\lambda)$ нейния първи стълб, умножен с $q(\lambda)$, и след това разменим местата на първия и j-тия стълб на получената матрица, ще имаме матрица, еквивалентна на матрицата $B(\lambda)$, в левия горен ъгъл на която стои ненулевият полином $r(\lambda)$, чиято степен е по-ниска от m. Това противоречи на посоченото в а) свойство на матрицата $B(\lambda)$. Следователно $r(\lambda)=0$ и затова $e_1(\lambda)$ дели полинома $b_{1j}(\lambda)$. Сега, като извадим от j-тия стълб на матрицата $B(\lambda)$ нейния първи стълб, умножен с $q(\lambda)$, ние ще заменим елемента $b_{1j}(\lambda)$ с нула. По същия начин заменяме с нули елементите $b_{1j}(\lambda)$ за $j=2, 3, \ldots, n$. Аналогично постъпваме и с елементите b_{i1} $(i=2, 3, \ldots, n)$. Така достигаме до матрицата

$$F(\lambda)=\begin{pmatrix} e_1(\lambda) & 0 & \cdots & 0 \\ 0 & f_{22}(\lambda) & \cdots & f_{2n}(\lambda) \\ \cdots & \cdots & \cdots & \cdots \\ 0 & f_{n2}(\lambda) & \cdots & f_{nn}(\lambda) \end{pmatrix},$$

която е еквивалентна на $A(\lambda)$ и в горния й ляв ъгъл стои полиномът $e_1(\lambda)$, а останалите елементи от първия ред и първия стълб са нули.

По индуктивното предположение матрицата от $(n-1)$-ви ред, която стои в долния десен ъгъл на матрицата $F(\lambda)$, с елементарни преобразувания се привежда в каноничен вид, т. е.

$$\begin{pmatrix} f_{22}(\lambda) & \cdots & f_{2n}(\lambda) \\ \cdots & \cdots & \cdots \\ f_{n2}(\lambda) & \cdots & f_{nn}(\lambda) \end{pmatrix} \sim \begin{pmatrix} e_2(\lambda) & & 0 \\ & \ddots & \\ 0 & & e_n(\lambda) \end{pmatrix}.$$

Като извършим същите преобразувания над съответните редове и стълбове на матрицата $F(\lambda)$ (при това първия ред и първия стълб на тази матрица очевидно не се променят), получаваме, че

$$A(\lambda)\sim D(\lambda)=\begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix}.$$

в) Остава да покажем, че матрицата $D(\lambda)$ е канонична. За целта достатъчно е да покажем, че полиномът $e_1(\lambda)$ дели полинома $e_2(\lambda)$. Нека

$$e_2(\lambda)=q(\lambda)e_1(\lambda)+r(\lambda),$$

където степента на полинома $r(\lambda)$ е по-ниска от степента m на полинома $e_1(\lambda)$. Да допуснем, че $r(\lambda)\neq 0$. Прибавяме втория стълб на матрицата $D(\lambda)$ към първия, след това изваждаме от втория ред на получената матрица нейния първия ред, умножен с полинома $q(\lambda)$, и сменяме местата на първия и втория ред на получената матрица. В резултат на тази редица от елементарни преобразувания матрицата $D(\lambda)$, а следователно и матрицата $B(\lambda)$ ще се окажат еквивалентни на матрица, в горния ляв ъгъл на която стои ненулевият полином $r(\lambda)$. Това обаче противоречи на посоченото в точка а) свойство на матрицата $B(\lambda)$. Следователно полиномът $r(\lambda)$ е нулев и $e_1(\lambda)$ дели $e_2(\lambda)$, Теоремата е доказана

По този начин показахме, че всеки клас от еквивалентни λ-матрици съдържа поне една канонична λ-матрица. Сега най-близката ни цел е да докажем, че всеки такъв клас съдържа само една-единствена канонична матрица.

Нека $A(\lambda)$ е произволна λ-матрица от ред n и разглеждаме множеството от всички минори на матрицата $A(\lambda)$ от ред k, където $1\leqq k\leqq n$. Да означим с $d_k(\lambda)$ нормирания (ако $d_k(\lambda)\neq 0$) най-голям общ делител на всички минори от k-ти ред. По този начин на λ-матрицата $A(\lambda)$ се съпоставят полиномите

$$d_1(\lambda),\ d_2(\lambda),\ \ldots,\ d_n(\lambda),$$

които еднозначно се определят от самата матрица $A(\lambda)$.

Задача. Докажете, че за матрицата $A(\lambda)$ е изпълнено равенството

$$d_1(\lambda)=0$$

тогава и само тогава, когато $A(\lambda)$ е нулевата матрица.

Очевидно е, че $d_n(\lambda)$ е равен на детерминантата $|A(\lambda)|$ на матрицата $A(\lambda)$, разделена (ако $|A(\lambda)|\neq 0$) с коефициента пред най-високата степен на λ.

Задача. Докажете, че ако за λ-матрицата $A(\lambda)$ е изпълнено равенството $d_n(\lambda)=1$, то $d_1(\lambda)=d_2(\lambda)=\ldots=d_n(\lambda)=1$.

Упътване. Използувайте теоремата на Лаплас за детерминантите.

Ще отбележим още, че ако матрицата $A(\lambda)$ има ранг r, то $d_{r+1}(\lambda)=\ldots=d_n(\lambda)=0$, а полиномите $d_1(\lambda),\ldots,d_r(\lambda)$ са различни от нула.

Твърдение 12. *Ако матрицата*

$$D(\lambda)=\begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix}$$

е каноничка, то за съответствуващите ѝ полиноми $d_1(\lambda), \ldots, d_n(\lambda)$ *са изпълнени равенствата*

$$d_k(\lambda)=e_1(\lambda)\,e_2(\lambda)\ldots e_k(\lambda),\ k=1,\ 2,\ \ldots,\ n.$$

Доказателство. Нека k е естествено число и $1\leqq k\leqq n$. Минорът на матрицата $D(\lambda)$, който стои в редовете с номера $i_1, i_2, \ldots, i_k$ $(i_1<i_2<\ldots<i_k)$ и в стълбовете със същите номера, е равен на произведението $e_{i_1}(\lambda)\,e_{i_2}(\lambda)\ldots e_{i_k}(\lambda)$. Този минор се дели на минора от ред k, който е равен на произведението $e_1(\lambda)\,e_2(\lambda)\ldots e_k(\lambda)$ и стои в горния ляв ъгъл на матрицата $D(\lambda)$. Наистина $1\leqq i_1$ и затова $e_1(\lambda)$ дели $e_{i_1}(\lambda)$; $2\leqq i_2$ и затова $e_2(\lambda)$ дели $e_{i_2}(\lambda)$, $\ldots$, $k\leqq i_k$ и затова $e_k(\lambda)$ дели полинома $e_{i_k}(\lambda)$, т. е. полиномът $e_1(\lambda)\,e_2(\lambda)\ldots e_k(\lambda)$ дели произведението $e_{i_1}(\lambda)\,e_{i_2}(\lambda)\ldots e_{i_k}(\lambda)$. Всеки минор от ред k на матрицата $D(\lambda)$, през който минава i-тият ред, но не минава i-тият стълб, съдържа един ред от нули и затова е равен на нула. Следователно полиномът $e_1(\lambda)\,e_2(\lambda)\ldots e_k(\lambda)$ дели всички минори от ред k, има коефициент единица пред най-високата степен на λ (ако е различен от нула) и е равен на един от тези минори. С други думи, този полином е най-голям общ делител на минорите от ред k на матрицата $D(\lambda)$ и понеже е нормиран, то

$$e_1(\lambda)\,e_2(\lambda)\ldots e_k(\lambda)=d_k(\lambda).$$

Твърдението е доказано.

Лема 2. *Най-големият общ делител* $d_k(\lambda)$ *на всички минори от ред* k *на* λ*-матрицата* $A(\lambda)$ $(k=1,\ 2,\ \ldots,\ n)$ *не се изменя, когато в матрицата* $A(\lambda)$ *се извършват елементарни преобразувания.*

Доказателство. Нека в матрицата $A(\lambda)$ е извършено елементарно преобразуване от вида 1). Например ако i-тият ѝ ред е умножен на ненулевото комплексно число α, то минорите от ред k на получената матрица, през които минава i-тият ред, са равни на съответните минори на матрицата $A(\lambda)$, умножени на числото α, а минорите, през които не минава този ред, са равни на съответните минори на матрицата $A(\lambda)$. Но при намирането на НОД на няколко полинома всеки от тях може да се умножава с произволни ненулеви числа, без това да влияе на крайния резултат. Аналогично се разглежда случаят, когато в $A(\lambda)$ е извършено преобразуване от вида 2).

Нека сега в матрицата $A(\lambda)$ е извършено елементарно преобразуване от вида 3) или 4). За конкретност да разгледаме например случая, когато към i-тия ред на матрицата $A(\lambda)$ е прибавен нейният j-ти ред $(j\neq i)$, умножен с полинома $f(\lambda)$. Да озна-

чим с $\bar{A}(\lambda)$ получената след това преобразувание матрица, а с $\bar{d}_k(\lambda)$ — нормирания НОД на нейните минори от ред k. Трябва да докажем, че $d_k(\lambda)=\bar{d}_k(\lambda)$.

Ясно е, че минорите на $\bar{A}(\lambda)$, през които не минава i-тият ред, са равни на съответните минори на $A(\lambda)$. Също така минорите на $\bar{A}(\lambda)$, през които минават както i-тият ред, така и j-тият ред, са равни на съответните минори на $A(\lambda)$, понеже детерминантата не се променя, ако към един неин ред се прибави кратен на друг ред. Затова нека M е произволен минор на матрицата $\bar{A}(\lambda)$ от ред k, през който минава i-тият ред, но не минава j-тият ред. Да означим с M съответствуващия на $\bar{M}$ минор на матрицата $A(\lambda)$, а с M' — детерминантата, получена от M, като в M елементите от i-тия ред на $A(\lambda)$ се заменят със съответните елементи на j-тия ред на $A(\lambda)$. Ясно е, че M' се различава от минор на $A(\lambda)$ евентуално само по разположението на един от редовете, т. е. M' с точност до знак е минор от ред k на матрицата $A(\lambda)$. Тъй като

$$\bar{M}=M+f(\lambda)M'$$

и минорите M и M' се делят на полинома $d_k(\lambda)$, то минорът $\bar{M}$ се дели на $d_k(\lambda)$.

От казаното следва, че полиномът $d_k(\lambda)$ дели всички минори от ред k на матрицата $\bar{A}(\lambda)$, т. е. $d_k(\lambda)$ дели полинома $\bar{d}_k(\lambda)$. Тъй като за разглежданото елементарно преобразувание съществува обратно елементарно преобразувание от същия вид, то и $\bar{d}_k(\lambda)$ дели $d_k(\lambda)$. Като вземем под внимание, че $d_k(\lambda)$ и $\bar{d}_k(\lambda)$ са нормирани, заключаваме, че $d_k(\lambda)=\bar{d}_k(\lambda)$, което трябваше да докажем.

Следствие 3. *Нека на λ-матрицата $A(\lambda)$ са съпоставени полиномите*

$$d_1(\lambda),\ d_2(\lambda),\ \ldots,\ d_n(\lambda),$$

а на λ-матрицата $B(\lambda)$ — полиномите

$$\tilde{d}_1(\lambda),\ \tilde{d}_2(\lambda),\ \ldots,\ \tilde{d}_n(\lambda).$$

Ако матриците $A(\lambda)$ и $B(\lambda)$ са еквивалентни, то

$$d_k(\lambda)=\tilde{d}_k(\lambda),\ k=1,\ 2,\ \ldots,\ n,$$

т. е. на еквивалентните матрици съответствува една и съща система от полиноми $d_1(\lambda),\ d_2(\lambda),\ \ldots,\ d_n(\lambda)$.

Наистина ако $A(\lambda)\sim B(\lambda)$, то от $A(\lambda)$ към $B(\lambda)$ може да се премине с краен брой елементарни преобразувания. Но според лема 2 при извършването на всяко елементарно преобразувание системата полиноми $d_1(\lambda),\ \ldots,\ d_n(\lambda)$ не се изменя и затова $d_k(\lambda)=\tilde{d}_k(\lambda)$ за всяко $k=1,\ 2,\ \ldots,n$.

Теорема 3 (теорема за единственост на каноничния вид). ***Всяка λ-матрица е еквивалентна само на една каноничка матрица.***

Доказателство. Нека $A(\lambda)$ е произволна λ-матрица от ред n. По теорема 2 $A(\lambda)$ е еквивалентна на някоя канонична λ-матрица

$$D(\lambda)=\begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix}$$

Нека на λ-матрицата $A(\lambda)$ са съпоставени полиномите $d_1(\lambda)$, $d_2(\lambda)$, ..., $d_n(\lambda)$. Тъй като $A(\lambda)\sim D(\lambda)$, по следствие 3 на матрицата $D(\lambda)$ се съпоставят същите полиноми. Но тогава съгласно твърдение 12 ще бъдат изпълнени равенствата

$$d_k(\lambda)=e_1(\lambda)\,e_2(\lambda)\ldots e_k(\lambda),\ k=1,\ 2,\ \ldots,\ n.$$

Ако рангът на матрицата $A(\lambda)$ е равен на r, то $d_r(\lambda)\neq 0$, $d_{r+1}(\lambda)=0$ и от равенството $d_{r+1}(\lambda)=d_r(\lambda)\,e_{r+1}(\lambda)$ ще следва, че $e_{r+1}(\lambda)=0$. Като вземем предвид свойствата на каноничната матрица, заключаваме, че ако рангът r на матрицата $A(\lambda)$ е по-малък от n, то

$$e_{r+1}(\lambda)=e_{r+2}(\lambda)=\ldots=e_n(\lambda)=0.$$

От друга страна, при $2\leqq k\leqq r$ имаме

$$d_k(\lambda)=d_{k-1}(\lambda)\,e_k(\lambda),\ d_{k-1}(\lambda)\neq 0$$

и затова

$$e_k(\lambda)=\frac{d_k(\lambda)}{d_{k-1}(\lambda)}\ (2\leqq k\leqq r).$$

Следователно ако r е рангът на матрицата $A(\lambda)$, то

$$(1)\qquad e_1(\lambda)=d_1(\lambda),\ e_k(\lambda)=\frac{d_k(\lambda)}{d_{k-1}(\lambda)}\ (k=2,\ 3,\ \ldots,\ r),$$

а останалите полиноми (при $r<n$) $d_{r+1}(\lambda)$, ..., $d_n(\lambda)$ и $e_{r+1}(\lambda)$, ..., $e_n(\lambda)$ са равни на нула. Тъй като полиномите $e_1(\lambda)$, $e_2(\lambda)$, ..., $e_n(\lambda)$ се изразяват чрез полиномите $d_1(\lambda)$, ..., $d_n(\lambda)$ по посочения начин, а последните полиноми са едни и същи за всички матрици, еквивалентни на матрицата $A(\lambda)$, то каноничният вид $D(\lambda)$ на матрицата $A(\lambda)$ еднозначно се определя от самата матрица $A(\lambda)$. Теоремата е доказана.

Определение 7. Ако λ-матрицата $A(\lambda)$ е еквивалентна на каноничната матрица

$$D(\lambda)=\begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix},$$

то полиномите $e_1(\lambda), e_2(\lambda), \ldots, e_n(\lambda)$ се наричат *инвариантни множители* на матрицата $A(\lambda)$.

От самото определение следва, че инвариантни множители на една канонична матрица са елементите от главния й диагонал.

Получените по-горе резултати показват, че намирането на каноничния вид $D(\lambda)$ на една λ-матрица $A(\lambda)$ е еквивалентно на намирането на нейните инвариантни множители и затова имаме два практически начина за намиране на $D(\lambda)$:

1) матрицата $A(\lambda)$ с елементарни преобразувания се привежда до канонична матрица $D(\lambda)$;

2) за матрицата $A(\lambda)$ пресмятаме полиномите $d_1(\lambda), d_2(\lambda), \ldots, d_n(\lambda)$, изчисляваме инвариантните множители $e_1(\lambda), \ldots, e_n(\lambda)$ на $A(\lambda)$ по формулите (1) и записваме каноничния вид $D(\lambda)$ на $A(\lambda)$.

Пример. Да се приведе в каноничен вид матрицата

$$A(\lambda)=\begin{pmatrix}\lambda^2-1 & \lambda-1\\ \lambda^3-1 & 2\lambda-2\end{pmatrix}.$$

С елементарни преобразувания последователно получаваме

$$A(\lambda)\sim\begin{pmatrix}\lambda^2-1 & \lambda-1\\ \frac{1}{2}\lambda^3-\frac{1}{2} & \lambda-1\end{pmatrix}\sim\begin{pmatrix}-\frac{1}{2}\lambda^3+\lambda^2-\frac{1}{2} & 0\\ \frac{1}{2}\lambda^3-\frac{1}{2} & \lambda-1\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}-\frac{1}{2}\lambda^3+\lambda^2-\frac{1}{2} & 0\\ 0 & \lambda-1\end{pmatrix}\sim\begin{pmatrix}\lambda^3-2\lambda^2+1 & 0\\ 0 & \lambda-1\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}\lambda-1 & 0\\ 0 & \lambda^3-2\lambda^2+1\end{pmatrix}.$$

От друга страна, като пресметнем НОД на елементите на матрицата $A(\lambda)$, получаваме

$$d_1(\lambda)=e_1(\lambda)=\lambda-1.$$

Освен това $|A(\lambda)|=-\lambda^4+3\lambda^3-2\lambda^2-\lambda+1$, така че

$$d_2(\lambda)=\lambda^4-3\lambda^3+2\lambda^2+\lambda-1.$$

Тогава

$$e_2(\lambda)=\frac{d_2(\lambda)}{d_1(\lambda)}=\lambda^3-2\lambda^2+1.$$

Следователно

$$A(\lambda)\sim\begin{pmatrix}\lambda-1 & 0\\ 0 & \lambda^3-2\lambda^2+1\end{pmatrix}.$$

§ 6. Унимодулярни λ-матрици

За да получим един нов критерий за еквивалентност на λ-матрици, в настоящия параграф ще разгледаме λ-матрици от специален тип.

Определение 8. λ-матрицата $U(\lambda)$ се нарича *унимодулярна*, ако всичките ѝ инвариантни множители са равни на единица, т. е. ако каноничната матрица на $U(\lambda)$ е единичната матрица E.

Твърдение 13. *λ-матрицата $U(\lambda)$ е унимодулярна тогава и само тогава, когато детерминантата ѝ $|U(\lambda)|$ е равна на комплексно число, различно от нула.*

Доказателство. Нека $U(\lambda)$ е унимодулярна. Тогава $U(\lambda) \sim E$ и затова на $U(\lambda)$ и E съответствува един и същ полином $d_n(\lambda)$. Но за единичната матрица $d_n(\lambda) = 1$. Следователно детерминантата $|U(\lambda)|$, която се различава от $d_n(\lambda)$ само с различен от нула числов множител, е различно от нула комплексно число.

Обратно, нека $|U(\lambda)|$ е различно от нула комплексно число. Тогава за матрицата $U(\lambda)$ ще имаме $d_n(\lambda) = 1$. Тъй като инвариантните множители $e_1(\lambda), \ldots, e_n(\lambda)$ на $U(\lambda)$ се изразяват с равенствата

$$d_1(\lambda) = e_1(\lambda),\ e_k(\lambda) = \frac{d_k(\lambda)}{d_{k-1}(\lambda)},\ k = 2, 3, \ldots, n;$$

от $d_n(\lambda) = 1$ следва, че $e_k(\lambda) = 1$ $(k = 1, 2, \ldots, n)$. Следователно $U(\lambda)$ е унимодулярна матрица.

Следствие 4. *Произведение на унимодулярни матрици е унимодулярна матрица.*

Наистина ако $U(\lambda) = U_1(\lambda) U_2(\lambda) \ldots U_n(\lambda)$, където $U_i(\lambda)$ са унимодулярни, то детерминантата $|U(\lambda)|$ на $U(\lambda)$ е равна на произведението $|U_1(\lambda)| . |U_2(\lambda)| \ldots |U_n(\lambda)|$ и затова тя е различно от нула комплексно число.

Следствие 5. *Всяка неособена комплексна матрица е унимодулярна λ-матрица.*

Твърдение 14. *Една λ-матрица е унимодулярна тогава и само тогава, когато притежава обратна матрица, която е също λ-матрица.*

Доказателство. Ако λ-матрицата $U(\lambda)$ притежава обратна матрица $F(\lambda)$, която е също λ-матрица, от равенството $U(\lambda) F(\lambda) = E$ следва равенството $|U(\lambda)| . |F(\lambda)| = 1$, което е възможно само тогава, когато полиномите $|U(\lambda)|$ и $|F(\lambda)|$ са различни от нула комплексни числа, т. е. $U(\lambda)$ е унимодулярна λ-матрица.

Ако $U(\lambda)$ е унимодулярна матрица, то детерминантата ѝ $|U(\lambda)|$ е ненулево комплексно число. При намиране на обратната матрица на $U(\lambda)$ се налага да делим адюнгираните количества на $U(\lambda)$, които са полиноми на λ, на ненулевото комплексно число $|U(\lambda)|$ и затова елементите на обратната матрица на $U(\lambda)$ са полиноми на λ, т. е. тя също е λ-матрица.

Следствие 6. *Ако една λ-матрица е обратна на унимодулярна матрица, то и тя е унимодулярна.*

Определение 9. *Матрици от вида*

$$E_{ii}(\alpha)=\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & 0 & \\ & & & 1 & & & \\ & & & & \alpha & & \\ & & & & & 1 & \\ & 0 & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix}, \quad 0 \neq \alpha \in C,$$

и

$$E_{ij}(f(\lambda))=\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix}, \quad f(\lambda) \in C[\lambda],\ i \neq j,$$

които се различават от единичната матрица E само по това, че в i-тия ред и i-тия стълб на $E_{ii}(\alpha)$ стои ненулевото комплексно число α, а в i-тия ред и j-тия стълб на $E_{ij}(f(\lambda))$ стои полиномът $f(\lambda)$, се наричат *елементарни λ-матрици.*

Очевидно е, че всяка елементарна λ-матрица е унимодулярна, тъй като $|E_{ii}(\alpha)|=\alpha$ $(\alpha \neq 0)$ и $|E_{ij}(f(\lambda))|=1$.

Лема 3. *Всяко елементарно преобразуване на λ-матрицата $A(\lambda)$ е равносилно на умножаване на тази матрица отляво или отдясно с някоя елементарна матрица. По-точно:*

1) *умножаването на матрицата $A(\lambda)$ отляво с матрицата $E_{ii}(\alpha)$ е равносилно на умножаване на i-тия ред на $A(\lambda)$ с числото α;*

2) *умножаването на матрицата $A(\lambda)$ отдясно с матрицата $E_{ii}(\alpha)$ е равносилно на умножаване на i-тия стълб на $A(\lambda)$ с числото α;*

3) *умножаването на матрицата $A(\lambda)$ отляво с матрицата $E_{ij}(f(\lambda))$ е равносилно на прибавяне на нейния j-ти ред, множен с $f(\lambda)$, към i-тия й ред;*

4. *умножаването на матрицата $A(\lambda)$ отдясно с матрицата $E_{ij}(f(\lambda))$ е равносилно на прибавяне на нейния i-ти стълб, умножен с $f(\lambda)$, към j-тия й стълб.*

Освен това обратните преобразувания на преобразуванията 1)—4) *се осъществяват съответно с матрици от вида $E_{ii}(\alpha^{-1})$ и $E_{ij}(-f(\lambda))$.*

Лемата се доказва чрез непосредствена проверка.

Понятието унимодулярна λ-матрица се използува в следния критерий за еквивалентност на λ-матриците.

Теорема 4. *Две λ-матрици $A(\lambda)$ и $B(\lambda)$ от ред n са еквивалентни тогава и само тогава, когато съществуват такива унимодулярни λ-матрици $U(\lambda)$ и $V(\lambda)$ от същия ред n, че*

$$B(\lambda)=U(\lambda)\,A(\lambda)\,V(\lambda). \tag{1}$$

Доказателство. Нека $A(\lambda)\sim B(\lambda)$, т. е. $B(\lambda)$ може да се получи от матрицата $A(\lambda)$ посредством краен брой елементарни преобразувания. Но съгласно лема 3 всяко от тези преобразувания можем да заменим с умножаване отляво или отдясно с елементарна матрица. След съответната замяна получаваме

$$B(\lambda)=U_1(\lambda)\,U_2(\lambda)\,\ldots\,U_k(\lambda)\,A(\lambda)\,V_1(\lambda)\,\ldots\,V_l(\lambda),$$

където матриците $U_1(\lambda),\ldots,U_k(\lambda)$ и $V_1(\lambda),\ldots,V_l(\lambda)$ са елементарни и следователно те са унимодулярни λ-матрици. Тогава според следствие 4 унимодулярни са и матриците

$$U(\lambda)=U_1(\lambda)\,U_2(\lambda)\,\ldots\,U_k(\lambda),\quad V(\lambda)=V_1(\lambda)\,V_2(\lambda)\,\ldots\,V_l(\lambda).$$

Да отбележим, че ако например $k=0$, т. е. ако сме извършили елементарни преобразувания само над стълбовете, просто полагаме $U(\lambda)=E$. Така получаваме равенство (1), където $U(\lambda)$ и $V(\lambda)$ са унимодулярни матрици.

Тази част от доказателството позволява да се формулира следното твърдение, което ще бъде нужно за втората част от доказателството на теоремата.

Твърдение 15. *Една λ-матрица е унимодулярна тогава и само тогава, когато може да се представи като произведение на елементарни λ-матрици.*

Доказателство. По-горе вече използувахме, че произведението на елементарни матрици е унимодулярна матрица. Обратно, ако е дадена произволна унимодулярна матрица $W(\lambda)$, тя е еквивалентна на единичната матрица E. Ако в горното доказателство вместо $A(\lambda)$ и $B(\lambda)$ вземем съответно E и $W(\lambda)$, получаваме равенството

$$W(\lambda)=U_1(\lambda)\,\ldots\,U_k(\lambda)\,EV_1(\lambda)\,\ldots\,V_l(\lambda),$$

т. е. матрицата $W(\lambda)$ е произведение на елементарни матрици.

Сега лесно може да се проведе и втората част от доказателството на теорема 4. Нека за λ-матриците $A(\lambda)$ и $B(\lambda)$ е изпълнено равенството (1), където $U(\lambda)$ и $V(\lambda)$ са унимодулярни матрици. Съгласно твърдение 15 имаме

$$U(\lambda)=U_1(\lambda)\,\ldots\,U_k(\lambda),\quad V(\lambda)=V_1(\lambda)\,\ldots\,V_l(\lambda),$$

където $U_1(\lambda),\ldots,U_k(\lambda)$, $V_1(\lambda),\ldots,V_l(\lambda)$ са елементарни λ-матрици. Тогава

$$B(\lambda)=U_1(\lambda)\,\ldots\,U_k(\lambda)\,A(\lambda)\,V_1(\lambda)\,\ldots\,V_l(\lambda).$$

Като заменим всяко умножение на елементарна матрица със съответното елементарно преобразуване (лема 3), получаваме $A(\lambda) \sim B(\lambda)$. Теоремата е доказана.

От разглежданията в последните два параграфа се получават следните три критерия за еквивалентност на λ-матриците:

Критерий 1. *Две λ-матрици са еквивалентни тогава и само тогава, когато се привеждат в един и същ каноничен вид.*

Критерий 2. *Две λ-матрици са еквивалентни тогава и само тогава, когато имат едни и същи инвариантни множители.*

Критерий 3. *Две λ-матрици $A(\lambda)$ и $B(\lambda)$ от ред n са еквивалентни тогава и само тогава, когато съществуват такива унимодулярни λ-матрици $U(\lambda)$ и $V(\lambda)$ от същия ред n, че да е изпълнено равенството* (1).

Забележка. Определенията и резултатите, които изложихме в последните два параграфа, остават същите, ако разгледаме λ-матрици, елементите на които са полиноми с коефициенти от произволно поле P. За да се установи това, достатъчно е навсякъде да се смени полето C с полето P и вместо за числа и числови полиноми да се говори за елементи на полето P и за полиноми над P. При тази смяна твърденията и доказателствата остават същите.

§ 7. Основна теорема за подобие на числови матрици

В този параграф ще дадем метод за отговор на въпроса, подобни ли са две квадратни матрици A и B, т. е. ще отговорим утвърдително на втория и частично на третия от поставените в началото въпроси.

Определение 10. Матричен λ-полином от ред n над полето C се нарича *полином на* λ, коефициентите на който са квадратни комплексни матрици от един и същ ред n.

Общият вид на произволен матричен λ-полином от ред n е

$$A_k\lambda^k + A_{k-1}\lambda^{k-1} + \ldots + A_1\lambda + A_0,$$

където $A_i \in M(n, C)$ за $i = 0, 1, 2, \ldots, k$. Ако $A_k \neq 0$, то k се нарича *степен* на този полином. *Ще се условим под $A_i\lambda^i$ да разбираме произведението на матрицата A_i с λ^i в обикновения смисъл, т. е. елементите на A_i се умножават на λ^i.* Тогава всеки матричен λ-полином от ред n може да се разглежда или като полином на λ с матрични коефициенти, или като λ-матрица от ред n, получена след извършване на съответните умножения и събирания в записването на самия полином. Например

$$\begin{pmatrix} 1 & 5 \\ 0 & 0 \end{pmatrix}\lambda^3 + \begin{pmatrix} 2 & 0 \\ 3 & -1 \end{pmatrix}\lambda^2 + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\lambda + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda^3 + 2\lambda^2 & 5\lambda^3 \\ 3\lambda^2 + 1 & -\lambda^2 \end{pmatrix}.$$

Обратно, всяка λ-матрица от ред n може да се запише като матричен λ-полином от ред n.

Ще казваме, че λ-матрицата *е от степен* k, ако съответният матричен λ-полином е от степен k. Ясно е, че степента на една λ-матрица е равна на максималната степен на нейните елементи, разглеждани като полиноми на λ.

Да означим с $M(n, \mathbf{C}[\lambda])$ множеството на всички λ-матрици от ред n, а с $M(n, \mathbf{C})[\lambda]$ — множеството на всички матрични λ-полиноми от ред n. Очевидно е, че $M(n, \mathbf{C}[\lambda])$ и $M(n, \mathbf{C})[\lambda]$ са пръстени спрямо обикновените операции събиране и умножение съответно на λ-матрици и λ-полиноми.

Задача. Докажете, че посоченото по-горе съответствие между λ-матриците и матричните λ-полиноми е изоморфизъм между пръстените $M(n, \mathbf{C}[\lambda])$ и $M(n, \mathbf{C})[\lambda]$.

Разглеждането на λ-матриците като матрични λ-полиноми позволява за λ-матриците да се развие теория за делимост, аналогична на теорията за делимост на числови полиноми. Тази теория е по-сложна от последната поради некомутативността на умножението и наличието на делители на нулата в матричния пръстен $M(n, \mathbf{C})$. Например степента на произведението на два матрични λ-полинома невинаги е равна на сумата от степените на отделните множители, тъй като може да се случи произведението на старшите им членове да бъде равно на нулевата матрица. Но тази степен ще бъде равна на сумата от степените на двата λ-полинома, ако поне един от техните старши членове не е делител на нулата. На нас ще ни бъде необходима само следната лема, която е частен случай на алгоритъма за деление с непълно частно и остатък.

Лема 4. *Нека* $A(\lambda)$ *е произволна* λ*-матрица от ред* n, *а* B *е произволна числова матрица от същия ред* n. *Тогава съществуват такива еднозначно определени* λ*-матрици* $Q_1(\lambda)$ *и* $Q_2(\lambda)$ *и числови матрици* R_1 *и* R_2 *от ред* n, *че да са изпълнени равенствата*

$$A(\lambda) = (B - \lambda E)\, Q_1(\lambda) + R_1, \quad A(\lambda) = Q_2(\lambda)\, (B - \lambda E) + R_2.$$

Доказателство. Ще докажем само съществуването и единствеността на матриците $Q_1(\lambda)$ и R_1. За $Q_2(\lambda)$ и R_2 доказателството е аналогично.

Нека λ-матрицата $A(\lambda)$ е от степен k и се представя във вида

$$A(\lambda) = A_k \lambda^k + A_{k-1} \lambda^{k-1} + \ldots + A_1 \lambda + A_0,$$

където $A_k \neq 0$.

Единственост. Ако матриците $\overline{Q}_1(\lambda)$ и $\overline{R}_1$ също удовлетворяват условията на лемата и

$$A(\lambda) = (B - \lambda E)\, \overline{Q}_1(\lambda) + \overline{R}_1,$$

чрез изваждане получаваме равенството

$$(B - \lambda E)\, [Q_1(\lambda) - \overline{Q}_1(\lambda)] = \overline{R}_1 - R_1.$$

Ако $Q_1(\lambda) \neq \bar{Q}_1(\lambda)$, то в лявата част на последното равенство имаме λ-матрица от положителна степен (степента на $Q_1(\lambda) - \bar{Q}_1(\lambda)$ плюс единица, тъй като единичната матрица E не е делител на нулата), а в дясната му част $\bar{R}_1 - R_1$ е числова матрица (нулевата матрица или матрица от нулева степен). Полученото противоречие показва, че $Q_1(\lambda) = \bar{Q}_1(\lambda)$, а тогава и $R_1 = \bar{R}_1$.

Съществуване. Лесно се вижда, че λ-матрицата $A(\lambda) + (B - \lambda E)A_k\lambda^{k-1}$ има степен, не по-висока от $k-1$. Ако

$$A(\lambda) + (B - \lambda E)A_k\lambda^{k-1} = A'_{k-1}\lambda^{k-1} + A'_{k-2}\lambda^{k-2} + \ldots + A'_0,$$

аналогично λ-матрицата

$$A(\lambda) + (B - \lambda E)A_k\lambda^{k-1} + (B - \lambda E)A'_{k-1}\lambda^{k-2}$$

има степен, не по-висока от $k-2$. Като продължим този процес ще достигнем до λ-матрицата

$$A(\lambda) + (B - \lambda E)(A_k\lambda^{k-1} + A'_{k-1}\lambda^{k-2} + A''_{k-2}\lambda^{k-3} + \ldots),$$

която има степен нула или е нулевата матрица, т. е. до числова матрица. Като означим тази матрица с R_1, получаваме

$$A(\lambda) = (B - \lambda E)(-A_k\lambda^{k-1} - A'_{k-1}\lambda^{k-2} - A''_{k-2}\lambda^{k-3} - \ldots) + R_1.$$

Полагаме $Q_1(\lambda) = -A_k\lambda^{k-1} - A'_{k-1}\lambda^{k-2} - A''_{k-2}\lambda^{k-3} - \ldots$ и виждаме че матриците $Q_1(\lambda)$ и R_1 удовлетворяват условията на лемата, с което доказателството е завършено.

Нека A и B са две произволни числови матрици. Засега не умеем да решаваме въпроса, дали тези матрици са подобни или не. Но техните характеристични матрици $A - \lambda E$ и $B - \lambda E$ са λ-матрици и въпросът за еквивалентността им се решава ефективно. Това подсказва идеята да се намери връзка между подобието на числовите матрици A и B и еквивалентността на техните характеристични матрици. Тази връзка се дава от следната важна

Теорема 5 (основна теорема за подобие на числовите матрици). *Числовите матрици A и B са подобни тогава и само тогава, когато техните характеристични λ-матрици $A - \lambda E$ и $B - \lambda E$ са еквивалентни.*

Доказателство. Нека матриците A и B са подобни, т. е. съществува такава неособена матрица T, че $B = T^{-1}AT$. Тогава

$$T^{-1}(A - \lambda E)T = T^{-1}AT - \lambda T^{-1}ET = B - \lambda E.$$

Но неособените матрици T^{-1} и T са унимодулярни. Следователно λ-матрицата $B - \lambda E$ се получава от λ-матрицата $A - \lambda E$ чрез умножаване отляво и отдясно с унимодулярни матрици, т. е. по теорема 4, $A - \lambda E$ е еквивалентна на $B - \lambda E$.

Обратно, нека $A - \lambda E \sim B - \lambda E$. Трябва да покажем, че матриците A и B са подобни. Съгласно теорема 4 съществуват такива унимодулярни матрици $U(\lambda)$ и $V(\lambda)$, че

(1) $$U(\lambda)(A-\lambda E)V(\lambda)=B-\lambda E.$$

Тъй като унимодулярните матрици притежават обратни матрици, които са също λ-матрици, от (1) получаваме равенствата

$$U(\lambda)(A-\lambda E)=(B-\lambda E)V_1^{-1}(\lambda),$$

(2) $$(A-\lambda E)V(\lambda)=U^{-1}(\lambda)(B-\lambda E).$$

Според лема 4 съществуват λ-матрица $Q_1(\lambda)$ и числова матрица R_1, така че

(3) $$U(\lambda)=(B-\lambda E)Q_1(\lambda)+R_1.$$

Аналогично

(4) $$V(\lambda)=Q_2(\lambda)(B-\lambda E)+R_2,$$

където R_2 е числова матрица.

Като заместим във формула (1) матрицата $U(\lambda)$ с нейното равно от (?) и извършим умножението, ще получим

$$B-\lambda E=(B-\lambda E)\ Q_1(\lambda)(A-\lambda E)V(\lambda)+R_1(A-\lambda E)V(\lambda).$$

Във второто събираемо на последното равенство заместваме матрицата $V(\lambda)$ с нейното равно от (4), извършваме умноженията и пренасяме събираемото $R_1(A-\lambda E)R_2$ в лявата част на равенството. Така получаваме равенството

(5) $$B-\lambda E-R_1(A-\lambda E)R_2=F(\lambda),$$

където

$$F(\lambda)=(B-\lambda E)Q_1(\lambda)(A-\lambda E)V(\lambda)+$$
$$+R_1(A-\lambda E)Q_2(\lambda)(B-\lambda E).$$

От (3) следва, че $R_1=U(\lambda)-(B-\lambda E)Q_1(\lambda)$. Заместваме R_1 с този израз във второто събираемо на $F(\lambda)$ и получаваме

$$F(\lambda)=(B-\lambda E)Q_1(\lambda)(A-\lambda E)V(\lambda)+U(\lambda)(A-\lambda E)Q_2(\lambda)(B-\lambda E)-$$
$$-(B-\lambda E)Q_1(\lambda)(A-\lambda E)Q_2(\lambda)(B-\lambda E).$$

Като използуваме изразите от (2) за $U(\lambda)(A-\lambda E)$ и $(A-\lambda E)V(\lambda)$ последното равенство можем да представим във вида

(6) $$F(\lambda)=(B-\lambda E)\Phi(\lambda)(B-\lambda E),$$

където $\Phi(\lambda)$ е λ-матрица. Ще докажем, че $\Phi(\lambda)=0$. Действително, ако $\Phi(\lambda)\neq 0$, матричният λ-полином $\Phi(\lambda)$ ще има степен $m\geqq 0$. Тогава от (6) ще следва, че λ-полиномът $F(\lambda)$ има степен $m+2\geqq 2$, тъй като старши коефициентът на $B-\lambda E$ не е делител на нулата. От друга страна, равенството (5) показва, че степента на $F(\lambda)$ е не по-висока от 1.

Полученото противоречие означава, че $\Phi(\lambda)=0$ и затова $F(\lambda)=0$. По този начин от (5) получаваме

$$B-\lambda E=R_1(A-\lambda E)R_2=R_1AR_2-\lambda R_1R_2.$$

Като сравним коефициентите в последното равенство съответно пред нулевата и пред първата степен на λ заключаваме, че

$$B=R_1AR_2,\ E=R_1R_2.$$

От второто равенство следва, че $R_1=R_2^{-1}$ и като заместим R_1 с R_2^{-1} в първото равенство, получаваме

$$B=R_2^{-1}AR_2, \tag{7}$$

т. е. матриците A и B са подобни. Теоремата е доказана.

Ако вземем предвид, че две λ-матрици са еквивалентни тогава и само тогава, когато съвпадат техните инвариантни множители (виж § 5), доказаната теорема можем да формулираме и по следния начин.

Следствие 7. *Числовите матрици A и B са подобни тогава и само тогава, когато инвариантните множители на техните характеристични матрици $A-\lambda E$ и $B-\lambda E$ съвпадат.*

Заедно с доказателството на теорема 5 получихме и метод за отговор на въпроса, подобни ли са две числови матрици A и B, който се състои в следното:

1. Намираме по един от познатите ни начини каноничните форми на λ-матриците $A-\lambda E$ и $B-\lambda E$.

2. Ако получените канонични матрици съвпадат, то $A-\lambda E\sim B-\lambda E$ и затова A и B са подобни; ако те не съвпадат, то A и B не са подобни.

Ако искаме да намерим и неособената матрица R_2, която в (7) трансформира матрицата A в матрицата B (при положение че $A-\lambda E\sim B-\lambda E$), достатъчно е да намерим матрицата $V(\lambda)$ от (1), а след това и нейния остатък R_2 от (4). Унимодулярната λ-матрица $V(\lambda)$ е произведение на елементарните λ-матрици, които съответстват на елементарните преобразувания на стълбовете при преминаването от $A-\lambda E$ към $B-\lambda E$, взети в същия ред с тези преобразувания, тъй като $V(\lambda)$ е десен множител на $A-\lambda E$ в равенството (1).

Пример. Дадени са матриците

$$A=\begin{pmatrix}4 & 9\\ -1 & -2\end{pmatrix}\ \text{и}\ B=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

Да се докаже, че A и B са подобни, и да се намери матрица T, за която $B=T^{-1}AT$.

Решение. С елементарни преобразувания привеждаме характеристичните матрици $A-\lambda E$ и $B-\lambda E$ в каноничен вид. Тъй като за намирането на споменатата λ-матрица $V(\lambda)$ ще ни интересуват само елементарните преобразувания на стълбовете, само в тези случаи над знака за еквивалентност „$\sim$“ ще записваме елементарната матрица, която отговаря на съответното преобразуване. За матрицата $A-\lambda E$ получаваме

$$A-\lambda E=\begin{pmatrix}4-\lambda & 9\\ -1 & -2-\lambda\end{pmatrix}\sim\begin{pmatrix}4-\lambda & 9\\ 1 & 2+\lambda\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}1 & 2+\lambda\\ 4-\lambda & 9\end{pmatrix}\sim\begin{pmatrix}1 & 2+\lambda\\ 0 & \lambda^2-2\lambda+1\end{pmatrix}\ E_{12}(-2-\lambda)\ \sim\ \begin{pmatrix}1 & 0\\ 0 & (\lambda-1)^2\end{pmatrix},$$

където само последното преобразуване се отнася за стълбовете и се състои в прибавяне на първия стълб, умножен с $-\lambda-2$, към втория.

Аналогично имаме

$$B-\lambda E=\begin{pmatrix}1-\lambda & 1\\ 0 & 1-\lambda\end{pmatrix}E_{21}(\lambda)\sim\begin{pmatrix}1 & 1\\ \lambda(1-\lambda) & 1-\lambda\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}1 & 1\\ 0 & (\lambda-1)^2\end{pmatrix}E_{12}(-1)\sim\begin{pmatrix}1 & 0\\ 0 & (\lambda-1)^2\end{pmatrix},$$

където първото и последното преобразуване се отнасят за стълбовете и са съответно прибавяне на втория стълб, умножен с λ, към първия стълб и прибавяне на първия стълб, умножен с -1, към втория стълб.

Каноничните матрици на $A-\lambda E$ и $B-\lambda E$ съвпадат и затова A и B са подобни. За да получим матрицата T, първо трябва да намерим редица от елементарни преобразувания, която привежда $A-\lambda E$ в матрицата $B-\lambda E$. Очевидно една такава радица е редицата от преобразувания, която привежда $A-\lambda E$ в каноничния вид, допълнена с преобразуванията, които привеждат този канонничен вид в матрицата $B-\lambda E$. Както вече посочихме, нас ни интересуват само матриците, които съответстват на елементарните преобразувания на стълбовете. Затова търсената редица от елементарни матрици е

$$E_{12}(-2-\lambda)=\begin{pmatrix}1 & -2-\lambda\\ 0 & 1\end{pmatrix},\quad E_{12}(1)=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\quad E_{21}(-\lambda)=$$

$$=\begin{pmatrix}1 & 0\\ -\lambda & 1\end{pmatrix},$$

тъй като матриците $E_{12}(1)$ и $E_{21}(-\lambda)$ съответстват на обратните преобразувания, които се осъществяват посредством матриците $E_{12}(-1)$ и $E_{21}(\lambda)$ (виж лема 3). Следователно

$$V(\lambda)=E_{12}(-2-\lambda)E_{12}(1)E_{21}(-\lambda)=\begin{pmatrix}\lambda^2+\lambda+1 & -\lambda-1\\ -\lambda & 1\end{pmatrix}=$$

$$=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\lambda^2+\begin{pmatrix}1 & -1\\ -1 & 0\end{pmatrix}\lambda+\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}.$$

Сега делим $V(\lambda)$ на $B-\lambda E$ така, че частното да е отляво на $B-\lambda E$, т. е.

$$V(\lambda)+\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}(B-\lambda E)\lambda=\begin{pmatrix}2 & 0\\ -1 & 0\end{pmatrix}\lambda+\begin{pmatrix}1-1\\ 0 & 1\end{pmatrix},$$

$$V(\lambda)+\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}(B-\lambda E)\lambda+\begin{pmatrix}2 & 0\\ -1 & 0\end{pmatrix}(B-\lambda E)=\begin{pmatrix}3 & 1\\ -1 & 0\end{pmatrix}.$$

Следователно търсената матрица T, която трансформира A в B, е матрицата

$$T=\begin{pmatrix}3 & 1\\ -1 & 0\end{pmatrix}.$$

Разбира се, матрицата, която трансформира A и B, далеч не е единствена. Такава е например и матрицата

$$T_1=\begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}.$$

Забележка. Тук отново следва да обърнем внимание, че ограничението да разглеждаме само числови матрици е несъществено за получените в този параграф резултати — те остават верни и доказателствата им са същите за квадратни матрици с елементи от произволно поле.

§ 8. Единственост на нормалната форма на линейните преобразувания

В параграф 3 доказахме, че всяко линейно преобразуване φ в крайномерно комплексно линейно пространство V може да се приведе в нормална форма, т. е. може да се намери такъв базис във V, че матрицата на φ в този базис да бъде жорданова. Но как може практически да намерим нормалната форма на преобразуването φ? Тази задача се състои от две части:

1. Ако A е матрица на линейното преобразуване φ в базиса $e_1, e_2, \ldots, e_n$ на пространството V, то трябва да се намери жорданова матрица J, която е подобна на A (J ще наричаме още *жорданова форма* на A).

2. След като сме намерили подобната на A жорданова матрица J, трябва да намерим базис $f_1, f_2, \ldots, f_n$ на V, в който J е матрица на φ. Това е равносилно на задачата да се намери такава неособена матрица $T=(\tau_{ij})$, че $A=TJT^{-1}$, тъй като след намирането на T базисът $f_1, f_2, \ldots, f_n$ е непълно определен от равенствата

$$f_j=\sum_{i=1}^{n} \tau_{ij} e_i \quad (j=1, 2, \ldots, n).$$

Втората част на поставената задача, както видяхме в предишния параграф, можем да решим напълно ефективно. Затова нашата цел е да посочим метод за решаване на първата ѝ част.

Твърдение 16. *Ако J_1 е жорданова клетка от ред n_1 с характеристичен корен λ_1, то инвариантните множители на характеристичната ѝ матрица $J_1-\lambda E$ са*

$$e_1(\lambda)=e_2(\lambda)=\ldots=e_{n_1-1}(\lambda)=1,\ e_{n_1}(\lambda)=(\lambda-\lambda_1)^{n_1},$$

т. е. $J_1-\lambda E$ е еквивалентна на каноничната матрица

$$(1) \qquad \begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ 0 & & & & (\lambda-\lambda_1)^{n_1} \end{pmatrix}$$

от ред n_1.

Доказателство. Тъй като детерминантата $|J_1-\lambda E|$ на матрицата

$$J_1-\lambda E=\begin{pmatrix} \lambda_1-\lambda & 0 & \dots & 0 & 0 \\ 1 & \lambda_1-\lambda & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_1-\lambda & 0 \\ 0 & 0 & \dots & 1 & \lambda_1-\lambda \end{pmatrix}$$

е равна на $(\lambda_1-\lambda)^{n_1}$, то

$$d_{n_1}(\lambda)=(-1)^{n_1}|J_1-\lambda E|=(\lambda-\lambda_1)^{n_1}.$$

От друга страна, между минорите от ред n_1-1 на матрицата $J_1-\lambda E$ има минор, който е равен на 1. Това е минорът, който се получава, като зачеркнем първия ред и последния стълб на $J_1-\lambda E$. Поради това $d_{n_1-1}(\lambda)=1$. Но тогава всички останали полиноми $d_1(\lambda), \dots, d_{n_1-2}(\lambda)$ са също равни на единица. Понеже

$$e_1(\lambda)=d_1(\lambda),\ e_k(\lambda)=\frac{d_k(\lambda)}{d_{k-1}(\lambda)}\ (k=2, 3, \dots, n_1),$$

получаваме, че

$$e_1(\lambda)=e_2(\lambda)=\dots=e_{n_1-1}(\lambda)=1,\ e_{n_1}(\lambda)=(\lambda-\lambda_1)^{n_1},$$

т. е. матрицата $J_1-\lambda E$ е еквивалентна на каноничната матрица (1).

Лема 5. *Ако полиномите* $f_1(\lambda), f_2(\lambda), \dots, f_n(\lambda)$ *от пръстена* $\mathbf{C}[\lambda]$ *са два по два взаимно прости, матрицата*

$$A(\lambda)=\begin{pmatrix} f_1(\lambda) & & & 0 \\ & f_2(\lambda) & & \\ & & \ddots & \\ 0 & & & f_n(\lambda) \end{pmatrix}$$

е еквивалентна на матрицата

$$B(\lambda)=\begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ & & & 1 \\ 0 & & & \prod_{i=1}^{n} f_i(\lambda) \end{pmatrix}$$

Доказателство. Нека $n=2$. Тъй като полиномите $f_1(\lambda)$ и $f_2(\lambda)$ са взаимно прости, съществуват такива полиноми $u(\lambda)$ и $v(\lambda)$, че да е изпълнено равенството

$$u(\lambda)f_1(\lambda)+v(\lambda)f_2(\lambda)=1.$$

Тогава

$$A(\lambda)=\begin{pmatrix} f_1(\lambda) & 0 \\ 0 & f_2(\lambda) \end{pmatrix}\sim\begin{pmatrix} f_1(\lambda) & u(\lambda)f_1(\lambda) \\ 0 & f_2(\lambda) \end{pmatrix}\sim$$

$$\sim\begin{pmatrix} f_1(\lambda) & u(\lambda)f_1(\lambda)+v(\lambda)f_2(\lambda) \\ 0 & f_2(\lambda) \end{pmatrix}\sim\begin{pmatrix} f_1(\lambda) & 1 \\ 0 & f_2(\lambda) \end{pmatrix}\sim$$

$$\sim\begin{pmatrix} 1 & f_1(\lambda) \\ f_2(\lambda) & 0 \end{pmatrix}\sim\begin{pmatrix} 1 & f_1(\lambda) \\ 0 & -f_1(\lambda)f_2(\lambda) \end{pmatrix}\sim$$

$$\sim\begin{pmatrix} 1 & 0 \\ 0 & -f_1(\lambda)f_2(\lambda) \end{pmatrix}\sim\begin{pmatrix} 1 & 0 \\ 0 & f_1(\lambda)f_2(\lambda) \end{pmatrix}=B(\lambda).$$

По-нататък доказателството се провежда с индукция спрямо n, като се използват подобни съображения.

Нека сега

$$J=\begin{pmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_m \end{pmatrix} \tag{2}$$

е произволна жорданова матрица от ред n с жорданови клетки $J_1, J_2, \ldots, J_m$ и $\lambda_1, \lambda_2, \ldots, \lambda_s$ са всичките различни характеристични корени на J. Да предположим, че q_i на брой от жордановите клетки $J_1, J_2, \ldots, J_m$ са с характеристичен корен λ_i $(i=1, 2, \ldots, s)$, и нека редовете k_{ij} $(j=1, 2, \ldots, q_i)$ на тези клетки са разположени в нерастящ ред, т. е.

$$k_{i1}\geqq k_{i2}\geqq \ldots \geqq k_{iq_i}\ (i=1, 2, \ldots, s).$$

Да отбележим, че

$$\sum_{i=1}^{s} q_i=m,\ \sum_{i=1}^{s}\sum_{j=1}^{q_i} k_{ij}=n.$$

Тогава на жордановата матрица J можем да съпоставим следната таблица:

$$\begin{Bmatrix} \lambda_1 & \lambda_2 & \ldots & \lambda_s \\ k_{11} & k_{21} & \ldots & k_{s1} \\ k_{12} & k_{22} & \ldots & k_{s2} \\ \ldots & \ldots & \ldots & \ldots \\ k_{1q} & k_{2q} & \ldots & k_{sq} \end{Bmatrix}, \tag{3}$$

съставена от s стълба и от $q+1$ реда, където $q=\max\{q_1, q_2, \ldots, q_s\}$. При това, ако $q_i<q$, то в i-тия стълб на таблицата (3) под k_{iq_i} са поставени нули, т. е. $k_{i,\,q_i+1}=k_{i,\,q_i+2}=\ldots=k_{iq}=0$.

Таблицата (3) се нарича *таблица на жордановата матрица J*.

Очевидно *две жорданови матрици имат една и съща таб-*

лица тогава и само тогава, когато те имат съвпадащи системи от жордановн клетки, т. е. когато те се различават само по реда на записването на жордановите си клетки по главния диагонал.

Твърденне 17. *Ако жордановата матрица J има таблица (3), инвариантни множители на характеристичната й матрица $J-\lambda E$ са полиномите*

$$e_1(\lambda)=e_2(\lambda)=\ldots=e_{n-q}(\lambda)=1,$$

$$e_{n-j+1}(\lambda)=\prod_{j=1}^{s}(\lambda-\lambda_j)^{k_{ij}}\ (j=1,\ 2,\ \ldots,\ q). \tag{4}$$

Доказателство. Ако матрицата J има жордановн клетки $J_1, J_2, \ldots, J_m$, т. е. ако J е от вида (2), то характеристичната й матрица е от вида

$$J-\lambda E=\begin{pmatrix} J_1-\lambda E_1 & & 0 \\ & J_2-\lambda E_2 & \\ & & \\ 0 & & J_m-\lambda E_m \end{pmatrix}, \tag{5}$$

където $E_i\ (i=1,\ 2,\ \ldots,\ m)$ е единичната матрица от ред, равен на реда на клетката J_i. Очевидно е, че ако извършваме елементарни преобразувания само над редовете и стълбовете на матрицата (5), които минават през клетката й $J_i-\lambda E_i$, то не изменяме елементите, които са вън от тази клетка. Затова според твърдение 16 всяка от тези клетки може да се замени със съответната клетка от вида (1). С други думи, матрицата $J-\lambda E$ е еквивалентна на диагонална матрица $D_1(\lambda)$, по главния диагонал на която то стоят известен брой единици и неединичните полиноми измежду полиномите

$$\begin{array}{l} (\lambda-\lambda_1)^{k_{11}},\ (\lambda-\lambda_2)^{k_{21}},\ \ldots,\ (\lambda-\lambda_s)^{k_{s1}}, \\ (\lambda-\lambda_1)^{k_{12}},\ (\lambda-\lambda_2)^{k_{22}},\ \ldots,\ (\lambda-\lambda_s)^{k_{s2}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (\lambda-\lambda_1)^{k_{1q}},\ (\lambda-\lambda_2)^{k_{2q}},\ \ldots,\ (\lambda-\lambda_s)^{k_{sq}}, \end{array} \tag{6}$$

съответствуващи на всички жордановн клетки на матрицата J. Не посочваме местата по главния диагонал, на които стоят полиноми от (6), защото във всяка диагонална λ-матрица диагоналните елементи могат произволно да се разместват чрез разместване на едноименни редове и стълбове. Тази забележка по-нататък трябва да се има предвид. Очевидно произведението на полиномите от j-тия ред на (6) е точно полиномът $e_{n-j+1}(\lambda)$ от (4) $(j=1,\ 2,\ \ldots,\ q)$. Тъй като по условие числата $\lambda_1, \lambda_2, \ldots, \lambda_s$ са различни, то полиномите, които стоят в j-тия ред на (6), са два по два взаимно прости. Съгласно лема 5 чрез елементарни преобразувания те могат да се заменят с произведението им $e_{n-j+1}(\lambda)$

и известен брой единици. Като извършим това за $j=1, 2, \ldots q$, получаваме, че $J-\lambda E$ е еквивалентна на матрицата

$$D(\lambda)=\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & e_{n-q+1}(\lambda) & \\ & & & & \ddots \\ & & & & e_{n-1}(\lambda) \\ 0 & & & & e_n(\lambda) \end{pmatrix}$$

Матрицата $D(\lambda)$ е канонична, тъй като по условие $k_{ij} \geqq k_{i,j+1}$ за $j=1, 2, \ldots, q-1$, т. е. $e_{n-j+1}(\lambda)$ се дели на $e_{n-j}(\lambda)$ и всеки от тези полиноми е нормиран. Следователно инвариантните множители на жордановата матрица J са точно полиномите (4).

Пример. Нека

$$J=\begin{pmatrix} \left|\begin{matrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{matrix}\right| & & & & \\ & \left|\begin{matrix} 3 \end{matrix}\right| & & & \\ & & \left|\begin{matrix} 0 \end{matrix}\right| & & \\ & & & \left|\begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}\right| & \\ & & & & \end{pmatrix}.$$

Тогава таблицата на J е

$$\begin{pmatrix} \lambda_1=1 & \lambda_2=3 & \lambda_2=0 \\ 3 & 1 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Инвариантните множители на матрицата J, която е от ред 7, са следните:

$$e_1(\lambda)=e_2(\lambda)=e_3(\lambda)=e_4(\lambda)=e_5(\lambda)=1,$$
$$e_6(\lambda)=(\lambda-1)^0(\lambda-3)^0(\lambda-0)^1=\lambda,$$
$$e_7(\lambda)=(\lambda-1)^3(\lambda-1)^1(\lambda-0)^2=\lambda^2(\lambda-1)^3(\lambda-3).$$

Важно следствие от доказаното твърдение е следната

Теорема 6. *Две жорданови матрици са подобни тогава и само тогава, когато имат една и съща таблица, т. е. когато те се различават само по местата на клетките си по главния диагонал.*

Доказателство. Ако жордановите матрици J и J' имат една и съща таблица, съгласно твърдение 17 техните характеристични матрици $J-\lambda E$ и $J'-\lambda E$ имат еднакви инвариантни множители. Но тогава по следствие 7 матриците J и J' са подобни.

Обратно, нека жордановите матрици J и J' са подобни. Ха-

Рактеристичните матрици $J-\lambda E$ и $J'-\lambda E$ по следствие 7 имат еднакви инвариантни множители. Нека полиномите

$$e_{n-j+1}(\lambda)=\prod_{i=1}^{s}(\lambda-\lambda_i)^{k_{ij}}\ (j=1, 2, \ldots, q)$$

са различните им от единица инвариантни множители. Но по тези полиноми можем, като пресметнем кратностите k_{ij} на различните им корени, да възстановим таблицата (3) на жордановата матрица, т. е. J и J' имат една и съща таблица. Теоремата е доказана.

Следствие 8. *Всяка жорданова матрица, която е подобна на диагонална матрица, е диагонална. Две диагонални матрици са подобни тогава и само тогава, когато се получават една от друга с пермутиране на елементите, които стоят по главния диагонал.*

Не е трудно да се съобрази, че теорема 6 е всъщност едно твърдение за единствеността на нормалната форма на дадено линейно преобразуване, а именно тя може да се изкаже по следния начин:

Теорема 7 (теорема за единственост на нормалната форма на линейно преобразуване). *Нормалната форма на всяко линейно преобразуване φ в крайномерно пространство V е единствена с точност до реда на следване на групите от базисни вектори, във всяка от които φ има жарданова клетка за своя матрица.*

Доказателството на горните резултати ни дава следния практически метод за намиране на жордановата форма на една комплексна матрица A.

1. Намираме инвариантни множители $e_i(\lambda)$ на характеристичната матрица $A-\lambda E$ (те са инвариантни множители и на $J-\lambda E$). намираме корените на $e_i(\lambda)$ и пресмятаме кратностите на тези корени.

2. Съставяме таблица (3) с помощта на получените корени и кратностите им.

3. Построяваме жорданова матрица, която има таблица съвпадаща със съставената от нас.

С това дадохме пълен отговор на трите проблема, поставени в началото на настоящата глава. Накрая нека да отбележим, че твърденията от този параграф и техните доказателства остават в сила за линейни пространства и матрици над произволни полета

ГЛАВА XI

ТЕЛА. ЛИНЕЙНИ АСОЦИАТИВНИ АЛГЕБРИ НАД ПОЛЕТА

§ 1. Тела

В глава V разгледахме понятието пръстен и някои основни свойства, свързани с него. Пръстените в глава VI предполагахме, че са комутативни. Тук ще се освободим от това ограничение и ще насочим вниманието си към един клас от пръстени, които имат много общи свойства с полетата.

Нека A е произволен (в общия случай некомутативен) пръстен с единица e. Изображението $\chi: Z \to A$ на пръстена Z на целите числа в пръстена A, което се определя с равенството $\chi(m) = me$ за всяко $m \in Z$, е хомоморфизъм на пръстена Z в пръстена A, т. е. изпълнени са равенствата

$$\chi(m+n)=\chi(m)+\chi(n),\ \chi(mn)=\chi(m)\ \chi(n)$$

за всеки две цели числа m и n. Ако ядрото $\ker\varphi=\{k|k \in Z,\ \chi(k)=0\}$ на χ е нулевият идеал в Z, то χ е изоморфизъм на Z върху подпръстена на A, който се състои от всички елементи от вида me ($m \in Z$). В този случай казваме, че A е *пръстен с характеристика нула.*

Задача. Докажете, че пръстенът A с единица e има характеристика нула тогава и само тогава, когато от $m \neq n$ ($m, n \in Z$) следва $me \neq ne$.

Ако ядрото $\ker\chi$ на хомоморфизма $\chi: Z \to A$ е ненулев идеал, то $\ker\chi$ е главен идеал в Z, който се поражда от някое естествено число p, т. е. $\ker\chi=(p)$, където $p>0$. В този случай казваме, че пръстенът A има *положителна* или *крайна характеристика* p.

Задача. Докажете, че ако A е пръстен с положителна характеристика p, то p е най-малкото естествено число, за което $pa=0$ за всеки елемент a от A.

Като твърдение 7 от глава V се доказва и следното твърдение:

Твърдение 1. *Ако A е пръстен с единица и без делители на нулата, то характеристиката на A е или равна на нула, или е просто число.*

Определение 1. Ненулевият пръстен D с единица e се нарича *тяло*, ако мултипликативната му група D^* съвпада с множеството $D \setminus \{0\}$ от всички ненулеви елементи на D, т. е. ако всеки ненулев елемент на D е обратим в D.

Примери

1. Всяко поле е тяло, в което е изпълнен комутативния

закон за умножението. Обратно, всяко комутативно тяло е поле.

2. Нека K е подмножество на пръстена $M(2, \mathbb{C})$ на матриците от втори ред с комплексни елементи, което се състои от всички матрици от вида

$$\begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix},$$

където $z, t \in \mathbb{C}$, а $\bar{z}$ и $\bar{t}$ са съответно комплексно спрегнатите на z и t. Ако

$$a = \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix}$$

е ненулева матрица, поне едно от числата z и t е различно от нула и детерминантата $d = z\bar{z} + t\bar{t} = |z|^2 + |t|^2$ на a е положително реално число. В този случай

$$a^{-1} = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix},$$

където $u = \frac{\bar{z}}{d}$, $v = -\frac{t}{d}$. Следователно всеки ненулев елемент a от K е обратим и неговият обратен елемент a^{-1} също се съдържа в K. Нека

$$a = \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix}, \quad b = \begin{pmatrix} z_1 & t_1 \\ -\bar{t}_1 & \bar{z}_1 \end{pmatrix}$$

са две произволни матрици от K. Тогава

$$a - b = \begin{pmatrix} z - z_1 & t - t_1 \\ -\overline{(t - t_1)} & \overline{z - z_1} \end{pmatrix}, \quad ab = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix},$$

където $x = zz_1 - t\bar{t}_1$ и $y = zt_1 + t\bar{z}_1$. Следователно $a - b$ и ab са също елементи от K. Така проверихме, че K е подпръстен на пръстена $M(2, \mathbb{C})$. Освен това в пръстена K се съдържа единичната матрица $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и затова K е пръстен с единица. Тъй като всеки ненулев елемент от пръстена K е обратим в K, то K е тяло. Тялото K се нарича *тяло на кватернионите*. Тялото K на кватернионите е некомутативно, т. е. K не е поле. Действително матриците

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

се съдържат в K, но те не комутират, защото

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Тялото на кватернионите е най-простият пример на некомутативно тяло, но едновременно с това то е един от най-важните обекти в теорията на телата.

Подпръстенът B на тялото D се нарича подтяло на D, ако B съдържа единицата e на D и заедно с всеки ненулев елемент $b \in B$ в B се съдържа и неговият обратен b^{-1}. Ясно е, че подтялото, разглеждано като пръстен, е тяло.

Задача. Докажете, че сечението на произволна съвкупност от подтела на дадено тяло D е също подтяло на D.

Всяко комутативно подтяло на D се нарича подполе на тялото D.

Ако A е произволен пръстен, то със $Z(A)$ ще означаваме подмножеството на A, което се състои от всички елементи z на A, такива, че $za=az$ за всяко a от A, т. е.

$Z(A)=\{z \mid z \in A,\ az=za$ за всяко $a \in A\}$.

Подмножеството $Z(A)$ на A се нарича *център* на пръстена A.

Ако b е фиксиран елемент от пръстена A, подмножеството на A от всички елементи a от A, за които е изпълнено равенството $ab=ba$, се нарича *нормализатор* на елемента b и се означава с $N(b)$.

Задача

а) Докажете, че нормализаторът $N(b)$ на всеки елемент b от пръстена A е подпръстен на A.

в) Докажете, че $N(b)=A$ тогава и само тогава, когато $b \in Z(A)$.

с) Докажете равенството $Z(A)=\bigcap_{b \in A} N(b)$, т. е. докажете, че центърът на пръстена A е сечение на нормализаторите на всички елементи на пръстена A.

d) Докажете, че центърът $Z(A)$ на пръстена A е комутативен подпръстен на A, който съдържа единичния елемент на A (ако той съществува).

Твърдение 2. *Нормализаторът $N(d)$ на всеки елемент d от тялото D е подтяло на D.*

Наистина лесно се проверява, че $N(d)$ е подпръстен на D, който съдържа единицата e на тялото D. Нека $a \in N(d)$ и $a \neq 0$. Тогава $ad=da$. Като умножим последното равенство отляво и отдясно с a^{-1}, получаваме $da^{-1}=a^{-1}d$ и затова $a^{-1} \in N(d)$. Следователно $N(d)$ е подтяло на D.

Следствие 1. *Центърът $Z(D)$ на всяко тяло D е подполе на D.*

Действително от предишната задача знаем, че $Z(D)=\bigcap_{a \in D} N(d)$. Тъй като сечение на подтела е подтяло, то $Z(D)$ е комутативно подтяло на D, т. е. $Z(D)$ е подполе на D.

Следствие 2. *Нека D е тяло с характеристика $p \geqq 0$. Тогава ако $p=0$, то сечението на всички подтела на D е подполе на центъра $Z(D)$ на D, което е изоморфно на полето Q на рационалните числа. Ако $p>0$, то p е просто число и*

сечението на всички подтела на D е подполе на центъра $Z(D)$ на D, което е изоморфно на полето Z_p на класовете остатъци по модул p.

Наистина сечението на всички подтела на D съвпада със сечението на всички подполета на полето $Z(D)$ и характеристиките на D и на центъра $Z(D)$ на D са еднакви. Затова следствието се получава от съответния факт за сечението на всички подполета на едно поле (виж следствие 1 от глава VIII).

Примери

1. Нека P е произволно поле. От линейната алгебра е известно, че центърът $Z(M(n, P))$ на матричния пръстен $M(n, P)$ се състои от всички скаларни матрици αE, където E е единичната матрица от ред n, а $\alpha \in P$.

2. Всяка матрица от вида

$$\alpha E = \alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix},$$

където α е реално число, се съдържа в тялото K на кватернионите (защото $\alpha = \bar{\alpha}$) и комутира с всички елементи от K, т. е. $\alpha E \in Z(K)$. Нека матрицата

$$S = \begin{pmatrix} u & v \\ -\bar{v} & u \end{pmatrix}$$

е от центъра $Z(K)$. Тогава

$$S \cdot \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix} = \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix} \cdot S$$

за всеки две комплексни числа z и t. Като изчислим двете произведения в последното равенство и приравним елементите на получените матрици, получените равенствата

$$uz - v\bar{t} = zu - tv, \quad ut + v\bar{z} = zv + t\bar{u},$$
$$-\bar{v}z - \bar{u}\bar{t} = -tu - \bar{z}\bar{v}, \quad -\bar{v}t + \bar{z}\bar{u} = -\bar{t}v + \bar{z}\bar{u},$$

които са изпълнени за всеки две комплексни числа z и t. Като положим $z = 0$ и $t = 1$, от първите равенства получаваме $u = \bar{u}$ и $v = \bar{v}$. При $z = 0$ и $t = i$ пък получаваме $v = -\bar{v}$ и затова $v = 0$. Следователно матрицата S е от вида $u\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = uE$, където u е реално число. По такъв начин доказахме равенството

$$Z(K) = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} | \alpha \in R \right\}.$$

Задача. Докажете, че ненулевият пръстен D е тяло тогава и само тогава, когато за всяко b от D и за всеки ненулев елемент a от D уравненията

$$ax = b, \quad ya = b$$

имат по едно-единствено решение в D.

Задача. Докажете, че всеки ненулев краен пръстен без делители на нулата е тяло.

§ 2. Линейни асоциативни алгебри над дадено поле

Болшинството от най-важните и често срещани примери на пръстени се оказват едновременно и линейни пространства над някое поле. При това в тях добре се съчетават двете понятия пръстен и линейно пространство. Затова съвършено естествено възниква следното определение.

Определение 2. Пръстенът A се нарича *линейна асоциативна алгебра* над полето P, ако A е линейно пространство над P спрямо операциите събиране в пръстена A и умножение на елементи от A с елементи от полето P, при което за всеки два елемента a и b от A и за всяко λ от P са изпълнени равенствата

$$\lambda(ab)=(\lambda a)\,b=a\,(\lambda b).$$

Ако пръстенът A е комутативен, алгебрата A се нарича комутативна. Размерността $\dim_P A$ на линейното пространство A над P ще наричаме размерност на алгебрата A над полето P. Ако тази размерност е крайна, то A се нарича *крайномерна алгебра* над P. В противен случай A се нарича *безкрайномерна алгебра* над P. Алгебрите над полето R на реалните числа се наричат реални алгебри.

По-нататък ще разглеждаме само линейни асоциативни алгебри над поле P и затова за краткост ще ги наричаме алгебри над P.

Примери

1. Ако P е произволно поле, то P е едномерна алгебра над себе си. В частност полето R на реалните числа е едномерна алгебра над R, а полето C на комплексните числа е едномерна алгебра над C.

2. Ако L е произволно разширение на полето P, то L е комутативна алгебра над P. Алгебрата L над P е крайномерна тогава и само тогава, когато L е крайномерно разширение на P и в този случай степента $[L:P]$ на разширението L на P е равна на размерността $\dim_P L$ на алгебрата L над полето P. Полето C на комплексните числа е двумерна алгебра над полето R на реалните числа. Полетата R и C са безкрайномерни алгебри над полето Q на рационалните числа.

3. Нека V е произволно линейно пространство над полето P. Във V въвеждаме умножение с равенството $xy=0$ за всеки два вектора $x, y \in V$. Лесно се проверява, че относно това умножение линейното пространство V се превръща в алгебра над P. За да подчертаем факта, че произведението на всеки два елемента на алгебрата V е равно на нула, ще казваме, че V е алгебра с нулево умножение над полето P.

4. Пръстенът $P[x]$ на полиномите на променливата x с коефициенти от полето P е безкрайномерна алгебра над P. По-общо пръстенът $P[x_1, x_2, \ldots, x_n]$ на полиномите на променливите $x_1, x_2, \ldots, x_n$ е безкрайномерна алгебра над полето P.

5. Пръстенът $M(n, P)$ на всички квадратни матрици от ред n с елементи от полето P е алгебра над P с размерност n^2. Тази алгебра се нарича *алгебра на матриците от ред n над полето P*. В $M(n, P)$ базис образуват матричните единици E_{ij} $(i, j = 1, 2, \ldots, n)$.

Множеството $A(n, P)$ на всички триъгълни матрици от ред n с нули над главния диагонал и с елементи от полето P е също алгебра над P с размерност $\frac{n(n+1)}{2}$, базис на която образуват матричните единици E_{ij}, където $1 \leqq i \leqq j \leqq n$. Тази алгебра се нарича алгебра на триъгълните матрици от ред n над полето P.

6. Ако X е произволно непразно множество, а P е поле, множеството $\mathrm{Fun}(X, P)$ на всички функции, които са дефинирани в X и приемат стойностите си в P, е алгебра над P спрямо обичайните операции събиране, умножение на функции и умножение на елемент от P с функция — ако $f, g \in \mathrm{Fun}(X, P)$ и $\lambda \in P$, то $f+g$, fg и λf се определят с равенствата

$$(f+g)(x)=f(x)+g(x),\ (fg)(x)=f(x)\,g(x),\ (\lambda f)(x)=\lambda f(x).$$

Алгебрата $\mathrm{Fun}(X, P)$ над P е крайномерна тогава и само тогава, когато X е крайно множество. В последния случай броят на елементите на X съвпада с размерността на $\mathrm{Fun}(X, P)$ над P, защото базис образуват функциите f_x $(x \in X)$, които са определени по следния начин:

$$f_x(y)=\begin{cases} 1, & \text{ако } x=y; \\ 0, & \text{ако } x \neq y. \end{cases}$$

7. Ако V е линейно пространство над полето P, множеството $\mathrm{Hom}(V, V)$ на всички линейни преобразувания на V е алгебра над P относно събирането, умножението на линейни преобразувания и умножението на линейни преобразувания с елементи от P.

Определение 3. Ако A и B са две алгебри над едно и също поле P, то изображението $\varphi: A \to B$ ще наричаме *изоморфизъм* на алгебрата A върху алгебрата B, ако φ е взаимно еднозначно изображение на A върху B и ако за всеки два елемента $a, b \in A$ и за всяко $\lambda \in P$ са изпълнени равенствата

$$\begin{cases} \varphi(a+b)=\varphi(a)+\varphi(b),\ \varphi(ab)=\varphi(a)\,\varphi(b), \\ \varphi(\lambda a)=\lambda\varphi(a). \end{cases}$$

Другояче казано, *изображението φ на A в B е изоморфизъм на алгебри, ако φ е едновременно изоморфизъм на пръстена A върху пръстена B и изоморфизъм на линейното пространство A върху линейното пространство B.*

Ако съществува изоморфизъм на алгебрата A върху алгебрата B, ще казваме, че A е изоморфна на B и ще пишем $A \cong B$.

Задача. Нека L, M и N са три алгебри над полето P. Докажете, че:

1) $L \cong L$;

2) ако $L \cong M$, то $M \cong L$;

3) ако $L \cong M$ и $M \cong N$, то $L \cong N$.

От гледна точка на алгебричната теория всеки две изоморфни линейни алгебри са еднакви или по-точно те са две копия на един и същ обект. Ясно е, че алгебричните свойства на две изоморфни алгебри ще бъдат едни и същи. Трябва изрично да подчертаем, че за изоморфизъм на две алгебри над различни полета не можем да говорим.

Пример. Нека V е n-мерно линейно пространство над полето P, а $e_1, e_2, \ldots, e_n$ е фиксиран базис на V. Тогава, както знаем от курса по линейна алгебра, на всяко линейно преобразуване φ на V, т. е. на всяко φ от алгебрата $\mathrm{Hom}(V, V)$, се съпоставя матрица $a=(a_{ij})$ от $M(n, P)$ — това е матрицата на φ в базиса $e_1, e_2, \ldots, e_n$ и тя се определя от координатите на векторите $\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n)$, като координатите на $\varphi(e_i)$ образуват i-тия стълб на a $(i=1, 2, \ldots, n)$. От курса по линейна алгебра знаем също, че посоченото изображение на $\mathrm{Hom}(V, V)$ в $M(n, P)$ има всички свойства, които се изискват в определението за изоморфизъм на алгебри. Следователно, когато $n=\dim_P V$, имаме $\mathrm{Hom}(V, V) \cong M(n, P)$ и с помощта на всеки фиксиран базис на линейното пространство V се получава по един изоморфизъм на алгебрата $\mathrm{Hom}(V, V)$ върху алгебрата $M(n, P)$ — този изоморфизъм изобразява линейното преобразуване в неговата матрица във фиксирания базис.

Нека сега A е крайномерна алгебра над полето P и $a_1, a_2, \ldots, a_n$ е базис на A. Произведенията $a_i a_j$ $(i, j=1, 2, \ldots, n)$ са линейни комбинации на базисните елементи, т. е.

$$a_i a_j = \sum_{k=1}^{n} \gamma_{ijk} a_k \quad (1 \leqq i, \ j \leqq n),$$

Коефициентите γ_{ijk}, които са n^3 на брой, се наричат *структурни константи на алгебрата* A в базиса $a_1, a_2, \ldots, a_n$. Структурните константи на A в дадения базис определят еднозначно умножението в A. Наистина ако $x, y \in A$, то

$$x=\sum_{i=1}^{n} \xi_i a_i, \quad y=\sum_{j=1}^{n} \eta_j a_j.$$

Тогава

$$xy=\sum_{i=1}^{n}\sum_{j=1}^{n} \xi_i \eta_j a_i a_j = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} \xi_i \eta_j \gamma_{ijk} a_k =$$

$$= \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \xi_i \eta_j \gamma_{ijk} \right) a_k.$$

Твърдение 3. *Две крайномерни алгебри* A *и* B *над полето* P *са изоморфни тогава и само тогава, когато те имат една и съща размерност* n *над* P *и в* A *и* B *могат да се намерят съответно такива базиси* $a_1, a_2, \ldots, a_n$ *и* $b_1, b_2, \ldots, b_n$, *че структурните константи на* A *в базиса* $a_1, a_2, \ldots, a_n$ *съвпадат със структурните константи на* B *в базиса* $b_1, b_2, \ldots, b_n$.

Доказателство. Нека $\varphi: A \to B$ е изоморфизъм на A върху B. Понеже φ е изоморфизъм на линейното пространство A върху линейното пространство B, то $\dim_P A = \dim_P B$. Нека $n = \dim_P A$ и $a_1, a_2, \ldots, a_n$ е произволен базис в A. Тогава елементите $b_1 = \varphi(a_1), \ldots, b_n = \varphi(a_n)$ образуват базис в B. Нека γ_{ijk} $(1 \leqq i, j, k \leqq n)$ са структурните константи на A в базиса $a_1, a_2, \ldots, a_n$. Тогава са изпълнени равенствата (1). За да изчислим структурните константи на B в базиса $b_1, b_2, \ldots, b_n$, трябва да изразим произведенията $b_i b_j$ като линейни комбинации на елементите от този базис. Но

$$b_i b_j = \varphi(a_i)\varphi(a_j) = \varphi(a_i a_j) = \varphi\left(\sum_{k=1}^{n} \gamma_{ijk} a_k\right)$$

$$= \sum_{k=1}^{n} \gamma_{ijk} \varphi(a_k) = \sum_{k=1}^{n} \gamma_{ijk} b_k.$$

Следователно структурните константи на алгебрата B в базиса $b_1, b_2, \ldots, b_n$ са същите, както структурните константи на A в базиса $a_1, a_2, \ldots, a_n$.

Обратно, нека $\dim_P A = \dim_P B = n$, а $a_1, a_2, \ldots, a_n$ и $b_1, b_2, \ldots, b_n$ са съответно такива базиси на A и B, че структурните константи γ_{ijk} на A в базиса $a_1, a_2, \ldots, a_n$ съвпадат със съответните структурни константи δ_{ijk} на B базиса $b_1, b_2, \ldots, b_n$, т. е. $\gamma_{ijk} = \delta_{ijk}$ $(1 \leqq i, j, k \leqq n)$. От линейната алгебра е известно, че в този случай съществува еднозначно определен изоморфизъм φ на линейното пространство A върху линейното пространство B, който удовлетворява равенствата $\varphi(a_i) = b_i$ $(i = 1, 2, \ldots, n)$. Не е трудно да се провери, като се използуват формулите (1) и равенството на съответните структурни константи, че φ е изоморфизъм на алгебрата A върху алгебрата B.

Твърдението е доказано.

Нека S е произволна едномерна алгебра над полето P с базисен елемент e_1 $(e_1 \neq 0)$. Тогава алгебрата S се определя от единствената си структурна константа γ, която се получава от равенството $e_1^2 = \gamma e_1$. Ако $\gamma = 0$, то S е изоморфна на едномерната ал-

гебра с нулево умножение над P. Ако $\gamma \neq 0$, разглеждаме елемента $e=\gamma^{-1}e_1 \neq 0$ от S. Тъй като $e^2=e$, то S в базиса си $\{e\}$ има същата структурна константа, равна на единица, както и алгебрата P над P в базиса си, съставен от единичния елемент. Според горното твърдение S е изоморфна на полето P, разглеждано като алгебра над себе си. Така получихме следното

Твърдение 4. *Всяка едномерна алгебра над полето P е изоморфна на едномерната алгебра над P с нулево умножение, или на полето P, разглеждано като алгебра над себе си, т. е. с точност до изоморфизъм над всяко поле P има само две неизоморфни едномерни алгебри.*

Задача. Докажете, че всяка n-мерна алгебра A над полето P е изоморфна на подалгебра на матричната алгебра $M(n, P)$.

Упътване. На произволен елемент $x=\alpha_1 a_1+\ldots+\alpha_n a_n (\alpha_i \in P)$ от n-мерната алгебра A с базис $a_1, a_2, \ldots, a_n$ съпоставяме матрицата X от $M(n, P)$, на която елементите от i-тия ред ($i=1, 2, \ldots, n$) са съответно равни на координатите елемента $a_i x$ в базиса $a_1, a_2, \ldots, a_n$.

Твърдение 5. *Ако A е пръстен с единица e и L е подполе на центъра $Z(A)$ на A, което съдържа единицата e на пръстена A, то A е алгебра над полето L.*

Действително ако λ е елемент от L, а a е от A, то произведението λa е определено и $\lambda a \in A$, защото L се съдържа в пръстена A. Освен това $\lambda(ab)=(\lambda a)b=a(\lambda b)$ за всяко $\lambda \in L$, $a, b \in A$, понеже $\lambda \in L \subseteq Z(A)$. Това, че A е линейно пространство над L, следва непосредствено от аксиомите за събирането и умножението, които са изпълнени в пръстена A.

Следствие 3. *Всяко тяло D е алгебра над своя център $Z(D)$.*

Твърдение 6. *Ако A е алгебра с единица e ($e \neq 0$) над полето P, подмножеството $L=\{pe \mid p \in P\}$ на A е подполе на центъра $Z(A)$ и е изоморфно на полето P.*

Доказателство. Нека 1 е единицата на полето P. Тъй като $1 \cdot e=e$, то $e \in L$. Очевидно е, че изображението $\varphi: P \to L$, определено от равенствата $\varphi(p)=pe$ ($p \in P$), е изображение на P върху L. Ще покажем, че L е подпръстен на $Z(A)$ и че φ е изоморфизъм на P върху L.

Действително нека pe е произволен елемент от L и $a \in A$. Тогава $(pe)a=p(ea)=p(ae)=a(pe)$ и следователно L е подмножество на $Z(A)$. Освен това

$$pe-p_1e=(p-p_1)e,\ (pe)(p_1e)=(pp_1)e,$$

където pe, p_1e са произволни елементи от L, т. е. L е подпръстен на $Z(A)$. От друга страна,

$$\varphi(p+p_1)=(p+p_1)e=pe+p_1e=\varphi(p)+\varphi(p_1),$$

$$\varphi(pp_1)=(pp_1)e=(pe)(p_1e)=\varphi(p)\varphi(p_1)$$

за всеки два елемента p, $p_1 \in P$. Затова φ е хомоморфизъм на полето P върху пръстена L. Ядрото $\ker\varphi$ на φ не съдържа единицата 1 на P, тъй като $\varphi(1)=1e=e\neq 0$, т. е. $\ker\varphi$ е идеал на P, който не съвпада с P. Но полето P има само два идеала — нулевия и цялото P. Следователно $\ker\varphi=(0)$ и φ е изоморфизъм на P върху L. Оттук следва, че L е също поле. Твърдението е доказано.

От предишните две твърдения следва, че когато A е алгебра с единица $e\neq 0$ над полето P, то полето P може да се отъждестви с подполето $L=\{pe|p\in P\}$ на центъра на A, т. е. можем да считаме, че P е подполе на центъра $Z(A)$ на A, което съдържа единицата e на A. Например елементите на дадено поле P могат да бъдат отъждествени със съответните скаларни матрици от $M(n, P)$ и да считаме, че $P=Z[M(n, P)]$ и $M(n, P)$ се разглежда като алгебра над своя център.

Нека A е алгебра над полето P. Ако в пръстена A няма делители на нулата, казваме, че A е алгебра без делители на нулата. Ако пръстенът A е тяло, казваме, че алгебрата A е алгебра с деление над полето P. В последния случай можем да считаме, че P е подполе на центъра на тялото A.

Твърдение 7. *Всяка ненулева крайномерна алгебра A над полето P, в която няма делители на нулата, е алгебра с деление.*

Доказателство. Нека $a_1, a_2, \ldots, a_n$ е произволен базис на алгебрата A над полето P. Трябва да докажем, че A е тяло. Ако a е ненулев елемент от A, системата елементи $aa_1, aa_2, \ldots, aa_n$ е линейно независима. Наистина ако

$$\lambda_1(aa_1)+\lambda_2(aa_2)+\ldots+\lambda_n(aa_n)=0$$

за някои $\lambda_i \in P$, то

$$a(\lambda_1 a_1+\lambda_2 a_2+\ldots+\lambda_n a_n)=0.$$

Тъй като $a\neq 0$ и в A няма делители на нулата, то

$$\lambda_1 a_1+\lambda_2 a_2+\ldots+\lambda_n a_n=0.$$

Но $a_1, a_2, \ldots, a_n$ са линейно независими над P и затова $\lambda_1=\lambda_2=\ldots=\lambda_n=0$. Понеже $n=\dim_P A$ и системата $aa_1, aa_2, \ldots, aa_n$ е линейно независима, то тя ще бъде базис на A над P. Тогава всеки елемент $b\in A$ ще се представя във вида

$$b=\sum_{i=1}^{n}\mu_i(aa_i)=a\left(\sum_{i=1}^{n}\mu_i a_i\right)$$

за някои $\mu_1, \mu_2, \ldots, \mu_n$ от P. Следователно уравнението $ax=b$ при $a\neq 0$ има решение в A. Ако $ax_1=b$ и $ax_2=b$ ($x_1, x_2\in A$), то $a(x_1-x_2)=0$. Понеже в A няма делители на нулата и $a\neq 0$, от последното равенство следва равенството $x_1=x_2$, т. е. уравнението $ax=b$ за всяко b и за всяко ненулево a от A има едно-един-

ственo решение в A. Съвършено аналогично се доказва, че уравнението $ya=b$ ($a, b \in A, a \neq 0$) също има едно-единствено решение в A. Следователно пръстенът A е тяло и алгебрата A над P е алгебра с деление. Твърдението е доказано.

Забележка. Доказателството на горното твърдение след очевидна модификация дава решение на последната задача от § 1.

Ако A е алгебра над полето P, то непразното подмножество M в A се нарича *подалгебра* на A, ако M е алгебра спрямо операциите в A, т. е. за всеки два елемента x и y от M и за всяко λ от P, елементите $x+y$, xy и λx са също от M.

Очевидно е, че непразното подмножество M на A е подалгебра на A тогава и само тогава, когато M е подпръстен на пръстена A и подпространство на пространството A.

Примери

1. Алгебрата $A(n, P)$ от триъгълните матрици с нули над главния диагонал е $\frac{n(n+1)}{2}$-мерна подалгебра на алгебрата $M(n, P)$ на матриците от n-ти ред над полето P.

2. Подмножеството $\{0\}$ от нулевия елемент на алгебрата A е подалгебра на A, наречена нулева подалгебра.

3. Центърът $Z(A)$ на всяка алгебра A над поле P е подалгебра на A. В частност скаларните матрици от $M(n, P)$ образуват едномерна подалгебра на $M(n, P)$, която е изоморфна на P, разглеждано като алгебра над себе си.

4. Тялото K на кватернионите е подпръстен на алгебрата $M(2, \mathbf{C})$ над полето $\mathbf{C}$ на комплексните числа, но не е нейна подалгебра. Обаче пръстенът $M(2, \mathbf{C})$ може да се разглежда като алгебра над полето $\mathbf{R}$ на реалните числа и тялото на кватернионите K е подалгебра на реалната алгебра $M(2, \mathbf{C})$. Наистина ако $\alpha \in \mathbf{R}$, т. е. $\alpha = \bar{\alpha}$ и

$$a = \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix}$$

е произволна матрица от K, то

$$\alpha a = \alpha \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix} = \begin{pmatrix} \alpha z & \alpha t \\ -\alpha\bar{t} & \alpha\bar{z} \end{pmatrix} = \begin{pmatrix} \alpha z & \alpha t \\ -\alpha\bar{t} & \alpha\bar{z} \end{pmatrix}$$

е също матрица от K. Ще покажем, че K е четиримерна реална алгебра и неин базис образуват матриците

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$E_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Действително ако $z = a+bi$ и $t = c+di$ са две произволни комплексни числа, то

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} = \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix} = aE_1 + bE_2 + cE_3 + dE_4.$$

където $a, b, c, d \in \mathbf{R}$. Получихме, че всеки елемент от K се записва като линейна комбинация на E_1, E_2, E_3 и E_4 с реални коефициенти. Ако $\alpha, \beta, \gamma, \delta \in \mathbf{R}$, равенството

$$\alpha E_1 + \beta E_2 + \gamma E_3 + \delta E_4 = 0$$

е еквивалентно на равенството

$$\begin{pmatrix} \alpha+\beta i & \gamma+\delta i \\ -\gamma+\delta i & \alpha-\beta i \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

и затова $\alpha=\beta=\gamma=\delta=0$, т. е. матриците E_1, E_2, E_3 и E_4 са линейно независими над полето $\mathbf{R}$ на реалните числа. С това доказахме, че E_1, E_2, E_3, E_4 образуват базис на алгебрата K над полето $\mathbf{R}$, поради което $\dim_R K = 4$. Лесно се проверява, че са изпълнени равенствата

$$\begin{aligned} &E_1 E_k = E_k E_1 = E_k \quad (k=1, 2, 3, 4), \\ &E_2^2 = E_3^2 = E_4^2 = -E_1, \\ &E_2 E_3 = -E_3 E_2 = E_4, \quad E_2 E_4 = -E_4 E_2 = -E_3, \\ &E_3 E_4 = -E_4 E_3 = E_2. \end{aligned} \tag{2}$$

Удобно е последните равенства от (2) да се запишат във вид на следната таблица, в която на (r, k)-то място се посочва на какво е равно произведението $E_r E_k$ $(r, k=2, 3, 4)$:

	E_2	E_3	E_4
E_2	$-E_1$	E_4	$-E_3$
E_3	$-E_4$	$-E_1$	E_2
E_4	E_3	$-E_2$	$-E_1$

(3)

Ако отъждествим елементите на полето $\mathbf{R}$ на реалните числа със съответните скаларни матрици от K и за матриците E_1, E_2, E_3 и E_4 въведем съответно означенията 1, i, j и k, то получаваме, че тялото на кватернионите K има базис 1, i, j, k като алгебра над $\mathbf{R}$. Всеки елемент a от K се записва еднозначно във вида

$$a = \alpha + \beta i + \gamma j + \delta k, \tag{4}$$

където $\alpha, \beta, \gamma, \delta \in \mathbf{R}$, а базисните елементи 1, i, j, k се умножават така, както е посочено в таблица (3). В новите означения тя приема вида

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

(5)

като се има предвид, че 1 е единичният елемент на K.

Елементите на тялото K на кватернионите, записани във вида (4), се наричат кватерниони. С това показахме, че тялото на кватернионите е четиримерна реална алгебра с деление.

Задача. Ако a е кватернион от вида (4), кватернионът $\bar{a}=\alpha-\beta i-\gamma j-\delta k$ се нарича спрегнат на a. Докажете, че:

1) $N(a)=a\bar{a}=\alpha^2+\beta^2+\gamma^2+\delta^2$ и при $a\neq 0$ обратният елемент на a е $a^{-1}=\frac{1}{N(a)}\bar{a}$;

2) $N(ab)=N(a)N(b)$ за всяко a и b от K.

Задача. Докажете, че пръстенът $M(2, \mathbf{C})$ е осеммерна алгебра над полето $\mathbf{R}$ на реалните числа.

Задача. Докажете, че една едномерна алгебра B над полето P има само две подалгебри — цялата алгебра B и нулевата подалгебра.

Всяка подалгебра M на алгебрата A, която не съвпада с A, се нарича собствена подалгебра. Очевидно е, че само нулевата алгебра няма собствени подалгебри. Обаче, както следва от предната задача, едномерните алгебри имат една-единствена собствена подалгебра, а именно нулевата подалгебра.

Подалгебрата N на алгебрата A се нарича *идеал* на A, ако за всеки елемент x от N и за всяко a от A двете произведения ax и xa са елементи от N. Например нулевата подалгебра и цялата алгебра A са идеали на A. Подалгебрата $A(n, P)$ от триъгълните матрици не е идеал на алгебрата $M(n, P)$ на матриците от ред n над полето P.

Всяка алгебра A, която не е с нулево умножение и която няма ненулеви собствени идеали, се нарича *проста алгебра*. Например ако L е разширение на полето P, то L е проста комутативна алгебра над P. Всяко тяло D е проста алгебра над центъра си $Z(D)$ или над което да е подполе на центъра $Z(D)$.

Твърдение 8. *За всяко поле P и за всяко естествено число n матричната алгебра $M(n, P)$ е проста.*

Доказателство. Нека N е произволен ненулев идеал на $M(n, P)$. Ще покажем, че N съвпада с $M(n, P)$, т. е. N не е собствен идеал. Достатъчно е да покажем, че всяка матрична единица E_{kr} се съдържа в N, тъй като матричните единици образуват базис на алгебрата $M(n, P)$ над P. Тъй като $N\neq(0)$, то съществува ненулева матрица $x=(x_{ij})$, която се съдържа в N. Тогава поне един от елементите x_{ij} на x, например x_{st}, е ненулев. Нека k и r са произволно избрани числа измежду числата $1, 2, \ldots, n$. Ще покажем, че произведението $(x_{st}^{-1}E_{ks})xE_{tr}$ съвпада с E_{kr}. Наистина

$$x=\sum_{j=1}^{n}\sum^{n} x_{ij}E_{ij}.$$

Затова

$$(x_{st}^{-1}E_{ks})xE_{tr}=x_{st}^{-1}E_{ks}\left(\sum_{i=1}^{n}x_{it}E_{ir}\right)=x_{st}^{-1}(x_{st}E_{kr})=E_{kr}.$$

Понеже N е идеал на $M(n, P)$ и $x \in N$, то

$$E_{kr} = (x_{sl}^{-1} E_{ks})\, x E_{tr} \in N \quad (k, r = 1, 2, \ldots, n).$$

Следователно $N = M(n, P)$, с което твърдението е доказано.

Определение 4. Ако A и B са две алгебри над едно и също поле P, изображението $\varphi: A \to B$ се нарича *хомоморфизъм* на алгебрата A в алгебрата B, ако за всеки два елемента a и b от A и за всяко λ от P са изпълнени равенствата

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\,\varphi(b),$$

$$\varphi(\lambda a) = \lambda \varphi(a).$$

Ако φ е хомоморфизъм на алгебрата A в алгебрата B над полето P, множеството от всички елементи от A, които φ изобразява в нулевия елемент на B, се нарича ядро на хомоморфизма φ и се бележи с $\ker \varphi$, т. е.

$$\ker \varphi = \{a \mid a \in A,\ \varphi(a) = 0\}.$$

Множеството от всички елементи x от B, които имат първообраз в A при хомоморфизма φ, се означава с $\operatorname{Im} \varphi$ или с $\varphi(A)$ и се нарича образ на хомоморфизма φ, т. е. $\operatorname{Im} \varphi = \{\varphi(a) \mid a \in A\}$.

Задача. Докажете, че ако φ е хомоморфизъм на алгебрата A в алгебрата B, то $\ker \varphi$ е идеал на A, а $\operatorname{Im} \varphi$ е подалгебра на B.

Ще казваме, че хомоморфизмът φ на A в B е хоморфизъм на алгебрата A върху алгебрата B, ако $\operatorname{Im} \varphi = B$, т. е. ако за всеки елемент x от B съществува такъв елемент a от A, че $\varphi(a) = x$.

Очевидно е, че изоморфизъм φ на алгебрата A върху алгебрата B е хомоморфизъм на A върху B, ядрото на който съвпада с нулевия идеал на A, т. е. понятието изоморфизъм е частен случай на понятието хомоморфизъм.

Нека N е произволен идеал на алгебрата A над полето P. Тъй като A е модул (линейно пространство) над P спрямо операцията събиране на елементи от A и умножението им с елементи от P, а N е подмодул на A, можем да образуваме фактор модула (фактор-пространството) A/N. Нека $\eta: A \to A/N$ е естественият хомоморфизъм на линейното пространство A върху линейното пространство A/N. Във фактор-пространство A/N обаче можем да въведем операция умножение: ако $x+N$ и $y+N$ са два съседни класа на A по N, т. е. $x+N$ и $y+N$ са два елемента от A/N, то по определение полагаме

$$(x+N)(y+N) = xy+N.$$

Тъй като N е идеал на пръстена A, операцията умножение е коректно определена (виж например § 4 на глава V). Лесно се проверява, че пространството A/N с въведената операция умножение се превръща в алгебра над полето P, а η се оказва хомоморфизъм на алгебрата A върху алгебрата A/N. Така построената алгебра A/N се нарича *фактор-алгебра* на A по нейния идеал N,

а η — естествен хомоморфизъм на A върху нейната фактор-алгебра A/N.

Задача. Докажете, че $\ker\eta=N$ и η е изоморфизъм на A върху A/N тогава и само тогава, когато N е нулевият идеал на A.

Ако съществува хомоморфизъм на алгебрата A върху алгебрата B, казваме, че B е хомоморфен образ на алгебрата A. Например всяка фактор-алгебра A/N на A е нейн хомоморфен образ и това го установихме с естествения хомоморфизъм на A върху A/N.

За алгебри е в сила също съответната теорема за хомоморфизмите.

Теорема 1. *Нека $\varphi: A\to B$ е произволен хомоморфизъм на алгебрата A върху алгебрата B и $N=\ker\varphi$ е ядрото на φ. Ако $\eta: A\to A/N$ е естественият хомоморфизъм на A върху нейната фактор-алгебра A/N, то съществува такъв изоморфизъм τ на фактор-алгебрата A/N върху алгебрата B, че последователното прилагане на хомоморфизма η и изоморфизма τ съвпада с хомоморфизма φ, т. е. $\varphi=\tau\eta$.*

Действително от теоремата за модулите над комутативни пръстени знаем, че изображението $\tau: A/N\to B$, което се определя с равенството $\tau(x+N)=\varphi(x)$ за всеки елемент $x+N$ от A/N, е изоморфизъм на линейното пространство A/N върху B и че $\varphi=\tau\eta$. Остава само да се провери, че τ изобразява произведение на елементи от A/N в произведение на техните образи, т. е. че τ е изоморфизъм на алгебри. Нека $x+N$ и $y+N$ са два елемента от A/N. Тогава

$$\tau[(x+N)(y+N)]=\tau(xy+N)=\varphi(xy)=\varphi(x)\varphi(y)=$$
$$=\tau(x+N)\tau(y+N)$$

и затова τ е изоморфизъм на алгебрата A/N върху алгебрата B. Теоремата е доказана.

§ 3. Теорема на Фробениус

В този параграф ще докажем забележителния факт, че полето $\mathbf{R}$ на реалните числа, полето $\mathbf{C}$ на комплексните числа и телото $\mathbf{K}$ на кватернионите с точност до изоморфизъм са единствените асоциативни крайномерни алгебри над полето $\mathbf{R}$ без делители на нулата.

Лема 1. *Нека D е произволно тяло, S е комутативен подпръстен на D и a е такъв елемент на D, че за всяко s от S е изпълнено равенството $as=sa$. Тогава D притежава такъв комутативен подпръстен T, който едновременно съдържа a и S.*

Действително нека T е множеството от всички елементи на D, които могат да се запишат като полиноми на a с коефициенти от S. Ако

$$t=s_0+s_1a+s_2a^2+\ldots+s_ma^m\ (s_i\in S),$$

$$t' = s_0' + s_1' a + s_2' a^2 + \ldots + s_n' a^m \ (s_i' \in S)$$

са два произволни елемента от T, очевидно е, че $t - t'$ и tt' са също елементи от T. Освен това $tt' = t't$. Следователно T е комутативен подпръстен на D, който съдържа a и S.

Лема 2. *Всеки комутативен подпръстен S на тялото D се съдържа в подполе на D.*

Доказателство. Ако S е нулевият подпръстен на D съгласно следствие 1 центърът $Z(D)$ е подполе на D, което съдържа S.

Нека S е ненулев подпръстен на D. Ще покажем, че в този случай полето от частни на S се съдържа в D. Наистина нека $0 \neq s \in S$ и s^{-1} е обратният на s в тялото D. Тъй като равенството $ss_1 = s_1 s$ е изпълнено за всяко $s_1 \in S$, чрез умножаване на това равенство отляво и отдясно с s^{-1} получаваме, че $s_1 s^{-1} = s^{-1} s_1$, т. е. s^{-1} комутира с всички елементи от S. Ако и елементът s_1 е ненулев, от равенството $ss_1 = s_1 s$ следва, че $s^{-1} s_1^{-1} = (s_1 s)^{-1} = (ss_1)^{-1} = s_1^{-1} s^{-1}$, т. е. обратните на елементите от S също комутират помежду си. Нека сега L е множеството от всички елементи от вида $s_1 s_2^{-1}$, където s_1 пробягва всички елементи от S, а s_2 пробягва всички ненулеви елементи от S. Понеже $S \neq (0)$, то L е непразно подмножество на D. От предните разглеждания следва, че елементите на L комутират помежду си. Лесно се проверява, че L е подполе на D, което съдържа подпръстена S.

Наистина ако $a = s_1 s_2^{-1}$ и $b = s_3 s_4^{-1}$ са два произволни елемента от L, то

$$a \pm b = (s_1 s_4 \pm s_2 s_3)(s_2 s_4)^{-1}, \ ab = (s_1 s_3)(s_2 s_4)^{-1}$$

са също елементи от L. Следователно L е комутативен подпръстен на D. Освен това ако $s_1 s_2^{-1}$ е ненулев елемент от L, то $s_1 \neq 0$ и обратният $(s_1 s_2^{-1})^{-1} = s_2 s_1^{-1}$ е също от L, т. е. L е подполе на D. Ако s_0 е фиксиран ненулев елемент от S, то всяко $s \in S$ се представя във вида $s = (ss_0) s_0^{-1}$ и затова $S \subseteq L$. Лемата е доказана.

Следствие 4. *Ако S е подполе на центъра на тялото D и a е произволен елемент от D, то D притежава такова подполе L, което едновременно съдържа S и a.*

Наистина за подпръстена S и елемента a са изпълнени условията на лема 1. Следователно S и a се съдържат в комутативен подпръстен T на тялото D. Но съгласно лема 2 подпръстенът T се съдържа в подполе L на тялото D, поради което S и a са в подполето L.

Ще напомним, че алгебрически затворено поле се нарича такова поле, което съвпада с всяко свое алгебрично разширение (виж глава VIII, § 10). Следващата теорема дава пълна характеризация на крайномерните алгебри с деление над алгебрически затворените полета.

Теорема 2. *Нека A е произволна ненулева алгебра без делители на нулата, която е крайномерна над алгебрически затвореното поле F. Тогава A е едномерна алгебра над F и A е изоморфна на полето F, разглеждано като алгебра над себе си.*

Доказателство. От твърдение 7 следва, че A е алгебра с деление над F. В частност в A съществува единица e ($e\neq 0$). Както видяхме в предишния параграф, всеки елемент λ от F можем да отъждествим със съответния елемент λe от A и да считаме, че F е подполе на центъра на A. Единицата 1 на F се отъждествява с единицата $1e=e$ на A и затова с 1 ще означаваме по-нататък единицата на A. За да докажем теоремата след посоченото отъждествяване, трябва да установим, че A съвпада с подполето F. Нека a е произволен елемент от A. Тъй като $F\subseteq Z(A)$ според лема 2 F и a се съдържат в подполе L на алгебрата A. Нека $n=\dim_F A$. Тогава елементите $1, a, a^2, \ldots, a^n$ са $n+1$ на брой и затова образуват линейно зависима система над F. Следователно елементът a е алгебричен над полето F. Тъй като F е алгебрически затворено поле и простото алгебрично разширение $F(a)$ е алгебрично разширение на F, то $F(a)=F$. Но a се съдържа в $F(a)$ и затова $a\in F$. С това показахме, че $A=F$. Теоремата е доказана.

Следствие 5. *Полето* **C** *на комплексните числа е единствената (с точност до изоморфизъм) крайномерна комплексна алгебра с деление.*

Да насочим сега своето внимание към крайномерните реални алгебри с деление, т. е. към крайномерните алгебри без делители на нулата над полето **R** на реалните числа. Три такива алгебри вече познаваме — полето **R**, полето **C** на комплексните числа и тялото K на кватернионните (виж предишния параграф). Тези реални алгебри са с размерност съответно 1, 2 и 4 над **R**. Оказва се, че всяка друга реална крайномерна асоциативна алгебра с деление е изоморфна на една от посочените три алгебри. Този важен факт е доказан от Фробениус и е известен като теорема на Фробениус.

Теорема 3 (теорема на Фробениус). *Полето* **R** *на реалните числа и полето* **C** *на комплексните числа са единствените (с точност до изоморфизъм) ненулеви крайномерни реални асоциативни и комутативни алгебри без делители на нулата.*

Тялото K на кватернионите е единствената крайномерна реална асоциативна, но некомутативна алгебра без делители на нулата.

Доказателство. Нека A е произволна крайномерна реална алгебра без делители на нулата и нека $n=\dim_R A$. Според твърдение 7 A е алгебра с деление. Ако e ($e\neq 0$) е единичният елемент на A, то e е единственият ненулев елемент на A, за който $e^2=e$. Наистина ако $d^2=d$, $0\neq d\in A$, то $d(d-e)=0$ и понеже в A няма делители на нулата, от последното равенство следва

$d=e$. Ако отъждествим единичния елемент e на A с числото 1, можем да считаме, че $\mathbf{R}$ е подполе на центъра $Z(A)$ на алгебрата A.

Нека $n=\dim_{\mathbf{R}} A=1$. Понеже $\mathbf{R}\subseteq A$ и $\dim_{\mathbf{R}}\mathbf{R}=1$, то в този случай $A=\mathbf{R}$. По-нататък ще предполагаме, че $n>1$. Доказателството ще проведем на няколко етапа.

1. Ако a е произволен елемент от A, който не се съдържа в $\mathbf{R}$, то $\mathbf{R}$ и a се съдържат в подполе на A, което е изоморфно на полето $\mathbf{C}$ на комплексните числа.

Наистина, тъй като $\mathbf{R}\subseteq Z(A)$, то според следствие 4 $\mathbf{R}$ и a се съдържат в някое подполе L на A. Понеже $n=\dim_{\mathbf{R}} A$, системата от $n+1$ елемента $1, a, a^2, \ldots, a^n$ е линейно зависима над $\mathbf{R}$. Затова a е алгебричен елемент над $\mathbf{R}$. Да разгледаме простото алгебрично разширение $\mathbf{R}(a)$, което се съдържа в L. Понеже $a\in\mathbf{R}(a)$ и $a\notin\mathbf{R}$, степента $[\mathbf{R}(a):\mathbf{R}]$ е по-голяма от единица. Нека $f(x)$ е минималният полином на a над $\mathbf{R}$. Понеже $f(x)$ е неразложим над $\mathbf{R}$, а неразложими над $\mathbf{R}$ са само полиномите от първа степен и полиномите от втора степен без реални корени, а $a\notin\mathbf{R}$, то

$$f(x)=x^2+\alpha x+\beta,$$

където $\alpha, \beta\in\mathbf{R}$ и $\alpha^2-4\beta<0$. Двата корена на $f(x)$ са $x_1=a$ и $x_2=-a-\alpha$ и се съдържат в $\mathbf{R}(a)$. Очевидно е, че $\mathbf{R}(a)$ е поле на разлагане на $f(x)$ над $\mathbf{R}$. Но полето $\mathbf{C}$ е също поле на разлагане на полинома $f(x)$. От следствие 8 на глава VIII следва, че двете полета $\mathbf{R}(a)$ и $\mathbf{C}$ са изоморфни над полето $\mathbf{R}$, т. е. те са изоморфни като алгебри над $\mathbf{R}$. Затова в $\mathbf{R}(a)$ има такъв елемент i, за който $i^2=-1$. Ясно е сега, че 1 и i образуват базис на $\mathbf{R}(a)$ като алгебра над $\mathbf{R}$. Елементите 1 и a също образуват базис на $\mathbf{R}(a)$.

От доказаното дотук следва, че ако $n=\dim_{\mathbf{R}} A=2$, то $A=\mathbf{R}(a)$, $a\notin\mathbf{R}$ и A е изоморфна на полето $\mathbf{C}$ като алгебра над $\mathbf{R}$. По-нататък ще предполагаме, че $n=\dim_{\mathbf{R}} A>2$.

2. Нека 1, a и b са линейно независими над $\mathbf{R}$ елементи на A. Ще докажем, че тогава 1, a и b се съдържат в четиримерна подалгебра L на A, изоморфна на тялото на кватернионите.

Действително по първата част на доказателството подполетата $\mathbf{R}(a)$ и $\mathbf{R}(b)$ са двумерни алгебри над $\mathbf{R}$, изоморфни на полето $\mathbf{C}$ на комплексните числа. Понеже елементите 1 и a образуват базис на $\mathbf{R}(a)$, а елементите 1, a и b са линейно независими, то b не се съдържа в $\mathbf{R}(a)$. В $\mathbf{R}(a)$ има такъв елемент i, че $i^2=-1$, а $\mathbf{R}(b)$ притежава елемент j_0, за който $j_0^2=-1$. Очевидно е, че $\mathbf{R}(a)=\mathbf{R}(i)$ и $\mathbf{R}(b)=\mathbf{R}(j_0)$. Затова системата 1, i, j_0 е линейно независима над $\mathbf{R}$. Но тогава $i+j_0$ и $i-j_0$ не се съдържат в полето $\mathbf{R}$. От първата част на доказателството следва, че минималните полиноми $\varphi(x)$ и $\psi(x)$ над $\mathbf{R}$ съответно на $i+j_0$ и $i-j_0$ са от втора степен и имат вида

$$\varphi(x)=x^2+\alpha x+\beta\ (\alpha, \beta\in\mathbf{R}),$$

$$\psi(x)=x^2+\gamma x+\delta \quad (\gamma,\ \delta\in \mathbf{R}).$$

Понеже $\varphi(i+j_0)=0$ и $\psi(i-j_0)=0$, то

(1) $$(i+j_0)^2=-2+(ij_0+j_0i)=-\alpha(i+j_0)-\beta,$$

$$(i-j_0)^2=-2-(ij_0+j_0i)=-\gamma(i-j_0)-\delta.$$

Като съберем последните две равенства, получаваме

$$-4=-(\alpha+\gamma)i-(\alpha-\gamma)j_0-(\beta+\delta).$$

Оттук, като вземем предвид линейната независимост на 1, i и j_0, заключаваме, че $\alpha+\gamma=\alpha-\gamma=0$ и $\beta+\delta=4$. Но тогава $\alpha=\gamma=0$ и от (1) се получава, че елементът $ij_0+j_0i=2-\beta=-2+\delta$ е реално число. Нека $2\mu=ij_0+j_0i=2-\beta=\delta-2$. Тъй като $\varphi(x)=x^2+\beta$ и $\psi(x)=x^2+\delta$ са неразложими над R, то $\delta>0$ и $\beta>0$, т. е. $2\mu=2-\beta<2$ и $2\mu=\delta-2>-2$. Затова реалното число μ удовлетворява неравенствата $-1<\mu<1$. Следователно

$$r=\frac{1}{\sqrt{1-\mu^2}}$$

ще бъде реално число, различно от 0.

Да означим с j елемента $\mu ri+rj_0$ на алгебрата A. Тогава

$$j^2=-\mu^2r^2-r^2+\mu r^2(ij_0+j_0i)=$$

$$=-\mu^2r^2-r^2+2\mu^2r^2=-r^2+\mu^2r^2=\frac{\mu^2-1}{1-\mu^2}=-1.$$

Очевидно от линейната независимост на 1, i и j_0 следва, че 1, i и j са линейно независими над R. Да означим с k произведението ij. Лесно се проверява, че $ij+ji=0$, т. е. $k=ij=-ji$. Да допуснем, че системата елементи

(2) $$1,\ i,\ j,\ k$$

е линейно зависима над R. Понеже 1, i, j е линейно независима, от допускането следва, че k е линейна комбинация на 1, i и j с коефициенти от R, т. е.

(3) $$k=\alpha_0+\alpha_1i+\alpha_2j \quad (\alpha_l\in \mathbf{R}).$$

Понеже $k=ij$, то $kj=-i$. Като умножим равенството (3) отдясно с j, получаваме

$$-i=\alpha_0j+\alpha_1k-\alpha_2=\alpha_0j+\alpha_1(\alpha_0+\alpha_1i+\alpha_2j)-\alpha_2$$

и следователно изпълнено е равенството

(4) $$(\alpha_0\alpha_1-\alpha_2)+(\alpha_1^2+1)i+(\alpha_0+\alpha_1\alpha_2)j=0.$$

От линейната независимост на 1, i и j следва, че коефициентите им в равенството (4) са равни на нула. В частност $\alpha_1^2=-1$, което е невъзможно, тъй като α_1 е реално число.

Следователно елементите 1, i, j, k са линейно независими над R. Нека L е четиримерното подпространство на A с базис 1, i, j, k. Вече не е трудно да се установи, че i, j и k се умно-

жават така, както е посочено в таблица (5) от § 2. Например

$$k^2=(ij)^2=ijij=-i^2j^2=-1,$$

$$jk=jij=-ijj=i=-kj.$$

По тази начин подпространството L е затворено относно умножението, т. е. L е подалгебра на A. От твърдение 3 следва, че L е реална алгебра, изоморфна на тялото K на кватернионите, тъй като L и K имат такива базиси, че съответните структурни константи на L и K съвпадат. Елементът a е линейна комбинация на 1 и i с коефициенти от R, а елементът b е линейна комбинация на 1 и j_0 над R. Тъй като $j_0=r^{-1}j-\mu i\in L$ и 1, $i\in L$, то 1, a и b се съдържат в L.

Получихме, че ако $n=\dim_R A>2$, то $n\geqq 4$ и ако $n=4$, то $A=L$ и затова A е изоморфна на тялото на кватернионите.

3. Да допуснем сега, че $n>4$. Нека L е четиримерна подалгебра на A, която е изоморфна на тялото K на кватернионите. В L има базис 1, i, j, k, елементите на който се умножават, както съответните кватерниони в K (виж таблица (5) от § 2). Тъй като размерността n на A е по-голяма от 4, то съществува елемент c от A, който не се съдържа в L. Тогава по първата част на доказателството простото алгебрично разширение $R(c)$ е подалгебра на A, изоморфна на полето C, и затова $R(c)=R(e)$, където $e^2=-1$. Ясно е, че e не се съдържа в L. Като повторим съответните разсъждения от втората част на доказателството, ще получим че съществуват такива реални числа α, β и γ, че

$$ie+ei=\alpha,\ je+ej=\beta,\ ke+ek=\gamma.$$

Но $k=ij$ и затова

$$ek=eij=(\alpha-ie)j=\alpha j-i(ej)=$$

$$=\alpha j-i(\beta-je)=\alpha j-\beta i+ke=\alpha j-\beta i+\gamma-ek,$$

т. е. $2ek=\alpha j-\beta i+\gamma$. Като умножим последното равенство отдясно с k, получаваме $-2e=\alpha i+\beta j+\gamma k$. Това обаче означава, че e е елемент от L, което е невъзможно. Полученото противоречие показва, че A не може да има размерност, по-голяма от 4. Теоремата е доказана.

§ 4. Теорема на Ведербърн за крайните тела

В предишния параграф дадохме пълна характеризация на крайномерните алгебри с деление над произволно алгебрически затворено поле и над полето R на реалните числа. В този параграф ще изучим крайномерните алгебри с деление над крайно поле.

Нека F е крайно поле, а $q=|F|$ е броят на елементите в F. Ако A е произволна крайномерна алгебра над F и $\dim_F A=m$, то A има краен брой елементи, който е равен на q^m, защото A има

точно толкова различни елемента, колкото са наредените m-торки от елементи на F — координатите на елементите на A в един фиксиран базис. В частност ако A е крайномерна алгебра с деление над F, то A е крайно тяло. Обратно, ако D е едно крайно тяло, неговият център $Z(D)$ е крайно поле и D е крайномерна алгебра с деление над $Z(D)$ и над всяко подполе на $Z(D)$ (следствие 1, твърдение 5, следствие 3). Следователно възниква най-напред задачата да се изучават всички крайни тела. Ясно е, че всяко крайно поле е пример на крайно комутативно тяло. Ще докажем, че крайни некомутативни тела не съществуват. За целта най-напред ще припомним някои теоретико-групови факти и ще докажем някои помощни твърдения.

Нека G е произволна (мултипликативно записана) крайна група, а g е един елемент от G. Броят на различните елементи от G, които са спрегнати с g, дели реда на групата G (виж глав. IV). Да означим с $T_1, T_2, \ldots, T_k$ всички различни класове от спрегнати елементи в G, които съдържат повече от един елемент. Нека $c_i (c_i > 1)$ е броят на елементите на $T_i (i = 1, 2, \ldots, k)$. Понеже T_i съвпада с множеството от спрегнатите на кой да е елемент от T_i, то числото c_i дели реда на групата G. В § 9 на глава IV доказахме формулата

$$1) \qquad |G| = |C(G)| + c_1 + c_2 + \ldots + c_k,$$

където $|C(G)|$ е редът на центъра на G, а $c_i = |T_i| > 1$ е броят на елементите в T_i.

В § 8 на глава II доказахме, че циклотомичните полиноми $\Phi_n(x)$ $(n = 1, 2, \ldots)$ са полиноми с цели коефициенти. От този факт следва, че за всяко цяло число q и за всяко n стойността $\Phi_n(q)$ е цяло число.

Лема 3. *Нека n е цяло число, по-голямо от 1, а d е делител на n и $1 \leqq d < n$. Тогава за всяко естествено число $q > 1$ числото*

$$\frac{q^n - 1}{q^d - 1}$$

е цяло, а стойността $\Phi_n(q)$ за $x = q$ на n-тия циклотомичен полином $\Phi_n(x)$ е цяло число, което дели числата $q^n - 1$ и $\frac{q^n - 1}{q^d - 1}$, но не дели числото $q - 1$.

Доказателство. Тъй като циклотомичните полиноми са с цели коефициенти и

$$x^n - 1 = \prod_s \Phi_s(x),$$

където s пробягва всички положителни делители на числото n, то

$$x^n - 1 = \Phi_n(x)\ (x^d - 1) f(x)$$

и полиномът

$$f(x)=\prod_{r}' \Phi_r(x)$$

е с цели коефициенти. Затова $f(q)$ е цяло число и

$$q^n-1=\Phi_n(q)\ (q^d-1)\ f(q)$$

е разлагане на q^n-1 в произведение на цели числа, т. е. $\Phi_n(q)$ дели числата q^n-1 и $\frac{q^n-1}{d}$. Остава да покажем, че $\Phi_n(q)$ не дели числото $q-1$.

От определението на $\Phi_n(x)$ следва, че

$$\Phi_n(q)=\prod_{\varepsilon} (q-\varepsilon), \tag{2}$$

където ε пробягва всичките $\varphi(n)$ на брой примитивни n-ти корени на числото 1. Понеже $n>1$, то всяко ε от (2) е различно от 1. Модулът $|q-\varepsilon|$ на множителя $q-\varepsilon$ от (2) е равен на разстоянието от точката ε, която е върху единичната окръжност, до точката q, $q\geqq 2$. Затова $|q-\varepsilon|>q-1\geqq 1$ за всеки примитивен n-ти ($n>1$) корен ε на единицата и

$$|\Phi_n(q)|=\prod_{\varepsilon} |q-\varepsilon|>(q-1)^{\varphi(n)}\geqq q-1. \tag{3}$$

От полученото строго неравенство $|\Phi_n(q)|>q-1$ следва, че цялото число $\Phi_n(q)$ не може да бъде делител на числото $q-1$. Лемата е доказана.

Нека D е крайно тяло. Да означим с F центъра $Z(D)$ на тялото D. От резултати, изложени в § 1 и § 2, следва, че F е поле, а D е алгебра над F. Нека $n=\dim_F D$. Ако N е едно подтяло на D, което съдържа центъра F на D, то N е подалгебра на D над F.

Лема 4. *Размерността $d=\dim_F N$ на подтялото N над центъра F на крайното тяло D дели размерността n на D над F.*

Доказателство. Ще казваме, че системата елементи $d_1, d_2, \ldots, d_s$ от D е линейно зависима (отляво) над подтялото N, ако съществуват такива елементи $\beta_1, \beta_2, \ldots, \beta_s$ от N, поне един от които е различен от нула, че да е изпълнено равенството

$$\beta_1 d_1+\beta_2 d_2+\ldots+\beta_s d_s=0.$$

В противен случай системата $d_1, d_2, \ldots, d_s$ се нарича линейно независима (отляво) над N. Очевидно е, че всеки ненулев елемент d от D образува линейно независима система над N. Да разгледаме всички линейно независими системи от елементи на D над N. Понеже D е крайно тяло, тези системи са краен брой и поне една от тях, например $u_1, u_2, \ldots, u_r$, ще бъде с възможно най-голям брой

елементи. Ако $x \in D$, то системата $x, u_1, u_2, \ldots, u_r$ има $r+1$ елемента и следователно тя ще бъде линейно зависима (отляво) над N. Тогава ще съществуват такива елементи $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_r$ в N, поне един от които е ненулев, че

$$\alpha x + \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_r u_r = 0.$$

Ако допуснем, че $\alpha = 0$, получаваме, че системата $u_1, u_2, \ldots, u_r$ е линейно зависима над N, което противоречи на избора ѝ. Следователно $\alpha \neq 0$ и

$$x = \sigma_1 u_1 + \sigma_2 u_2 + \ldots + \sigma_r u_r, \tag{4}$$

където $\sigma_j = -\alpha^{-1}\alpha_j$ $(j = 1, 2, \ldots, r)$, т. е. всеки елемент x на D се записва като линейна комбинация от вида (4) с коефициенти от N.

Нека сега $e_1, e_2, \ldots, e_d$ е базис на N над F. Не е трудно да се покаже (както при доказателството на теорема 2 от § 2 на глава VII), че системата от dr елемента $e_i u_j$ $(i = 1, 2, \ldots, d;$ $j = 1, 2, \ldots, r)$ образува базис на D над F. Следователно $n = \dim_F D = dr$ и лемата е доказана.

Теорема 4 (теорема на Ведербърн). *Всяко крайно тяло е комутативно, т. е. всяко крайно тяло е поле.*

Доказателство. Нека D е произволно крайно тяло и F е центърът на D. Ясно е, че D е поле точно тогава, когато $D = F$, т. е. когато размерността n на D над F е равна на единица.

Да допуснем, че $n > 1$. Нека $q = |F|$ е броят на елементите на полето F. Тогава броят на елементите на тялото D е равен на q^n. Тъй като мултипликативната група $D^* = D \setminus \{0\}$ на D има $q^n - 1$ елемента, а тази на F съдържа $q - 1$ елемента и съвпада с центъра $Z(D^*)$ на D^*, то от формула (1) получаваме

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} c_i, \tag{5}$$

където k е броят на всички неедноелементни класове от спрегнати елементи в D^*, а c_i $(c_i > 1)$ дели $q^n - 1$, защото c_i е броят на елементите на i-тия клас от спрегнати елементи в групата D^*.

Нека $a \in D^*$, т. е. a е ненулев елемент от D. Според твърдение 2 нормализаторът $N(a)$ на a в тялото D е подтяло, което съдържа F. Да означим с d размерността на $N(a)$ над F. Тогава $N(a)$ съдържа q^d елемента. Мултипликативната група $N^*(a) = N(a) \setminus \{0\}$ има $q^d - 1$ елемента и очевидно $N^*(a)$ съвпада с централизатора $C(a)$ на a в групата D^*. Затова броят на спрегнатите елементи с a в групата D^* е равен на индекса на централизатора $C(a)$ в D^*, т. е. на $\frac{q^n - 1}{q^d - 1}$, където числото $d = \dim_F N(a)$ съгласно лема 4 дели числото n.

По този начин установихме, че числата c_i от равенството (5) са от вида $c_i = \frac{q^n - 1}{q^{d_i} - 1}$, където $d_i | n$ и $d_i \neq n$ понеже $c_i > 1$ $(i = 1,$

2, ..., k). Сега равенството (5) се записва във вида

$$q^n-1=q-1+\sum_{i=1}^{k}\frac{q^n-1}{q^{d_i}-1}, \tag{6}$$

където d_i/n и $d_i\neq n$.

Съгласно лема 3 стойността $\Phi_n(q)$ при $x=q$ на n-тия циклотомичен полином $\Phi_n(x)$ дели **лявата страна** на (6) и числата $\frac{q^n-1}{q^{d_i}-1}$ $(i=1, 2, \ldots, k)$. Следователно $\Phi_n(q)$ дели $q-1$, което противоречи на лема 3. Полученото противоречие се дължи на допускането, че $n=\dim_F D>1$. Затова $n=1$ и $D=F$, т. е. тялото D е поле. Теоремата е доказана.

Тази теорема показва, че задачата да се характеризират всички крайни тела съвпада със задачата да се опишат всички крайни полета. Последната задача бе решена с теорема 11 на глава VIII, според която за всяко просто число p и за всяко естествено число n съществува едно-единствено поле с p^n елемента и всяко крайно поле е от този вид.

Прието е крайните полета да се наричат *полета на Галоа* и единственото поле с характеристика p и с $q=p^n$ елемента се означава с $GF(q)$ или $GF(p^n)$.

Задачата да се характеризират всички крайномерни алгебри с деление над дадено крайно поле вече не представлява особена трудност.

Твърдение 9. *Нека P е поле с характеристика p и с p^n елемента, т. е. $P=GF(p^n)$. Ако m е произволно естествено число, а $L=GF(p^{mn})$, то L е алгебра с размерност m над полето P.*

Доказателство. Най-напред ще докажем, че в L се съдържа подполе M, изоморфно на P. Да разгледаме полиномите

$$f(x)=x^{p^n}-x,\ g(x)=x^{p^{nm}}-x$$

над полето Z_p. Както знаем от § 7 на глава VIII, P е полето на разлагане на $f(x)$ над Z_p, а L е полето на разлагане на $g(x)$ над Z_p. Освен това P и L съвпадат съответно с множествата от корените на $f(x)$ и $g(x)$. Нека α е корен на $f(x)$. Тогава $\alpha^{p^n}=\alpha$. Да допуснем, че за някое естествено число k сме доказали равенството $\alpha^{p^{nk}}=\alpha$. Тогава

$$\alpha^{p^{n(k+1)}}=(\alpha^{p^{nk}})^{p^n}=\alpha^{p^n}=\alpha.$$

Следователно за всяко естествено число s имаме $\alpha^{p^{ns}}=\alpha$. В частност $g(\alpha)=\alpha^{p^{nm}}-\alpha=\alpha-\alpha=0$, т. е. всеки корен на полинома $f(x)$ е корен и на полинома $g(x)$. Понеже корените на $f(x)$ са прости (еднократни), то $f(x)$ ще дели $g(x)$. Нека $g(x)=f(x)h(x)$ където $h(x)$ е полином също с коефициенти от полето Z_p. Да

означим с M подмножеството на полето L от всички корени на $g(x)$, които са корени и на $f(x)$. Понеже L е поле на разлагане на $g(x)$, то M ще се състои точно от $q=p^n$ елемента и ще бъде поле на разлагане на $f(x)$ над Z_p, т. е. M и P съгласно следствие 3 на глава VIII ще бъдат изоморфни.

Нека $\tau: P \to M \subseteq L$ е един изоморфизъм на P върху M. Сега дефинираме произведение на елемента $\lambda \in P$ с елемента a от L, като полагаме $\lambda a = \tau(\lambda)\, a$, където в дясната страна на равенството е произведението на елемента $\tau(\lambda)$ от подполето M на L с елемента a от L. Лесно се проверява, че L е алгебра над P спрямо събирането и умножението в L и така определеното умножение на елементи от L с елементи от P.

Теорема 5. *Нека P е крайно поле с характеристика p и с $q=p^n$ елемента. Полетата на Галоа $GF(p^{nm})$, $m=1, 2, \ldots$, са единствените крайномерни алгебри с деление над полето P.*

Доказателство. Според твърдение 9 всяко от полетата $GF(p^{nm})$ $(m=1, 2, \ldots)$ може по определен начин да се разглежда като крайномерна алгебра с деление над полето P.

Обратно, нека A е крайномерна алгебра с деление над полето P и $r=\dim_P A$. Тогава A е тяло с $q^r=p^{nr}$ елемента. От теорема 4 следва, че A е поле. По познат вече начин (§ 2) можем да отъждествим P с изоморфното му подполе на A. Тогава алгебрата A е разширение на P от степен $[A:P]=r$. Но A е поле с p^{nr} елемента и затова A е поле на разлагане на полинома $h(x)=x^{p^{nr}}-x$ над Z_p. Очевидно е, че A е поле на разлагане на $h(x)$ и над полето P.

Ако сега B е друга алгебра с деление над P, която има същата размерност r, по същия начин се вижда, че B е поле на разлагане на $h(x)$ над P. Съгласно следствие 8 от глава VIII A и B са изоморфни над P полета, т. е. A и B са изоморфни като алгебри над P. Теоремата е доказана.

ГЛАВА XII

ЕЛЕМЕНТИ ОТ ТЕОРИЯТА НА ГАЛОА

В § 9 на глава II се запознахме с формулите, които изразяват корените на алгебричните уравнения от трета и четвърта степен чрез техните коефициенти. В тези формули, както и във формулите за корените на квадратните уравнения, освен основните аритметични действия участвуват само операциите коренуване, т. е., както се казва, *уравненията от степен, не по-големи от 4, са решими в радикали или са решими алгебрично.*

В настоящата глава ще се запознаем накратко с теорията на Галоа, която дава точните условия, при които дадено алгебрично уравнение е решимо в радикали. Гениалният френски математик Е. Галоа успява да съпостави на всяко алгебрично уравнение конкретна крайна група, наричана днес *група на Галоа на уравнението*, и да установи, че уравнението е решимо в радикали точно тогава, когато неговата група е *разрешима*, т. е. когато тя е „изградена" по специален начин от крайни абелеви групи. Тази блестяща идея е една от фундаменталните идеи на съвременната математика.

Докато резултатите на § 1 се отнасят до полета с произволна характеристика, то от началото на § 2 до края разглежданите полета са с нулева характеристика. От многобройните приложения на теорията на Галоа ще приведем само две — намирането на конкретни уравнения, които са нерешими в радикали, и доказателството на теоремата на Руфини—Абел за алгебричната нерешимост на общото уравнение от степен $\geqq 5$.

§ 1. Автоморфизми на поле

Всеки изоморфизъм на едно поле K върху себе си се нарича *автоморфизъм* на K, а множеството от всички автоморфизми на K се бележи с $\mathrm{Aut}\,K$. Ясно е, че автоморфизмът σ на полето K е едновременно автоморфизъм на адитивната и мултипликативната група на полето K. Затова σ оставя неподвижни нулевия и единичния елемент на K, т. е. $\sigma(0)=0$ и $\sigma(1)=1$.

Задача 1. Да се докаже, че подмножеството K^σ на полето K, което е съставено от всички неподвижни елементи относно даден автоморфизъм σ на K, е подполе на K и следователно елементите на простото (минималното) подполе на K са неподвижни относно всеки автоморфизъм на K.

Примери

1. Тъждественото преобразуване ε на полето K ($\varepsilon(a)=a$ за всяко $a \in K$) е автоморфизъм на K. Това показва, че множест-

то Aut K не е празно. Ако K е просто поле, то ε е единственият автоморфизъм на K, т. е. в този случай Aut $K=\{\varepsilon\}$.

2. Ако $K=\mathbf{C}$ е полето на комплексните числа, то изображението σ, за което $\sigma(a+bi)=a-bi$, $a, b \in \mathbf{R}$, е автоморфизъм на полето $\mathbf{C}$, а подполето от неподвижните числа спрямо σ е полето $\mathbf{R}$ на реалните числа, т. е. $\mathbf{C}^{\sigma}=\mathbf{R}$. Този автоморфизъм ще наричаме *комплексно спрягане*.

Задача 2. Нека σ е автоморфизъм на полето K. Да се докаже, че обратното изображение σ^{-1} на σ е също автоморфизъм на K.

Произведението (т. е. последователното прилагане) на два автоморфизма на полето K е също автоморфизъм на K (докажете го!). По този начин в множеството Aut K имаме операция умножение на автоморфизми. Лесно се проверява, че Aut K е група относно това умножение. Тъждественият автоморфизъм ε на полето K е единичният елемент на тази група и затова ε се нарича също *единичен автоморфизъм* на полето K. В общия случай групата Aut K не е абелева, т. е. произведенията $\sigma\tau$ и $\tau\sigma$ невинаги съвпадат.

Определение 1. Ако L е подполе на полето K, а σ е автоморфизъм на K, то ще казваме, че σ е *автоморфизъм на K над L* или че L е *неподвижно спрямо автоморфизма* σ, ако σ оставя неподвижни елементите на L.

Според твърдението на задача 1 подмножеството K^{σ} от неподвижните спрямо σ елементи на K е максималното неподвижно подполе относно σ — то съдържа всяко подполе, което е неподвижно относно σ.

Задача 3. Нека подполето L на полето K е неподвижно спрямо автоморфизма $\sigma \in$ Aut K. Да се докаже, че σ е обратим линеен оператор на линейното пространство K над полето L.

Простото подполе на K е неподвижно относно всеки автоморфизъм на K, а всяко подполе на K е неподвижно относно единичния автоморфизъм. Подполетата на полето $\mathbf{R}$ на реалните числа и само те са неподвижни относно автоморфизма комплексно спрягане в полето $\mathbf{C}$ на комплексните числа.

Лема 1. *Автоморфизмът σ на простото алгебрично разширение $P(a)$ над полето P съвпада с тъждественния автоморфизъм ε на $P(a)$ тогава и само тогава, когато $\sigma(a)=a$.*

Наистина всеки елемент b от $P(a)$ се записва във вида $b=p_0+p_1a+p_2a^2+\ldots+p_{n-1}a^{n-1}$, където $n=[P(a):P]$ и $p_0, p_1, \ldots, p_{n-1}$ са от P. Тъй като по условие $\sigma(p_i)=p_i$, то

$$\sigma(b)=p_0+p_1\sigma(a)+p_2\sigma(a)^2+\ldots+p_{n-1}\sigma(a)^{n-1}.$$

Следователно ако $\sigma(a)=a$, то за всяко b от $P(a)$ ще се получи $\sigma(b)=b$. Обратното е очевидно.

Следствие 1. *Нека $K=P(a_1, a_2, \ldots, a_n)$ е алгебрично породено разширение на полето P. Автоморфизъм σ на K над P съвпада с тъждественния автоморфизъм ε тогава и само тогава, когато $\sigma(a_i)=a_i$ за всяко $i=1, 2, \ldots, n$.*

Действително, понеже полето K съвпада със съставното алгебрично разширение $P(a_1)(a_2)\ldots(a_n)$, то с индукция по n и прилагане на предната лема доказателството се провежда елементарно.

Два автоморфизма σ и τ на полето K съвпадат тогава и само тогава, когато $\tau^{-1}\sigma=\varepsilon$. Затова предното следствие може да се изкаже и по следния начин:

Следствие 2. *При условията и означенията на предното следствие два автоморфизма σ и τ на полето K над подполето P съвпадат тогава и само тогава, когато $\sigma(a_i)=\tau(a_i)$ за всяко $i=1, 2, \ldots, n$.*

Ако G е група, а K е поле, то навсякъде в тази глава с $H\leqq G$, $H\lhd G$ и $P\leqq K$ ще означаваме съответно, че H е подгрупа на групата G, че H е нормален делител на G и P е подполе на K. Макар че означението за подгрупа и подполе е едно и също, няма опасност от объркване на обектите подгрупа и подполе, тъй като предварително се съобщава от какъв вид е изходната алгебрична структура. Ако K е поле, а $\mathrm{Aut}\,K$ е групата от автоморфизмите на K, $L\leqq K$, то с $G(K/L)$ ще означаваме множеството от всички автоморфизми на K над L, а с K^W — множеството от неподвижните елементи на K спрямо всички автоморфизми от подмножеството W на $\mathrm{Aut}\,K$, т. е. $K^W=\bigcap\limits_{\sigma\in W} K^\sigma$. От твърдението на задача 1 следва, че K^W като сечение на подполета на K е също подполе на K.

Между подполетата на полето K и подгрупите на групата $\mathrm{Aut}\,K$ съществува естествено съответствие, което ще определим в следващото твърдение. По-късно ще покажем, че при някои ограничения това съответствие притежава редица важни свойства.

Твърдение 1. *Ако K е поле, $M\leqq L\leqq K$ и $V\leqq U\leqq \mathrm{Aut}\,K$, то*

а) $G(K/L)\leqq G(K/M)\leqq \mathrm{Aut}\,K$,

б) $K^U\leqq K^V\leqq K$ *и*

в) $L\leqq K^{G(K/L)}$, $H\leqq G(K/K^H)$.

Доказателство. а) Тъй като всяко подполе L на K е неподвижно относно единичния автоморфизъм ε, то $\varepsilon\in G(K/L)$. Нека $\sigma, \tau\in G(K/L)$. Автоморфизмите σ и τ оставят неподвижни елементите на L. Затова τ^{-1} също оставя неподвижни елементите на L и за всяко $a\in L$ следва $\sigma\tau^{-1}(a)=\sigma(\tau^{-1}(a))=\sigma(a)=a$, т. е. $\sigma\tau^{-1}\in G(K/L)$. Следователно $G(K/L)\leqq \mathrm{Aut}\,K$. Тъй като $M\leqq L$, то всеки автоморфизъм σ от $G(K/L)$ оставя неподвижни елементите на M и по тази причина $\sigma\in G(K/M)$. Следователно $G(K/L)\leqq G(K/M)$.

б) Както бе отбелязано по-горе, K^W е подполе на K за всяко непразно подмножество W на $\mathrm{Aut}\,K$. В частност K^U и K^V са подполета на K. Тъй като $V\leqq U$, то неподвижните елементи на K относно U са неподвижни и относно V, т. е. $K^U\leqq K^V$.

в) Включванията $L \leqq K^{G(K/L)}$, $H \leqq G(K/K^H)$ следват непосредствено от определенията на $G(K/L)$, $K^{G(K/L)}$ и K^H, $G(K/K^H)$. Твърдението е доказано.

Тук следва да отбележим, че съответствията, които определихме в предното твърдение, не са взаимно еднозначни. На различни подполета на K може да отговаря една и съща подгрупа на Aut K, а така също на различни подгрупи на Aut K често съответства едно и също поле. Както ще видим обаче, на различни крайни подгрупи на Aut K съответстуват различни подполета на K.

Задача 4. Нека L е подполе на полето K, а H е подгрупа на групата Aut K. Да се докажат равенствата

$$G(K/L) = G(K/K^{G(K/L)}),\ K^H = K^{G(K/K^H)}.$$

Определение 2. Ако W е непразно подмножество на групата Aut K, то подполето K^W се нарича *неподвижно подполе* на W.

Твърдение 2. а) *Нека σ е автоморфизъм на полето K над подполето P и елементът a от K е алгебричен над P. Тогава елементите a и $b = \sigma(a)$ имат един и същ минимален полином над P. Автоморфизмът σ изобразява изоморфно простото алгебрично разширение $P(a)$ върху простото алгебрично разширение $P(b)$.*

б) *Ако $P \leqq L \leqq K$ и L е поле на разлагане на някой полином над P, то автоморфизмът σ изобразява изоморфно L върху L, т. е. ограничението на σ върху подполето L е автоморфизъм на L.*

Доказателство. Нека

$$p(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$$

е минималният полином на a над P. Тогава $p(a) = a^n + a_1 a^{n-1} + a_2 a^{n-2} + \ldots + a_n = 0$. Като приложим автоморфизма σ към двете страни на това равенство и отчетем, че σ оставя неизменни коефициентите $a_1, a_2, \ldots, a_n \in P$, то получаваме равенството

$$b^n + a_1 b^{n-1} + \ldots + a_{n-1} b + a_n = 0,$$

което показва, че елементът b е корен на полинома $p(x)$ от $P[x]$. Ако сега $q(x)$ е минималният полином на b над P, то $q(x)$ дели $p(x)$. Двата полинома са неразложими над P и имат старши коефициенти 1. Следователно $q(x) = p(x)$.

Ако някой от елементите a, b е корен на полинома $f(x) \in P[x]$ то минималният му полином $p(x)$ дели $f(x)$ и затова и двата елемента a, b са корени на $f(x)$, т. е. те са корени на едни и същи полиноми над полето P.

Всеки елемент u от полето $F(a)$ се записва еднозначно във вида $u = p_0 + p_1 a + \ldots + p_{r-1} a^{r-1}$ и $\sigma(u) = p_0 + p_1 b + \ldots + p_{r-1} b^{r-1}$ е от $F(b)$. Затова σ е изоморфизъм на $F(a)$ върху $F(b)$.

в) Полетата L и K са линейни пространства над P, а σ е същевременно обратим линеен оператор на линейното пространство K. Операторът σ изобразява изоморфно подпространството L върху $M=\sigma(L)$. Освен това M е подполе на K, понеже σ е автоморфизъм на полето K. Тъй като M съдържа P, следва, че M е изоморфно на линейното пространство L като линейно пространство над P. Оттук следва и равенството на размерностите (степените) $[L:P]=\dim_P L=\dim_P M=[M:P]$.

Нека L е поле на разлагане на полинома $f(x)\in P[x]$. Ако $c_1, c_2, \ldots, c_n$ са корените на $f(x)$ в L, то $L=P(c_1, \ldots, c_n)=P(c_1)\ldots(c_n)$. Но тогава елементите на L се записват като полиноми на $c_1, c_2, \ldots, c_n$ с коефициенти от P. Следователно елементите на $M=\sigma(L)$ се записват като полиноми на $\sigma(c_1), \sigma(c_2), \ldots, \sigma(c_n)$ с коефициенти от P. По първата част а) на твърдението елементът $\sigma(c_i)$ съпада с някой корен c_j на $f(x)$, т. е. $\sigma(c_1), \sigma(c_2), \ldots, \sigma(c_n)$ е една пермутация на корените $c_1, c_2, \ldots, c_n$. Следователно $M\leqq L$. Тъй като $\dim_P M=\dim_P L$, то $M=\sigma(L)=L$ и ограничението на σ върху L е автоморфизъм на подполето L.

Следствие 3. *Нека K е разширение на полето P и L е междинно подполе (т. е. $P\leqq L\leqq K$), което е поле на разлагане на някой полином над P. Ако ψ е изображението, което на всеки автоморфизъм σ от групата $G(K/P)$ съпоставя неговото ограничение $\psi(\sigma)=\sigma|_L$ върху L, то ψ е хомоморфизъм на групата $G(K/P)$ в групата от автоморфизмите на L над P. Ядрото $\ker\psi$ на този хомоморфизъм съвпада с подгрупата $G(K/L)$.*

Доказателство. По предното твърдение ограничението $\psi(\sigma)=\sigma|_L$ е автоморфизъм на L. Ако $a\in P$, то $\sigma(a)=a$, тъй като $\sigma\in G(K/P)$. Но $P\leqq L$ и тогава $\psi(\sigma)(a)=\sigma(a)=a$. Следователно $\psi(\sigma)$ е автоморфизъм на L над P, т. е. ψ е изображение на групата $G(K/P)$ в групата от автоморфизмите на L над P. От $a\in L$ следва $\psi(\sigma)(a)=\sigma(a)\in L$. Ако $\tau\in G(K/P)$, то тогава равенствата

$$\psi(\tau\sigma)(a)=\tau\sigma(a)=\tau(\sigma(a))=\psi(\tau)(\sigma(a))$$

$$=\psi(\tau)(\psi(\sigma))(a)=\psi(\tau)\psi(\sigma)(a)$$

са валидни за всяко a от L, т. е. $\psi(\tau\sigma)=\psi(\tau)\psi(\sigma)$, което показва, че изображението ψ е хомоморфизъм на групата $G(K/P)$ в групата от автоморфизмите на L над P.

Съгласно твърдение 1 а) $G(K/L)$ е подгрупа на $G(K/P)$. Ядрото $\ker\psi$ на хомоморфизма ψ се състои точно от тези σ от $G(K/P)$, които оставят неподвижни елементите на L, т. е. то съвпада с подгрупата $G(K/L)$ на групата $G(K/P)$. Следствието е доказано.

Определение 3. Ще казваме, че два елемента a и b от полето K са *спрегнати над подполето* P на K тогава и само тогава, когато те са алгебрични над P и минималните им полиноми над P съвпадат.

Задача 5. Докажете, че елементите a и b от полето K са спрегнати над подполето P тогава и само тогава, когато a и b са корени на един и същ неразложим полином над P.

Понятието „спрегнати елементи над поле P" разглеждаме само за алгебрични елементи над P. За трансцендентен елемент t над P не се поставя въпросът за спрегнатите с t над P.

Примери

1. Ако P е реално числово поле ($P \leqq R$) и C е полето на комплексните числа, то числата i и $-i$ са спрегнати над P, тъй като x^2+1 е минималният полином над P на всяко едно от тези числа. Напротив, i и $-i$ не са спрегнати над полето $Q(i)$ от гаусовите числа, тъй като техните минимални полиноми над $Q(i)$ са $x-i$ и $x+i$, а $x-i \neq x+i$.

2. Числата $\sqrt{2}$ и $-\sqrt{2}$ са спрегнати над полето Q на рационалните числа.

Задача 6. Да се докаже, че числото z и неговото комплексно спрегнато $\bar{z}$ са спрегнати над полето R на реалните числа.

Задача 7. Нека a е елемент от разширението K на полето P. Да се докаже, че в K има само краен брой елементи, които са спрегнати с a над подполето P.

Твърдение 3. *Нека полето K е поле на разлагане на някой полином от P[x]. Два елемента a и b от K са спрегнати над P тогава и само тогава, когато съществува такъв автоморфизъм σ на K над подполето P, че $b=\sigma(a)$.*

Доказателство. Нека K е поле на разлагане на полинома $f(x) \in P[x]$ и $c_1, c_2, \ldots, c_n$ са корените на $f(x)$. Тъй като K съвпада с алгебрично породеното разширение $P(c_1, \ldots, c_n)$, то K е крайно разширение на P и всички елементи на K са алгебрични над P.

Ако $a, b \in K$ и $b=\sigma(a)$ при някой автоморфизъм σ на K над P, то по твърдение 2 минималните полиноми на a и b над P съвпадат, т. е. a и b са спрегнати над P.

Обратно, ако a, b от K са спрегнати над P, то те имат един и същ минимален полином $p(x)$ над P. Според теорема 7 от глава VIII тъждественият автоморфизъм на P се продължава до такъв изоморфизъм τ на полето $P(a)$ върху полето $P(b)$, че $\tau(a)=b$. Коефициентите на $f(x)$ са от P и затова те се намират както в полето $P(a)$, така и в полето $P(b)$. Очевидно е, че $K=P(a)(c_1, \ldots, c_n)$ и $K=P(b)(c_1 \ldots, c_n)$. Следователно полето K е поле на разлагане на $f(x)$ както над $P(a)$, така и над $P(b)$. По теорема 9 от глава VIII изоморфизмът τ се продължава до изоморфизъм σ на K върху K, т. е. до автоморфизъм на полето K. Автоморфизмът σ изобразява a в b и оставя неподвижни елементите на P, тъй като той е продължение на τ, а τ е продължение на единичния автоморфизъм на P. Твърдението е доказано.

Лема 2. *Нека K е произволно поле и $\sigma_1, \sigma_2, \ldots, \sigma_n$ са различни автоморфизми на полето K. Ако $a_1, a_2, \ldots a_n$ са та-*

к

сива елементи от K, че за всяко x от K е изпълнено равен-

(тво по

1) $$a_1\sigma_1(x)+a_2\sigma_2(x)+\ \ldots\ +a_n\sigma_n(x)=0,$$

то $a_1=a_2=\ \ldots\ =a_n=0.$

Доказателство. Ще извършим индукция по числото n. Ако $n=1$, то за $x=1\in K$ получаваме $0=a_1\sigma(1)=a_1.1=a_1$, т. е. лемата е вярна в този случай. Нека $n>1$ и да допуснем, че лемата е вярна за по-малко от n автоморфизма на K. Нека за автоморфизмите $\sigma_1, \sigma_2, \ldots, \sigma_n$ на K и $a_1, a_2, \ldots, a_n$ от K е изпълнено равенството (1) за всяко $x\in K$. Тъй като $\sigma_1\neq\sigma_n$, то съществува такъв елемент $b\in K$, че $\sigma_1(b)\neq\sigma_n(b)$. Като заместим в (1) елемента x с bx, получаваме

(2) $$a_1\sigma_1(b)\,\sigma_1(x)+a_2\sigma_2(b)\,\sigma_2(x)+\ldots\ +a_n\sigma_n(b)\,\sigma_n(x)=0,$$

а с умножаване на двете страни на (1) със $\sigma_1(b)$ се получава равенството

(3) $$a_1\sigma_1(b)\,\sigma_1(x)+a_2\sigma_1(b)\,\sigma_2(x)+\ \ldots\ +a_n\sigma_1(b)\,\sigma_n(x)=0.$$

Изваждаме почленно равенство (3) от равенство (2) и получаваме равенството

(4) $$a_2(\sigma_2(b)-\sigma_1(b))\,\sigma_2(x)+\ \ldots\ +a_n(\sigma_n(b)-\sigma_1(b))\,\sigma_n(x)=0,$$

което е валидно за всяко $x\in K$. По предположението на индукцията коефициентите в (4) са равни на нула. В частност $a_n(\sigma_n(b)-\sigma_1(b))=0$. Но според избора на елемента b, $\sigma_n(b)-\sigma_1(b)\neq 0$. Затова $a_n=0$. Тогава от (1) при $a_n=0$ отново от предположението на индукцията получаваме $a_1=a_2=\ \ldots\ =a_{n-1}=0$.

Лема 3. *Ако* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *са различни автоморфизми на полето K, а M е неподвижното подполе на K спрямо* $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, *то* $[K:M]\geqq n$.

Доказателство. Да означим с r степента $[K:M]$ и да допуснем, че лемата не е вярна. Тогава ще имаме $r<n$. Нека $a_1, a_2, \ldots, a_r$ е произволен базис на K над M. Да разгледаме системата линейни хомогенни уравнения

$$\sigma_1(a_i)\,x_1+\sigma_2(a_i)\,x_2+\ \ldots\ +\sigma_n(a_i)\,x_n=0,\quad i=1, 2, \ldots, r.$$

Тъй като броят r на уравненията е по-малък от броя n на неизвестните, то тази система има ненулево решение $(b_1, b_2, \ldots, b_n)$ в полето K. Поне един от елементите $b_1, b_2, \ldots, b_n$ е ненулев и са изпълнени равенствата

(5) $$\sigma_i(a_i)\,b_1+\sigma_2(a_i)\,b_2+\ \ldots\ +\sigma_n(a_i)\,b_n=0,\quad i=1, 2, \ldots, r.$$

Ако x е произволен елемент от K, то $x=q_1a_1+q_2a_2+\ \ldots\ +q_ra_r$, където $q_1, q_2, \ldots, q_r\in M$. Понеже M е неподвижното подполе на $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, то

$$\sigma_j(x)=\sigma_j\left(\sum_{i=1}^{r} q_i\,a_i\right)=\sum_{i=1}^{r} q_i\,\sigma_j(a_i),\quad j=1, 2, \ldots, n.$$

Оттук, като умножим равенството (5) с q_i и сумираме получените равенства за $i=1, 2, \ldots, r$, получаваме

$$\sigma_1(x)b_1+\sigma_2(x)b_2+\ \ldots\ +\sigma_n(x)b_n=0.$$

Понеже x е произволен елемент от K, то по лема 1 от последното равенство следва $b_1=b_2=\ \ldots\ =b_n=0$, което противоречи на избора на елементите $b_1, b_2, \ldots, b_n$. Лемата е доказана.

Следствие 4. *Ако K е крайно разширение на полето P, то групата $G(K/P)$ от автоморфизмите на K над P е крайна и $[K:P]\geqq|G(K/P)|$.*

Наистина ако L е неподвижното поле на $G(K/P)$, то по предната лема $[K:L]\geqq|G(K/P)|$, а по твърдение 1 в) имаме $P\leqq L\leqq K$, т. е. $[K:P]\geqq[K:L]\geqq|G(K/P)|$.

Теорема 1. *Нека H е крайна подгрупа на групата $\mathrm{Aut}\,K$ от автоморфизмите на полето K, а $M=K^H$ е неподвижното му подполе. Тогава K е крайно разширение на M, $[K:M]=|H|$ и подгрупата H съвпада с подгрупата $G(K/M)$ от автоморфизмите на K над M.*

Доказателство. Нека $\sigma_1, \sigma_2, \ldots, \sigma_n$ са елементите на H. От лема 3 знаем, че $[K:M]\geqq n$. За да докажем обратното неравенство, е достатъчно да покажем, че всяка система от $n+1$ елемента на K е линейно зависима над M.

Ако $a\in K$, то полагаме $S(a)=\sigma_1(a)+\sigma_2(a)+\ \ldots\ +\sigma_n(a)$, където $S(a)\in K$. За всяко $\sigma\in H$ елементите $\sigma\sigma_1, \sigma\sigma_2, \ldots, \sigma\sigma_n$ са същото всичките n елемента на H. Затова $\sigma(S(a))=S(a)$ за всяко $\sigma\in H$, т. е. елементът $S(a)$ се съдържа в M. Той се нарича *следа* на a и полученото показва, че следата на всеки елемент a от K се съдържа в M. От лема 2 непосредствено следва, че в K съществува поне един елемент b с ненулева следа $S(b)$.

Нека сега $a_1, a_2, \ldots, a_{n+1}$ са $n+1$ елемента от K. Разглеждаме следната система линейни хомогенни уравнения над полето K:

$$x_1\sigma_i^{-1}(a_1)+x_2\sigma^{-1}(a_2)+\ \ldots\ +x_{n+1}\sigma_i^{-1}(a_{n+1})=0,\quad i=1, 2, \ldots, n.$$

Броят n на уравненията в тази система е по-малък от броя $n+1$ на неизвестните. Затова тя притежава ненулево решение $(c_1, c_2, \ldots, c_{n+1})$. Можем да считаме, че $c_1\neq 0$. Лесно се вижда, че елементите $b_i=bc_1^{-1}c_i$ $(i=1, 2, \ldots, n+1)$ също образуват ненулево решение на разглежданата система. Следователно

$$b_1\sigma_i^{-1}(a_1)+b_2\sigma_i^{-1}(a_2)+\ \ldots\ +b_{n+1}\sigma_i^{-1}(a_{n+1})=0,\quad i=1, 2, \ldots, n.$$

Като приложим σ_i към двете страни на i-тото от тези равенства получаваме

$$\sigma_i(b_1)a_1+\sigma_i(b_2)a_2+\ \ldots\ +\sigma_i(b_{n+1})a_{n+1}=0,\quad i=1, 2, \ldots, n.$$

Чрез почленно сумиране на последните n равенства намираме, че

$$S(b_1)a_1+S(b_2)a_2+\ \ldots\ +S(b_{n+1})a_{n+1}=0,$$

където $S(b_i)\in M$ и $S(b_1)=S(b)\neq 0$.

Полученото равенство показва, че елементите $a_1, a_2, \ldots, a_{n+}$ са линейно зависими над полето M. Следователно $[K:M]=n=|H|$.

От твърдение 1 знаем, че $H \leqq G(K/M)=G(K/K^H)$. Ако съществува автоморфизъм σ от $G(K/M)$, който не принадлежи на H, то $\sigma_1, \sigma_2, \ldots, \sigma_n, \sigma$ е система от $n+1$ различни автоморфизма, на която неподвижното подполе е M. Като приложим лема 3 за тези $n+1$ автоморфизма, получаваме неравенството $[K:M] \geqq n+1$, което е невъзможно. Следователно $H=G(K/M)$. Теоремата е доказана.

Следствие 5. *Различни крайни подгрупи на групата* Aut K *от автоморфизмите на полето* K *имат различни неподвижни подполета в* K.

Наистина ако H_1 и H_2 са две крайни подгрупи на Aut K, които имат едно и също неподвижно подполе $M=K^{H_1}=K^{H_2}$, то по предната теорема $H_1=G(K/M)=H_2$.

§ 2. Нормални разширения

За да избегнем известни трудности, до края на настоящата глава ще предполагаме, че разглежданите полета са с нулева характеристика. От теоремата за примитивния елемент (глава VIII, теорема 12) следва, че всяко крайно разширение на поле с характеристика 0 е просто алгебрично разширение. Този факт ще бъде използуван често в доказателствата на твърденията, които следват по-нататък.

Теорема 2. *Нека* K *е крайно разширение на полето* P. *Тогава следните две свойства на полето* K *са еквивалентни:*

а) K *е поле на разлагане на някой полином от* $P[x]$;

б) *Ако един неразложим полином над* P *притежава поне един корен в* K, *то полето* K *съдържа поле на разлагане на този полином, т. е. той се разлага в произведение на линейни множители над полето* K.

Доказателство. 1) Нека K е поле на разлагане на полинома $f(x) \in P[x]$, а $g(x)$ е неразложим над P полином, който има корен a в полето K. Да допуснем, че $g(x)$ не се разлага на линейни множители над полето K. Коефициентите на $g(x)$ са от полето P, а P е подполе на K. Разглеждаме полинома $g(x)$ като полином над K. Нека M е поле на разлагане на $g(x)$ над полето K. Тогава $K \neq M$, а $g(x)$ има корен b от M, който не се съдържа в K. Полето M е крайно разширение на K, а K е крайно разширение на P. Затова M е крайно разширение на полето P. Следователно полето M е просто алгебрично разширение на P. Нека $M=P(\theta)$ и $p(x)$ да е минималният полином на θ над P. Да означим с T полето на разлагане на $p(x)$ над M. Ако $\theta_1=\theta, \theta_2, \ldots, \theta_s$ са корените на $p(x)$ в полето T, то $T=M(\theta_1, \theta_2, \ldots, \theta_s)$. Понеже $\theta_1=\theta$ и $M=P(\theta)$, то полето T очевидно съвпада с подполето си $P(\theta_1, \theta_2, \ldots, \theta_s)$, което е поле на разлагане на полинома $p(x)$ над P. Така полученото поле T съдържа полетата $P \leqq K \leqq M$ и е по-

ле на разлагане над полето P. Двата корена a от K и b от M на полинома $g(x)$ са елементи на полето T и те са спрегнати над P. Според твърдение 3 съществува такъв автоморфизъм σ на полето T над P, че $b=\sigma(a)$. Понеже подполето K на полето T е поле на разлагане над P, то от твърдението 2 следва, че $b=\sigma(a)\in\sigma(K)=K$. Но това противоречи на избора на корена b. Следователно полето K притежава и свойство б).

2) Обратно, нека полето K има свойството б). Тъй като полето K е крайно разширение на полето P, то K е просто алгебрично разширение на P. Нека $K=P(\alpha)$ и $r(x)$ е минималният полином на α над P. Понеже полиномът $r(x)$ е неразложим над P и има корен α в K, то той се разлага на линейни множители

$$r(x)=(x-\alpha_1)(x-\alpha_2)\ \ldots\ (x-\alpha_t)\ ,$$

над K, където $\alpha_1=\alpha, \alpha_2, \ldots, \alpha_t$ са елементи от $K=P(\alpha)$.

Очевидно полето K съвпада с подполето си $P(\alpha_1, \alpha_2, \ldots, \alpha_t)$, което е поле на разлагане на $r(x)$ над P. Следователно полето K притежава свойството а). Теоремата е доказана

Определение 4. Ще казваме, че крайното разширение K на полето P е *нормално*, ако то притежава едно от еквивалентните свойства а) и б) от теорема 2.

Тук възниква естественият въпрос, дали съществуват крайни разширения на основното поле P, които да не са нормални разширения. Отговорът зависи от свойствата на полето P. Ако например полето P е алгебрически затворено, то $K=P$ е единственото крайно разширение на P и то е нормално. Но този екстремален случай не е интересен за теорията, която развиваме. В общия случай отговорът на поставения въпрос е положителен. Например ако $P=\mathbf{Q}$ е полето на рационалните числа и $K=\mathbf{Q}(\sqrt[3]{2})$, то K е крайно разширение на $\mathbf{Q}$ от степен 3, което не е нормално разширение на $\mathbf{Q}$. Наистина полиномът x^3-2 е неразложим над $\mathbf{Q}$ (защо), притежава корен $\sqrt[3]{2}$ в K, но другите му два корена, които не са реални числа, не се съдържат в полето $K=\mathbf{Q}(\sqrt[3]{2})\subseteq\mathbf{R}$.

Задача 1. Нека K е крайно разширение на полето P и $[K:P]=2$. Докажете, че K е нормално разширение на P. Докажете също, че всяко крайно разширение на полето $\mathbf{R}$ на реалните числа е нормално.

Теорема 3. *Полето K е нормално разширение на подполето си P тогава и само тогава, когато P съвпада с неподвижното подполе на някоя крайна подгрупа на групата от автоморфизмите на полето K.*

Доказателство. 1) Нека K е нормално разширение на P. Тогава K е крайно разширение на полето P и по следствие 2 от предния параграф групата $H=G(K/P)$ от автоморфизмите на K над P е крайна, а нейният ред $n=|H|$ не е по-голям от степента $r=[K:P]$ на K над P. Подполето P се съдържа в неподвижното

подполе K^H на крайната подгрупа H на групата Aut K. Ще докажем, че P съвпада с K^H. Нека a е произволен елемент от K^H. Елементът a остава неподвижен относно всеки автоморфизъм на K над P и е алгебричен над P, понеже K е крайно разширение на P. От твърдение 3 следва, че елементът a е спрегнат над P само със себе си. Ако $p(x)$ е минималният полином на a над P, то $p(x)$ е неразложим над P и според твърдение 9 от глава VIII той няма многократни корени. Нормалното разширение K на P съдържа поле на разлагане на полинома $p(x)$ и корените на $p(x)$ от K са спрегнати над P с елемента a. Следователно полиномът $p(x)$ има един-единствен прост еднократен корен a, т. е. $p(x)=x-a$. Понеже $p(x)\in P[x]$, то $a\in P$. Следователно $K^H=P$, т. е. P е неподвижното поле на крайна подгрупа на групата Aut K на автоморфизмите на K

2) Обратно, нека подполето P е неподвижното подполе на някоя крайна подгрупа F на групата Aut K, а n е редът на F. Според теорема 1 полето K е крайно разширение на P, $[K:P]=n$ и подгрупата F съвпада с групата $G(K/P)$ от автоморфизмите на полето K над подполето P. Ще докажем, че K е поле на разлагане на някой полином над P. Тъй като K е крайно разширение на P, то $K=P(\alpha)$ за някой подходящ елемент α от K. Нека $p(x)$ е минималният полином на α над P. Тогава $\deg p(x)=[K:P]=n$. Ако $\sigma, \tau\in F$, то по следствие 2 на §1 $\sigma(\alpha)=\tau(\alpha)$ тогава и само тогава, когато $\sigma=\tau$. Следователно ако $\sigma_1=\varepsilon, \sigma_2, \ldots, \sigma_n$ са автоморфизмите от подгрупата F, то елементите $\alpha_1=\alpha=\sigma_1(\alpha)$, $\alpha_2=\sigma_2(\alpha)$, $\ldots$ $\alpha_n=\sigma_n(\alpha)$ са от K и са два по два различни. Според твърдение 3 тези n елемента са корени на полинома $p(x)$, чиято степен е равна на n. Следователно полиномът $p(x)$ се разлага на линейни множители $p(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ над полето K. Понеже $\alpha_1=\alpha$ и $K=P(\alpha)$, то $K=P(\alpha_1, \alpha_2, \ldots, \alpha_n)$, т. е. K е поле на разлагане на $p(x)$ над P. Теоремата е доказана.

Следствие 6. *Полето K е нормално разширение на подполето си P тогава и само тогава, когато групата $G=G(K/P)$ е крайна и подполето P съвпада с неподвижното подполе K^G на групата G.*

Наистина, когато K е нормално разширение на P, то, както видяхме в първата част на доказателството на предната теорема, групата G е крайна и $P=K^G$. Обратното пък е пряко следствие от тази теорема.

§ 3. Група на Галоа. Съответствие на Галоа

В този параграф ще считаме, че сред полетата с характеристика нула сме избрали едно произволно поле P, което ще наричаме *основно*, а всички разглеждани полета ще бъдат разширения на основното поле.

Ще казваме, че подполето L на полето K е *междинно* за M и K, ако $M\leqq L\leqq K$.

Определение 5. Ако полето K е нормално разширение на под-

полето си M, то групата $G(K/M)$ от всички автоморфизми на K над M ще означаваме $\mathrm{Gal}(K/M)$ и ще я наричаме *група на Галоа* на полето K над подполето M.

От твърдение 1 следва, че за всяка подгрупа H на групата $\mathrm{Gal}(K/M)$ е изпълнено включването $M \leqq K^H$, т. е. подполето K^H е междинно подполе за M и K.

Твърдение 4. *Ако K е нормално разширение на полето P и L е междинно подполе за P и K, то*

1) *K е нормално разширение на L;*
2) $H = \mathrm{Gal}(K/L) \leqq \mathrm{Gal}(K/P) = G$;
3) $L = K^H$ и
4) $[K:L] = |H|$.

Доказателство. По условие полето K е поле на разлагане на някой полином $f(x) \in P[x]$. Ако $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ са корените на $f(x)$, то $K = P(\alpha_1, \alpha_2, \ldots, \alpha_n) \leqq L(\alpha_1, \alpha_2, \ldots, \alpha_n) \leqq K$. Следователно изпълнено е равенството $K = L(\alpha_1, \alpha_2, \ldots, \alpha_n)$, което показва, че полето K е поле на разлагане на полинома $f(x)$ над полето, L т. е. K е нормално разширение на L.

Групата $H = \mathrm{Gal}(K/L)$ е подгрупа на групата G, тъй като $P \leqq L \leqq K$ (твърдение 1). Според следствие 6 от предния параграф имаме $L = K^H$, а от теорема 1 знаем, че имаме равенството $[K:L] = |H|$. Твърдението е доказано.

От предното твърдение следва, че на всяко междинно подполе L на нормалното разширение K на основното поле P съответствува подгрупата $\mathrm{Gal}(K/L)$ на $G = \mathrm{Gal}(K/P)$. От друга страна, на всяка подгрупа F на G отговаря неподвижното й подполе K^F, което е междинно подполе на P и K. Това съответствие между междинните подполета на нормалното разширение K на P и подгрупите на групата на Галоа G на K над P се нарича *съответствие на Галоа*. В следващите две теореми са посочени основните свойства на съответствието на Галоа.

Теорема 4. *Ако полето K е нормално разширение на полето P, то групата на Галоа $G = \mathrm{Gal}(K/P)$ е крайна и съответствието на Галоа притежава следните свойства:*

а) *на междинно подполе L на P и K отговаря подгрупата $H = \mathrm{Gal}(K/L)$ на G която има ред, равен на степента на K над L;*

б) *на подгрупа F на G отговаря неподвижното подполе $M = K^F$ на F, което е междинно подполе на P и K и степента $[K:M]$ е равна на реда на групата F;*

в) *за всяко междинно подполе L на P и K и за всяка подгрупа F на групата G са изпълнени равенствата*

$$L = K^{\mathrm{Gal}(K/L)}, \quad F = \mathrm{Gal}(K/K^F),$$

т. е. съответствието на Галоа е взаимно еднозначно съответствие между множеството на междинните подполета на P и K и множеството на подгрупите на групата на Галоа G на K над P;

г) *ако* L_1 *и* L_2 *са две междинни подполета на* K, *а* F_1 *и* F_2 *са две подгрупи на групата* G, *то от включването* $L_1 \leqq L_2$ *следва* $\mathrm{Gal}(K/L_1) \geqq \mathrm{Gal}(K/L_2)$, *а от* $F_1 \leqq F_2$ *следва* $K^{F_1} \geqq K^{F_2}$.

Наистина по следствие 6 от предния параграф групата G е крайна. Твърдение а) следва от твърдение 4, а твърдение б) — от теорема 1. Равенствата от твърдение в) са частен случай на равенствата от задача 4 на § 1. Те следват също директно от а) и б). Твърдение г) е частен случай на твърдение 1 от § 1.

Междинното подполе L на нормалното разширение K на полето P невинаги е нормално разширение на P. На въпроса, кога полето L е нормално разширение на основното поле P, отговаря следната теорема.

Теорема 5. *Нека* L *е междинно подполе на нормалното разширение* K *на полето* P *с група на Галоа* $G=\mathrm{Gal}(K/P)$, *а* $H=\mathrm{Gal}(K/L)$ *е подгрупата на* G, *която отговаря на* L *в съответствието на Галоа. Полето* L *е нормално разширение на основното поле* P *тогава и само тогава, когато* H *е нормален делител на групата* G. *Ако* L *е нормално разширение на полето* P, *то* $F=\mathrm{Gal}(L/P)$ *е изоморфна на фактор-групата* G/H.

Доказателство. Тъй като K е крайно разширение на P, то и L е крайно разширение на P. Затова $L=P(\alpha)$ за подходящ елемент α от L. Нека $p(x)$ е минималният полином на α над P, а $\alpha=\alpha_1, \alpha_2, \ldots, \alpha_t$ са корените му в полето K. Полиномът $p(x)$ е неразложим над P и има корен α в нормалното разширение K на P. Затова полето K съдържа поле на разлагане M на полинома $p(x)$. Тъй като $M=P(\alpha_1, \alpha_2, \ldots, \alpha_t)$, $\alpha_1=\alpha$ и $L=P(\alpha)$, то подполето L се съдържа в подполето M. Елементите α_i са спрегнати с $\alpha=\alpha_1$ над P. От твърдение 3 на § 1 следва, че съществува такъв автоморфизъм $\sigma_i \in G$, че $\sigma_i(\alpha)=\alpha_i$ за $i=1, 2, \ldots, t$.

1. Да допуснем, че подгрупата H е нормален делител на групата G. Тогава за всяко $h \in H$ автоморфизмът $h_i=\sigma_i^{-1} h \sigma_i$ е също елемент на H. Понеже $\alpha \in L$, то α е неподвижен относно автоморфизмите от H и $\alpha=h_i(\alpha)=\sigma_i^{-1} h \sigma_i(\alpha)$, т. е. $h(\sigma_i(\alpha))=\sigma_i(\alpha)$ и

$$h(\alpha_i)=h(\sigma_i(\alpha))=\sigma_i^{h}(\alpha)=\alpha_i, \quad i=1, 2, \ldots, t.$$

Тъй като тези равенства са валидни за всеки автоморфизъм h от H, то корените $\alpha_1, \alpha_2, \ldots, \alpha_t$ на $p(x)$ се съдържат в неподвижното подполе L на подгрупата H. Но това показва, че полето L съвпада с полето на разлагане $M=P(\alpha_1, \alpha_2, \ldots, \alpha_t)$ на полинома $p(x)$ над P. Следователно L е нормално разширение на полето P.

2. Обратно, нека сега L е нормално разширение на P. В този случай $L=P(\alpha)=P(\alpha_1, \alpha_2, \ldots, \alpha_t)=M$. Според следствие 3 от § 1 изображението $\psi: G \to F=\mathrm{Gal}(L/P)$, което съпоставя на всеки автоморфизъм σ от G ограничението му $\sigma|_L=\psi(\sigma)$ върху L, е хомоморфизъм на групата G в групата F и $\ker\psi=\mathrm{Gal}(K/L)=H$. Следователно подгрупата H като ядро на хомоморфизъм е нормален делител на G.

Понеже K и L са нормални разширения на P и K е нормално разширение на L, то от теорема 4 б) следват равенствата $[K:P]=|G|$, $[L:P]=|F|$ и $[K:L]=|H|$. Като използуваме равенството $[K:P]=[K:L][L:P]$, получаваме $|F|=[L:P]=[K:P]/[K:L]=|G|/|H|=|G/H|$. От теоремата за хомоморфизмите (глава IV, теорема 10) знаем, че фактор-групата G/H е изоморфна на образа $\mathrm{Im}\psi$, който е подгрупа на F. Така получаваме съвпадението $\mathrm{Im}\psi=F$, т. е. G/H е изоморфна на F. Теоремата е доказана.

§ 4. Група на Галоа на композита на две полета

Ако полетата L и M са подполета на някое поле K, то минималното подполе на K, което съдържа едновременно полетата L и M, се нарича *композит* на L и M и се бележи с LM. Ясно е, че композитът LM съвпада с композита ML и е равен на сечението на всички подполета на K, които съдържат едновременно L и M.

Ако $K=LM$, то ще казваме, че полето K е *композит на подполетата си* L и M.

Твърдение 5. *Нека L и M са две междинни подполета на разширението K на полето P. Тогава*

а) *ако L и M са нормални разширения на P, то и композитът LM е нормално разширение на P,*

б) *ако σ е автоморфизъм на K над P, то композитът LM е неподвижно подполе относно σ тогава и само тогава, когато L и M едновременно са неподвижни подполета относно σ.*

Наистина ако L и M са нормални разширения на P, то те са полета на разлагане на два полинома $f(x)$ и $g(x)$ над P. Лесно се вижда, че композитът LM в този случай е поле на разлагане на полинома $f(x)g(x)$ над P, т. е. LM е също нормално разширение на P.

Ако K^σ е неподвижното поле на σ, то от определението на композита следва, че $LM\leqq K^\sigma$ тогава и само тогава, когато $L\leqq K^\sigma$ и $M\leqq K^\sigma$.

Твърдение 6. *Нормалното разширение K на основното поле P е композит на междинните си подполета L и M тогава и само тогава, когато* $\mathrm{Gal}(K/L)\cap\mathrm{Gal}(K/M)=\langle\varepsilon\rangle$, *където ε е тъждественият автоморфизъм на K.*

Доказателство. Да въведем означенията $G=\mathrm{Gal}(K/P)$, $H=\mathrm{Gal}(K/L)$ и $F=\mathrm{Gal}(K/M)$. Нека $K=LM$. Ако $\sigma\in H\cap F$, то L и M са неподвижни подполета относно σ. По предното твърдение композитът $K=LM$ е също неподвижен относно σ, т. е. $\sigma=\varepsilon$ и $H\cap F=\langle\varepsilon\rangle$.

Обратно, нека $H\cap F=\langle\varepsilon\rangle$. Тъй като $L\leqq LM$ и $M\leqq LM$, то подгрупата $E=\mathrm{Gal}(K/LM)$ на групата G се съдържа както в H, така и в F. Следователно $E=\langle\varepsilon\rangle$. Но подполето LM съвпада с неподвижното подполе на $E=\langle\varepsilon\rangle$, което очевидно е полето K. Твърдението е доказано.

Теорема 6. *Ако K е поле, $P \leqq L \leqq K$, $P \leqq M \leqq K$ и L е нормално разширение на полето P, то композитът $T = LM$ е нормално разширение на M и групата $H = \mathrm{Gal}(T/M)$ е изоморфна на подгрупа на групата $G = \mathrm{Gal}(L/P)$.*

Доказателство. Полето L по условие е поле на разлагане на някой полином $f(x)$ над полето P. Ако $a_1, a_2, \ldots, a_n$ са корените на $f(x)$ в L, то $L = P(a_1, a_2, \ldots, a_n)$. Да разгледаме полето $T_1 = M(a_1, a_2, \ldots, a_n)$. Тъй като коефициентите на $f(x)$ са елементи на полето M, то T_1 е поле на разлагане на $f(x)$ над M. Затова T_1 е нормално разширение на M. Но T_1 съвпада с композита $LM = T$. Наистина от $M \leqq T$ и $a_1, a_2, \ldots, a_n \in L \leqq T$ следва, че T_1 е подполе на T. За да получим и обратното включване, да забележим първо, че $P \leqq M \leqq T_1$ и $a_1, a_2, \ldots, a_n \in T_1$ показват, че $L = P(a_1, a_2, \ldots, a_n) \leqq T_1$. Но двете включвания $L \leqq T_1$ и $M \leqq T_1$ и определението на композита $T = LM$ ни дават включването $T \leqq T_1$. Така получаваме $T_1 = T$ и затова T е нормално разширение на полето M.

Ако σ е елемент на групата $H = \mathrm{Gal}(T/M)$, то σ оставя неподвижни коефициентите на полинома $f(x)$, защото те се съдържат в подполето P на неподвижното подполе M на H. Следователно $\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)$ е една пермутация на корените $a_1, a_2, \ldots, a_n$ на полинома $f(x)$. Понеже елементите на $L = P(a_1, a_2, \ldots, a_n)$ са полиноми на $a_1, a_2, \ldots, a_n$ с коефициенти от P, то σ изобразява подполето L в себе си, т. е. $\sigma(L) \leqq L$. Но L и $\sigma(L)$ са две крайномерни пространства над полето P и $\sigma : L \to \sigma(L)$ е изоморфизъм между тези пространства, тъй като P е неподвижно относно σ. Следователно $\sigma(L) = L$, т. е. ограничението $\psi(\sigma)$ на σ върху L е автоморфизъм на L над P. Затова $\psi(\sigma)$ е елемент на групата G, а $\psi : H \to G$ е хомоморфизъм на групата H в групата G. Ако $\sigma \in \ker \psi$, то $\psi(\sigma) = \varepsilon$ и по тази причина σ оставя неподвижни корените $a_1, a_2, \ldots, a_n \in L$. Но σ оставя неподвижни и елементите на M. По следствие 1 σ оставя неподвижни елементите на $M(a_1, a_2, \ldots, a_n) = T$. Следователно $\sigma = \varepsilon$ и $\ker \psi = \langle \varepsilon \rangle$. Така ψ е изоморфизъм на H върху $\psi(H)$ и групата H е изоморфна на подгрупата $\psi(H) = \mathrm{Im}\,\psi$ на групата G.

Забележка. Може да се докаже, че групата $H = \mathrm{Gal}(T/M)$ е изоморфна на подгрупата $\mathrm{Gal}(L/L \cap M)$ на групата G, но този факт няма да ни бъде необходим.

§ 5. Допълнителни сведения от теория на групите

А. Разрешими групи. Нека $\mu : G \to H$ е произволен хомоморфизъм на групата G в групата H. Да напомним, че μ се нарича *мономорфизъм* (*влагане, инективен хомоморфизъм, инекция*) на G в H, ако μ изобразява различни елементи от G в различни елементи на H, а ако μ е хомоморфизъм на G върху H, то μ се нарича *епиморфизъм* (*сюрекция*).

Ясно е, че хомоморфизмът μ е изоморфизъм на G върху H

точно тогава, когато μ е едновременно мономорфизъм и епиморфизъм.

Задача 1. Да се докаже, че хомоморфизмът μ е мономорфизъм тогава и само тогава, когато ядрото $\ker \mu$ е единичната подгрупа на G.

Ако F е произволна подгрупа на G и $\nu = \mu|_F$ е ограничението (рестрикцията) на μ върху F, то ν е хомоморфизъм на F в H с ядро $\ker \nu = F \cap \ker \mu$ и образ $\operatorname{Im}\nu = \nu(F) = \mu(F)$, който е подгрупа на групата H. Хомоморфизмът ν е епиморфизъм на групата F върху образа $\operatorname{Im}\nu$. Той е мономорфизъм точно тогава, когато е изпълнено равенството $F \cap \ker \mu = \{e\}$.

Твърдение 7. *Ако G е група, $A \leqq G$ и $B \lhd G$, то $AB \leqq G$, $A \cap B \lhd A$ и $AB/B \cong A/(A \cap B)$.*

Доказателство. От $A \leqq G$ и $B \lhd G$ по твърдение 4 на глава IV следва, че $AB \leqq G$. Освен това $B \lhd AB$ и непосредствено се вижда, че изображението $\varphi : A \to AB/B$, дефинирано с $\varphi(a) = aB$ за $a \in A$, е хомоморфизъм с ядро $\ker \varphi = A \cap B$. Следователно $A \cap B \lhd A$.

Ако gB е произволен елемент на фактор-групата AB/B ($g \in AB$) то $g = ab$, $a \in A$, $b \in B$. Тъй като $a^{-1}g = b \in B$, то $gB = aB = \varphi(a)$ т. е φ е епиморфизъм на A върху AB/B. От теоремата за хомоморфизмите за групи следва, че $A/A \cap B = A/\ker \varphi \cong \operatorname{Im}\varphi = AB/B$. Твърдението е доказано.

Ако $\mu : G \to H$ е хомоморфизъм на групата G в групата H, а B е подгрупа на H, то множеството на всички елементи на g от G, за които $\mu(g) \in B$, се нарича *пълен праобраз* на подгрупата B при хомоморфизма μ и се бележи с $\mu^{-1}(B)$. Единичният елемент на G се съдържа в $\mu^{-1}(B)$, тъй като хомоморфизмът го изобразява в единичния елемент на H, който се съдържа във всяка подгрупа B на H. Ако $\mu(g_1) = b_1 \in B$ и $\mu(g_2) = b_2 \in B$, то $\mu(g_1 g_2^{-1}) = \mu(g_1)\mu(g_2)^{-1} = b_1 b_2^{-1} \in B$, т. е. $g_1 g_2^{-1} \in \mu^{-1}(B)$ и пълният праобраз на подгрупата B на групата H е подгрупа на G. Ясно е, че $\mu(\mu^{-1}(B))$ е подгрупа на H, която се съдържа в подгрупата B. В общия случай тази подгрупа не съвпада с B.

Задача 2. а) Да се докаже, че от $B \lhd H$ следва $\mu^{-1}(B) \lhd G$.

б) Да се докаже, че равенството $B = \mu(\mu^{-1}(B))$ е изпълнено точно тогава, когато $B \leqq \operatorname{Im}\mu = \mu(G)$.

Твърдение 8. *Нека $\mu : G \to H$ е хомоморфизъм на групи, $A \lhd C \leqq G$, $B \lhd D \leqq H$, $\mu(A) \leqq B$ и $\mu(C) \leqq D$. Тогава съществува хомоморфизъм $\bar{\mu} : C/A \to D/B$ на посочените фактор-групи, дефиниран с равенството*

$$\bar{\mu}(cA) = \mu(c)B, \quad c \in C. \tag{1}$$

Освен това:

а) *хомоморфизмът $\bar{\mu}$ е епиморфизъм на C/A върху D/B точно тогава, когато $D = \mu(C)B$;*

б) *хомоморфизъм $\bar{\mu}$ е мономорфизъм точно тогава, когато е изпълнено равенството $A = C \cap \mu^{-1}(B)$.*

Доказателство. Ако $cA=c_1A$, $c, c_1 \in C$, то $c^{-1}c_1 \in A$ и затова $\mu(c^{-1}c_1)=\mu(c)^{-1}\mu(c_1) \in \mu(A) \leqq B$. Но от $\mu(c)^{-1}\mu(c_1) \in B$ следва равенството $\mu(c)B=\mu(c_1)B$, което показва, че определението на μ не зависи от конкретния представител c на съседния клас cA, т. е. $\bar{\mu}$ е коректно определено чрез формула (1) и е изображение на групата C/A в групата D/B.

Изображението $\bar{\mu}$ е хомоморфизъм на групи. Наистина ако cA и $c'A$ са два елемента на групата C/A, то $\bar{\mu}(cAc'A)=\bar{\mu}(cc'A)=$ $=\mu(cc')B=\mu(c)\mu(c')B=\mu(c)B \cdot \mu(c')B=\bar{\mu}(cA)\bar{\mu}(c'A)$.

а) Да допуснем, че $D=\mu(C)B$. Ако dB е произволен елемент на фактор-групата D/B, то съществуват такива $c \in C$ и $b \in B$, че $d=\mu(c)b$. Тогава $\mu(c)B=\mu(c)bB=dB$ и затова $\bar{\mu}(cA)=\mu(c)B=dB$, т. е. $\bar{\mu}$ е епиморфизъм.

Обратно, ако $\bar{\mu}$ е епиморфизъм, то ще покажем, че $D=$ $=\mu(C)B$. Да допуснем, че това равенство не е вярно. Тогава от условията на твърдението следва включването $\mu(C)B<D$. Затова съществува елемент $d \in D$, който не се съдържа в произведението $\mu(C).B$. Да разгледаме елемента dB на фактор-групата D/B. Тъй като по условие $\bar{\mu}$ е епиморфизъм, то $dB=\mu(cA)$ за някой елемент cA от C/A. Но равенството $\mu(c)B=dB$ показва, че $d=\mu(c)b$ за някой елемент $b \in B$. Тогава $d \in \mu(C)B$, което противоречи на избора на елемента d. Полученото противоречие доказва равенството $D=\mu(C)B$.

б) Ще отбележим най-напред, че от условията $A \leqq C$ и $\mu(A) \leqq$ $\leqq B$ следва включването $A \leqq C \cap \mu^{-1}(B)$.

Нека $\bar{\mu}$ е мономорфизъм, а $x \in C \cap \mu^{-1}(B)$. Да разгледаме съседния клас $xA \in C/A$. Тъй като $\mu(x) \in B$ и $\bar{\mu}(xA)=\mu(x)B$, то $\bar{\mu}(xA)=B$, където B е единичният елемент на фактор-групата D/B. Така елементът xA е от ядрото $\ker \bar{\mu}$, което в разглежданията случай е единичната подгрупа на фактор-групата C/A. Следователно $x \in A$, т. е. изпълнено е равенството $A=C \cap \mu^{-1}(B)$.

Обратно, нека $A=C \cap \mu^{-1}(B)$. Ако $yA \in \ker \bar{\mu}$, $y \in C$, то $\bar{\mu}(yA)=$ $=\mu(y)B=B$ и затова $\mu(y) \in B$, т. е. $y \in \mu^{-1}(B)$. Тъй като y е елемент на C, то $y \in C \cap \mu^{-1}(B)=A$. Но $y \in A$ показва, че $yA=A$. Следователно ядрото $\ker \bar{\mu}$ съвпада с единичната подгрупа $\{A\}$ на фактор-групата C/A и $\bar{\mu}$ е мономорфизъм. Твърдението е доказано.

Следствие 7. *Нека $\mu: G \to H$ е хомоморфизъм на групата G в групата H и $A \lhd C \leqq G$. Тогава $\mu(A) \lhd \mu(C)$ и фактор-групата $\mu(C)/\mu(A)$ е хомоморфен образ на фактор-групата C/A. Ако C/A е абелева група, то и фактор-групата $\mu(C)/\mu(A)$ е абелева.*

Доказателство. Непосредствено се проверява, че $\mu(A) \lhd$ $\mu(C)$. Нека $B=\mu(A)$ и $D=\mu(C)$. Според предното твърдение съществува хомоморфизъм $\bar{\mu}: C/A \to D/B$, който е епиморфизъм,

понеже $\mu(C)B=\mu(C)\mu(A)=\mu(CA)=\mu(C)=D$. Следователно факторгрупата D/B е хомоморфен образ на C/A. Тъй като всеки хомоморфен образ на абелева група е също абелева група, то от комутативността на групата C/A следва комутативност на нейния хомоморфен образ D/B.

Следствие 8. *Нека $\mu: G\to H$ е хомоморфизъм на групата G в групата H и $B\lhd D\leqq H$. Тогава $\mu^{-1}(B)\lhd\mu^{-1}(D)$ и изображението $\bar{\mu}:\mu^{-1}(D)/\mu^{-1}(B)\to D/B$, дефинирано с $\bar{\mu}(c\mu^{-1}(B))=\mu(c)B$ за всяко $c\in\mu^{-1}(D)$, е мономорфизъм. Ако фактор-групата D/B е абелева, то фактор-групата $\mu^{-1}(D)/\mu^{-1}(B)$ е също абелева.*

Доказателство. Тъй като $B\leqq D$, то $A=\mu^{-1}(B)\leqq\mu^{-1}(D)=C$, т. е. A е подгрупа на групата C. Нека $a\in A$ и $c\in C$. Тогава $\mu(a)=b\in B$, $\mu(c)=d\in D$ и $\mu(c^{-1}ac)=\mu(c)^{-1}\mu(a)\mu(c)=d^{-1}bd\in B$, тъй като по условие B е нормален делител на D. Следователно елементът $c^{-1}ac$ се съдържа в $A=\mu^{-1}(B)$, т. е. A е нормален делител на C.

Условията на твърдение 8 са изпълнени, тъй като $\mu(A)=\mu(\mu^{-1}(B))\leqq B$ и $\mu(C)=\mu(\mu^{-1}(D))\leqq D$. Освен това $A=C\cap A=C\cap\mu^{-1}(B)$. Следователно съществува мономорфизъм $\bar{\mu}: C/A\to D/B$, който се определя с посочената формула.

Ако D/B е абелева група, то нейната подгрупа $\bar{\mu}(C/A)$ е също абелева. Понеже групата C/A е изоморфна на $\bar{\mu}(C/A)$, то и C/A е абелева група. Следствието е доказано.

Твърдение 9. *Нека G е група, $A\leqq G$ и $B\lhd C\leqq G$. Тогава $A\cap B\lhd A\cap C$ и фактор-групата $A\cap C/A\cap B$ е изоморфна на подгрупа на фактор-групата C/B. Ако C/B е абелева група, то и групата $A\cap C/A\cap B$ е абелева.*

Доказателство. Нека $\varphi: C\to C/B$ е естественият хомоморфизъм на групата C върху нейната фактор-група C/B, а ψ е ограничението на φ върху подгрупата $A\cap C$ на C. Тогава

$$\ker\psi=(A\cap C)\cap\ker\varphi=(A\cap C)\cap B=A\cap(C\cap B)=A\cap B.$$

Понеже $A\cap B$ е ядро на хомоморфизъм на групата $A\cap C$, то тя е нормален делител на $A\cap C$. От теоремата за хомоморфизмите следва, че фактор-групати $A\cap C/\ker\psi=A\cap C/A\cap B$ е изоморфна на $\operatorname{Im}\psi=\varphi(A\cap C)$, която е подгрупа на C/B.

Ако C/B е абелева, то нейната подгрупа $\operatorname{Im}\psi$ е абелева и изоморфната ѝ група $A\cap C/A\cap B$ е също абелева. Твърдението е доказано.

Определение 6. Всяка крайна намаляваща редица

$$G=G_0\geqq G_1\geqq\ldots\geqq G_n=\{e\} \tag{2}$$

от подгрупи на групата G, където $G_i\lhd G_{i-1}$ $(i=1, 2, \ldots, n)$, се нарича *нормален ред* на G, а фактор-групите G_{i-1}/G_i $(i=1, 2, \ldots, n)$ се наричат *фактори* на този ред.

Да отбележим, че в нормалния ред (2) на G подгрупата G_1 непременно е нормален делител на G, но $G_2, G_3, \ldots, G_{n-1}$ не са задължени да са нормални делители на G. Освен това в реда (2)

може да имаме на някои места повторение, т. е. G_i не е непременно различна от G_{i-1}.

Определение 7. Групата G се нарича *разрешима*, ако тя притежава нормален ред с абелеви фактори, а всеки такъв ред се нарича *разрешим ред*.

Например всяка абелева група A е разрешима, тъй като $A = A_0 \geqq A_1 = \{e\}$ е нормален ред на A с абелев фактор A_0/A_1, който е изоморфен на A.

Твърдение 10. *Всяка подгрупа на разрешима група е разрешима група.*

Доказателство. Нека G е разрешима група, а H е подгрупа на G. Групата G има нормален ред (2) с абелеви фактори G_{i-1}/G_i $(i=1, 2, \ldots, n)$. Да положим $H_i = H \cap G_i$ за $i=0, 1, \ldots, n$ и да разгледаме намаляващата редица от подгрупи

$$H = H_0 \geqq H_1 \geqq \ldots \geqq H_n = \{e\}. \tag{3}$$

От твърдение 9 следва, че $H_i = H \cap G_i$ е нормален делител на $H_{i-1} = H \cap G_{i-1}$, и понеже G_{i-1}/G_i е абелева група, то факторгрупата H_{i-1}/H_i е също абелева група. Следователно (3) е разрешим ред на H, т. е. H е разрешима група.

Твърдение 11. *Хомоморфен образ на разрешима група е разрешима група.*

Доказателство. Нека групата F е хомоморфен образ на разрешимата група G и нека $\mu: G \to F$ е епиморфизъм на G върху F. Групата G притежава нормален ред (2) с абелеви фактори. Полагаме $F_i = \mu(G_i)$ за $i=0, 1, \ldots, n$. Понеже $\mu(G) = F$ и $\mu(G_n) = \{e\}$, то $F = F_0$ и $F_n = \{e\}$. Да разгледаме намаляващата редица

$$F = F_0 \geqq F_1 \geqq \ldots \geqq F_n = \{e\} \tag{4}$$

от подгрупи на F. Тъй като G_i е нормален делител на G_{i-1}, то по следствие 7 F_i е нормален делител на F_{i-1}, а факторът F_{i-1}/F_i е абелева група, понеже G_{i-1}/G_i е абелева група. Следователно (4) е разрешим ред на F, т. е. F е разрешима група. Твърдението е доказано.

Твърдение 12. *Групата G е разрешима тогава и само тогава, когато някой неин нормален делител H и факторгрупата G/H са разрешими групи.*

Доказателство. Ако G е разрешима, то според предните две твърдения подгрупата H на G и хомоморфният образ G/H на G са разрешими групи.

Обратно, да допуснем, че някой нормален делител H и фактор-групата G/H са разрешими групи. Тогава те притежават разрешими редове

$$H = H_0 \geqq H_1 \geqq \ldots \geqq H_n = \{e\},$$
$$G/H = F_0 \geqq F_1 \geqq \ldots \geqq F_m = \{H\}.$$

Нека $\varphi: G \to G/H$ е естественият хомоморфизъм на G върху нейната фактор-група G/H. Полагаме $G_i = \varphi^{-1}(F_i)$ за $i=0, 1, \ldots, n$.

и $G_i = H_{i-m}$ за $i = m+1,\ m+2, \ldots, m+n$. Получаваме крайната намаляваща редица

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m \supseteq G_{m+1} \supseteq \ldots \supseteq G_{m+n} = \{e\} \tag{5}$$

от подгрупи на G. Съгласно следствие 8 в тази редица при $1 \leqq i \leqq m$ групата $G_i = \varphi^{-1}(F_i)$ е нормален делител на $G_{i-1} = \varphi^{-1}(F_{i-1})$ и G_{i-1}/G_i е абелева група, а при $m+1 \leqq i \leqq m+n$ имаме $G_{i-1} = H_{i-m-1}$ и $G_i = H_{i-m}$, т. е. и в този случай G_i е нормален делител на G_{i-1} с абелева фактор-група $G_{i-1}/G_i = H_{i-m-1}/H_{i-m}$. Следователно групата G има разрешим ред (5), т. е. G е разрешима група. Твърдението е доказано.

Б. Крайни разрешими групи. Подгрупата M на групата G се нарича *максимална* (*в* G), ако $M \neq G$ и ако от $M \leqq H \leqq G$ следва $H = M$ или $H = G$, т. е. M и G са единствените подгрупи на G, които съдържат M.

Очевидно единичната група няма максимални подгрупи, а всяка неединична крайна група притежава поне една максимална подгрупа. Една безкрайна група не е задължена да има максимални подгрупи. Например адитивната група $(\mathbf{Q}, +)$ на полето на рационалните числа не притежава максимални подгрупи.

Една максимална подгрупа в групата G невинаги е нормален делител на G.

Задача 3. Да се провери, че всяка силова 2-подгрупа на симетричната група S_3 е максимална подгрупа на S_3, но не е нормален делител на S_3.

Лема 4. *а) Единичната подгрупа $E = \{e\}$ на групата G е максимална в G тогава и само тогава, когато G е циклична група от прост ред.*

б) *Ако M е максимална подгрупа в G и $M \lhd G$, то факторгрупата G/M е циклична от прост ред.*

Доказателство. а) Ако редът на G е просто число, то по следствие 7 на глава IV G е циклична група и се поражда от всеки свой неединичен елемент. В този случай очевидно групата G има точно две подгрупи, а единичната подгрупа E е максимална в G.

Обратно, нека $E = \{e\}$ е максимална в G. Тогава $G \neq E$. Ако g е неединичен елемент на G, то $\langle g \rangle \neq E$ и $E \leqq \langle g \rangle \leqq G$. Следователно $G = \langle g \rangle$, т. е. G е циклична група и тя се поражда от всеки свой неединичен елемент. Цикличната група G има само две подгрупи E и G. Тя не може да бъде безкрайна циклична група, тъй като в последната има безброй много подгрупи. Като приложим теорема 3 на глава IV към крайната циклична група G получаваме, че нейният ред е просто число.

б) Ако $\varphi : G \to \bar{G} = G/M$ е естественият епиморфизъм, а B е подгрупа на $\bar{G}$, то $A = \varphi^{-1}(B)$ е подгрупа на G, за която имаме $M \leqq A \leqq G$. Тъй като M е максимална подгрупа в G, то в сила е точно едно от равенствата $A = M$, $A = G$. Когато $A = M$, то $B = \varphi(A) = \{M\}$ е единичната подгрупа на $\bar{G}$, а когато $A = G$, то

$B=\varphi(A)=\bar{G}$. Следователно групата $\bar{G}$ има точно две подгрупи, а единичната подгрупа на $\bar{G}$ е максимална в $\bar{G}$. По твърдение а) фактор-групата $\bar{G}$ е циклична от прост ред. Лемата е доказана.

Твърдение 13. а) *Ако* $H \triangleleft G$, $H \leqq M \leqq G$ *и фактор-групата* G/H *е абелева, то* $M \triangleleft G$.

б) *Ако* G *е неединична разрешима група, то в* G *съществува нормален делител* H, *такъв, че фактор-групата* G/H *е неединична абелева група.*

Доказателство. а) Нека $\varphi: G \to G/H$ е естественият епиморфизъм, $g \in G$ и $f \in M$. Тогава от комутативността на G/H следва. че $g^{-1}fgH = \varphi(g^{-1}fg) = \varphi(g)^{-1}\varphi(f)\varphi(g) = \varphi(g)^{-1}\varphi(g)\varphi(f) = \varphi(f) = fH$, т. е. $f^{-1}g^{-1}fg = h \in H \leqq M$. Затова $g^{-1}fg = fh \in M$ за всяко $f \in M$ и всяко g от G. Това показва, че $M \triangleleft G$.

б) Разрешимата група G има разрешим ред (2). По условие $G \neq G_n = \{e\}$. Нека i е най-малкото естествено число $(1 \leqq i \leqq n)$, такова, че $G \neq G_i$. Полагаме $H = G_i$. Тогава $G = G_0 = G_1 = \ldots = G_{i-1}$ и $G \neq G_i = H$. Тъй като $H = G_i \triangleleft G_{i-1}$ и $G_{i-1} = G$, то H е нормален делител в G, а $G/H = G_{i-1}/G_i$ е неединична абелева група. Твърдението е доказано.

Твърдение 14. *Всяка крайна неединична разрешима група* G *има поне една максимална подгрупа, която е нормален делител на* G.

Наистина според твърдение 13 б) в G има нормален делител H, такъв, че фактор-групата G/H е неединична абелева група. Тъй като $H \neq G$, а G е крайна група, то в G съществува максимална подгрупа M, която съдържа H. От предното твърдение следва, че $M \triangleleft G$.

Теорема 7. *Неединичната крайна група* G е *разрешима тогава и само тогава, когато тя има нормален ред с циклични фактори от прости редове.*

Доказателство. Ако групата G има нормален ред с циклични фактори от прости редове, то този ред е разрешим (тъй като цикличните групи са абелеви) и G е разрешима група.

Обратно, нека G е разрешима група. Ще проведем тази част на доказателството на теоремата с индукция по реда $n = |G|$ на групата G. Тъй като G е неединична, то $n \geqq 2$. Ако $n = 2$, то $G = G_0 > \{e\} = G_1$ е нормален ред в G с единствен цикличен фактор $G_0/G_1 \cong G$ от ред 2. Нека $n \geqq 2$ и теоремата да е вярна за групите с редове, по-малки от n. Полагаме $G = G_0$. Според твърдение 14 в G съществува максимална подгрупа G_1, която е нормален делител в G, а според лема 4 б) фактор-групата G_0/G_1 е циклична от прост ред.

Ако $G_1 = \{e\}$, то $G = G_0 > G_1 = \{e\}$ е нормален ред на G с единствен цикличен фактор от прост ред. Нека G_1 е неединична подгрупа на G. Тя е разрешима група (твърдение 10) и има ред, по-малък от n. По предположение на индукцията в G_1 има нормален ред $G_1 > G_2 > \ldots > G_n = \{e\}$ с циклични фактори от прости редове. Но тогава очевидно $G = G_0 > G_1 > \ldots > G_n = \{e\}$ е нормален ред в

G с циклични фактори от прости редове. Теоремата е доказана.

Да напомним, че една крайна група G се нарича *p-група*, ако p е просто число и редът на G е степен на числото p.

Твърдение 15. *Всяка крайна p-група е разрешима група.*

Доказателство. Нека G е крайна p-група. Тогава $|G|=p^n$ за някое $n\geqq 0$. Ако $n=0$, то G е единичната група и тя е разрешима. Ще проведем доказателството с индукция по n. Нека $n>0$ и за p-групите с ред, по-малък от p^n, твърдението е вярно. Да разгледаме центъра $C(G)$ на групата G. Според теорема 11 на глава IV $C(G)$ е неединична подгрупа на G, т. е. $|C(G)|>1$. Понеже центърът $C(G)$ се състои от елементите на G, които комутират с всички елементи на G, то $C(G)$ е абелев нормален делител на G. От $|C(G)|>1$ следва, че фактор-групата $G/C(G)$ има ред $m<p^n$. Освен това редът m дели p^n, т. е. $m=p^k$, $k<n$. Следователно $G/C(G)$ е крайна p-група от ред, по-малък от p^n. По индукционното предположение тази фактор-група е разрешима. Но тогава според твърдение 12 групата G също е разрешима. Твърдението е доказано.

Като се използуват теоремите на Силов (глава IV, § 10), може да се докаже, че всяка крайна група от ред, по-малък от 60, е разрешима. Както ще покажем по-нататък, алтернативната група A_5, която е от ред 60, не е разрешима, т. е. тя е най-малката крайна група, която не е разрешима.

Да разгледаме симетричната група S_4. В нея алтернативната група A_4 има индекс 2 и е нормален делител от ред 12. Лесно се проверява, че единичната субституция e заедно със субституциите $a=(12)\,(34)$, $b=(14)\,(13)$ и $c=(13)\,(24)$ образуват абелев нормален делител B_4 на S_4, който се съдържа в A_4. Фактор-групата A_4/B_4 е от ред 3 и затова е абелева. Следователно редът $S_4>A_4>B_4>\{e\}$ е разрешим ред на S_4, а S_4 е разрешима група.

Твърдение 15. *Симетричните групи S_1, S_2, S_3, S_4 и алтернативните групи A_1, A_2, A_3, A_4 са разрешими групи.*

Наистина вече установихме, че групата S_4 е разрешима. Понеже указаните в твърдението групи са изоморфни на подгрупи на S_4, то по твърдение 10 те също са разрешими.

Да разгледаме сега симетричните групи S_n при $n\geqq 5$. Да напомним, че троен цикъл или цикъл с дължина 3 от S_n е субституция σ, която мести циклично 3 различни числа, а останалите числа ги оставя неподвижни (вж. § 2 на глава IV).

Лема 5. *Ако $H\lhd G\leqq S_n$, $n\geqq 5$, ако G съдържа тройните цикли на S_n и ако фактор-групата G/H е абелева, то и H съдържа тройните цикли на S_n.*

Доказателство. Нека $\varphi: G\to G/H$ е естественият хомоморфизъм и $g=(ijk)\in G$ е произволен троен цикъл. Тъй като $n\geqq 5$, то съществуват две естествени числа s и t $(1\leqq s<t\leqq n)$, които са различни от i, j и k. Тройните цикли $g_1=(sji)$ и $g_2=(itk)$ са елементи на групата G. Да разгледаме елемента $g_3=g_1^{-1}g_2^{-1}g_1g_2$. Тъй като по условие фактор-групата G/H е комутативна, то $\varphi(g_3)=$

$=\varphi(g_1)^{-1}\varphi(g_2)^{-1}\varphi(g_1)(g_2)=\bar{e}$, където $\bar{e}=H$ е единичният елемент на G/H. Следователно елементът g_3 се съдържа в $\ker\varphi=H$. Но

$$g_3=(ijs)(kti)(sji)(itk)=(ijk)=g,$$

т. е. тройният цикъл $g=(ijk)$ се съдържа в H. Лемата е доказана.

Следствие 9. *Ако подгрупата G на симетричната група S_n при $n\geqq 5$ съдържа тройните цикли на S_n, то групата G не е разрешима.*

Доказателство. Нека G съдържа всеки троен цикъл и да допуснем, че G е разрешима група. Тогава G има разрешим ред $G=G_0\geqq G_1\geqq\ldots\geqq G_s=\{e\}$. Понеже G/G_1 е абелева група, то по предната лема G_1 също съдържа всеки троен цикъл. Ако вече сме получили, че подгрупата G_{t-1} съдържа всеки троен цикъл, то от комутативността на фактор-групата G_{t-1}/G_t и от лемата следва, че всеки троен цикъл се съдържа в G_t. Следователно всеки троен цикъл се съдържа в $G_s=\{e\}$, което е невъзможно. Следователно G не е разрешима група. Следствието е доказано.

Теорема 8. *Алтернативната група A_n и симетричната група S_n при $n\geqq 5$ не са разрешими групи.*

Наистина всеки троен цикъл е четна субституция и затова той се съдържа в $A_n\leqq S_n$. Затова по предното следствие групите A_n и S_n не са разрешими групи.

Накрая ще построим една серия от крайни разрешими групи, които ще ни бъдат необходими по-нататък.

Ако $n\geqq 2$ е естествено число, то съгласно означенията в § 3 на глава V $n\mathbf{Z}=(n)$ е главният идеал на пръстена $\mathbf{Z}$ от всички цели числа, които се делят на n, а $\mathbf{Z}_n$ е фактор-пръстенът $\mathbf{Z}/(n)$. Тук ще бъде по-удобно съседният клас $m+(n)$ да означаваме с $[m]$. Пръстенът $\mathbf{Z}_n$ се състои от съседните класове $[0], [1], \ldots, [n-1]$ и неговата адитивна група $\mathbf{Z}_n(+)$ е циклична група от ред n. Мултипликативната група $\mathbf{Z}_n^*$ е от ред $\varphi(n)$, където φ е функцията на Ойлер. Класът $[m]$ се съдържа в $\mathbf{Z}_n^*$ тогава и само тогава, когато n и m са взаимно прости числа. Двете групи $\mathbf{Z}_n(+)$ и $\mathbf{Z}_n^*(\,.\,)$ са абелеви и затова те са разрешими. Да отбележим че групата $\mathbf{Z}_n^*$ в общия случай не е циклична. Както споменахме в § 10 на глава VII, тя е циклична тогава и само тогава, когато n е равно на една от числата 2, 4, p^k и $2p^k$ ($k\geqq 1$), където p е нечетно просто число.

Да означим сега с V множеството на тези наредени двойки (a, b) от цели числа, за които a и n са взаимно прости. Нека D_n е декартовото произведение на множествата $\mathbf{Z}_n^*$ и $\mathbf{Z}_n$, т. е. D_n е множеството на наредените двойки $([a], [b])$ от съседни класове по модул n, където $[a]\in\mathbf{Z}_n^*$ и $[b]\in\mathbf{Z}_n$. Множеството D_n има точно $n\varphi(n)$ различни елемента. Нека $f: V\to D_n$ е изображението, което съпоставя на всяко $(a, b)\in V$ елемента $([a], [b])$ от D_n. Ясно е, че f изобразява множеството V върху множеството D_n.

Тъй като D_n има $n\varphi(n)$ елемента, то с помощта на изображението f множеството V се разбива на $n\varphi(n)$ различни класа: *два елемента* (a, b) и (a_1, b_1) *попадат в един и същ клас точно тогива, когато* $f((a, b))=f((a_1, b_1))$, *т. е. когато* $[a]=[a_1]$ и $[b]=[b_1]$. Единственият клас, на който принадлежи $(a, b)\in V$, ще бележим с $[a, b]$, а множеството на така получените $n\varphi(n)$ класа ще бележим с M_n. Ако $[a, b]\in M_n$, то $a, b\in Z$ и $(a, n)=1$. *Два елемента* $[a, b]$ *и* $[a_1, b_1]$ *от* M_n *са равни тогава и само тогава, когато числото* n *дели едновременно разликите* $a-a_1$ *и* $b-b_1$. Двойката (a, b) се нарича *представител* на класа $[a, b]$.

В множеството M_n определяме умножение с формулата

$$[a, b][c, d]=[ac, ad+b].$$

Понеже от $(a, n)=1$ и $(c, n)=1$, следва, че $(ac, n)=1$, то в дясната страна на определящото равенство се намира коректно определен елемент на M_n.

Задача 4. Докажете, че горната формула определя коректно операция умножение в M_n, т. е. докажете, че ако $[a, b]=[a_1, b_1]$ и $[c, d]=[c_1, d_1]$, то $[ac, ad+b]=[a_1c_1, a_1d_1+b_1]$.

Относно така определеното умножение множеството M_n е група. Единицата на тази група е класът $[1, 0]$, а обратният $[a, b]^{-1}$ на класа $[a, b]$ в M_n се определя с формулата $[a, b]^{-1}=[c, -cb]$, където c е цяло число, за което $[c]=[a]^{-1}$ в Z_n^*.

Групата M_2 е от ред 2 и е абелева, но при $n>2$ групата M_n не е абелева.

От определението на елементите и операцията на групата M_n следва, че формулата $\psi([a, b])=[a]$ определя хомоморфизъм на групата M_n върху групата Z_n^*. Ако N_n е ядрото $\ker\psi$ на този хомоморфизъм, то по теоремата за хомоморфизмите фактор-групата M_n/N_n е изоморфна на абелевата група Z_n^*. Ядрото N_n се състои от всички класове от вида $[1, b]$, които са точно n на брой. Нека μ е изображението, което на класа $[1, b]$ съпоставя елемента $[b]$ от Z_n. Тогава μ е взаимно еднозначно изображение на N_n върху Z_n и

$$\mu([1, b][1, b_1])=\mu([1, b+b_1])=[b+b_1]$$

$$=[b]+[b_1]=\mu([1, b])+\mu([1, b_1]).$$

Следователно изображението μ е изоморфизъм на мултипликативната група N_n върху цикличната адитивна група Z_n. Тъй като $\mu([1, 1])=[1]$ е образуващ на Z_n, то $[1, 1]$ е образуващ на цикличната група N_n.

Елементите от вида $[a, 0]$ образуват подгрупа B_n в M_n, която е абелева и изоморфно се изобразява чрез ψ върху групата Z_n^*. Лесно се вижда, че $M_n=B_nN_n$ и $B_n\cap N_n=\{[1, 0]\}$.

По такъв начин получихме

Твърдение 17. *Ако* n *е естествено число,* $n\geqq 2$, *то*

а) *Подмножеството* $B_n=\{[a, 0] \mid a\in Z, (a, n)=1\}$ *на групата* M_n *е подгрупа, която е изоморфна на мултипликативната група* Z_n^* *на пръстена* Z_n *от остатъците по модул* n,

б) *Подмножеството* $N_n=\{[1, b] \mid b\in Z\}$ *на* M_n *е циклична нормален делител на групата* M_n, *фактор-групата* $M_n/N_n\cong Z_n^*$ *и нормалният делител* N_n *е изоморфен на адитивната група на пръстена* Z_n. *Елементът* $[1, 1]$ *е пораждащ елемент на цикличната група* N_n, *а* $M_n=B_nN_n$ *и* $B_n\cap N_n=\{[1, 0]\}$ *е единичната подгрупа на* M_n,

в) *Редът* $M_n\geqq N_n\geqq\{[1, 0]\}$ *е разрешим ред на* M_n, *а* M_n *е разрешима група*.

§ 6. Прости радикални разширения

Разширението K на полето P се нарича *просто радикално разширение* на P, ако K е поле на разлагане на полином от вида $f(x)=x^n-a$, $0\neq a\in P$.

Нека L е поле на разлагане на полинома $g(x)=x^n-1$ над полето K и $\zeta\in L$ е примитивен n-ти корен на единицата (ζ е образуващ на мултипликативната група от n-тите корени на единицата). Ако $\theta\in K$ е един от корените на $f(x)$ в K, които са точно n на брой, то елементите

$$\theta_1=\theta=\theta\zeta^0,\ \theta_2=\theta\zeta,\ \ldots,\ \theta_n=\theta\zeta^{n-1}$$

от K изчерпват корените на $f(x)$ и $K=P(\theta_1, \theta_2, \ldots, \theta_n)$. Очевидно $P(\theta_1, \theta_2, \ldots, \theta_n)\leqq P(\theta, \zeta)$. Обратното включване следва от $\zeta=\theta_2\theta_1^{-1}\in P(\theta_1, \theta_2, \ldots \theta_n)$. Следователно

$$K=P(\theta, \zeta)=L.$$

Ако полето P е такова, че полиномът $g(x)=x^n-1$ се разлага на линейни множители над P, т. е. P съдържа примитивен n-ти корен на единицата, то тогава $K=P(\theta)$. Ако пък $a=1$, то $f(x)=g(x)=x^n-1$ и $K=P(\zeta)$.

Нека $G=\mathrm{Gal}(K/P)$ е групата на Галоа на простото радикално разширение $K=P(\zeta, \theta)$ на полето P, а σ е произволен автоморфизъм от G. Тъй като σ е автоморфизъм и на цикличната група $\langle\zeta\rangle=\{1, \zeta, \ldots, \zeta^{n-1}\}$ от n-тите корени на единицата, то $\sigma(\zeta)$ е също примитивен n-ти корен на единицата. Следователно $\sigma(\zeta)=\zeta^a$, където a е взаимно просто с n.

Елементът $\sigma(\theta)$ е също корен на полинома $f(x)=x^n-a$ и затова той има вида $\sigma(\theta)=\zeta^b\theta$, където b е цяло число.

По този начин на елемента σ от G се съпоставя наредената двойка цели числа (a, b), където a и n са взаимно прости. Това съпоставяне обаче не е единозначно. Ако (a_1, b_1) е друга такава наредена двойка цели числа, че a_1 и n са взаимно прости и $\zeta^a=\zeta^{a_1}$, $\zeta^b=\zeta^{b_1}$, то тя съответствува на същия автоморфизъм σ. Но равенствата $\zeta^a=\zeta^{a_1}$, $\zeta^b=\zeta^{b_1}$ са изпълнени точно тогава, когато числото n дели едновременно двете разлики $a-a_1$ и $b-b_1$.

понеже ζ е примитивен n-ти корен от единицата. Затова на елемента σ от G ще съответствува елемент $[a, b]$ на групата M_n, която определихме в края на предния параграф. Да означим това съответствие на групата $G=\mathrm{Gal}(K/P)$ в групата M_n с ψ, т. е.

$$\psi(\sigma)=[a, b],$$

където $\sigma(\zeta)=\zeta^a$, $\sigma(\theta)=\zeta^b\theta$ и $(a, n)=1$.

Ако $\psi(\tau)=[c, d]$, то тогава

$$\sigma\tau(\zeta)=\sigma(\zeta^c)=\sigma(\zeta)^c=\zeta^{ac},$$
$$\sigma\tau(\theta)=\sigma(\zeta^d\theta)=\sigma(\zeta)^d\sigma(\theta)=\zeta^{ad}\zeta^b\theta=\zeta^{ad+b}\theta,$$

т. е.

$$\psi(\sigma\tau)=[ac, ad+b]=[a, b][c, d]=\psi(\sigma)\psi(\tau)$$

и ψ е хомоморфизъм на групата G в групата M_n. Да разгледаме ядрото $\ker\psi$ на този хомоморфизъм. Ако $\mu\in\ker\psi$, то $\psi(\mu)=[1, 0]$ и затова $\mu(\zeta)=\zeta$ и $\mu(\theta)=\theta$. По следствие 1 автоморфизмът μ е единичният автоморфизъм ε на полето $K=P(\zeta, \theta)$. Следователно $\ker\psi=\{\varepsilon\}$ и ψ е мономорфизъм на групата G в групата M_n. Тъй като M_n е разрешима група (твърдение 17), а G е изоморфна на подгрупата $I_m\psi=\psi(G)$ на M_n, то G е също разрешима група. Така получихме следното твърдение.

Твърдение 18. *Групата на Галоа на произволно просто радикално разширение е разрешима.*

Следствие 10. Нека K е просто радикално разширение на полето P, което отговаря на полинома $f(x)=x^n-a$, $0\neq a\in P$ и полето P съдържа примитивен n-ти корен на единицата. Тогава групата на Галоа $G=\mathrm{Gal}(K, a)$ е циклична и редът ѝ $|G|$ дели числото n.

Наистина в този случай $K=P(\theta)$ и хомоморфизмът ψ изобразява всяко $\sigma\in G$ в класа $\psi(\sigma)=[1, b]$, който е елемент на нормалния делител N_n на групата M_n. Понеже групата N_n съгласно твърдение 17 е изоморфна на цикличната адитивна група Z_n и G е изоморфна на подгрупа на N_n, то G е циклична група от ред, който дели числото $n=|Z_n|$.

Следствие 11. *Ако P е поле и ζ е корен на единицата, то $P(\zeta)$ е просто радикално разширение, а групата* $\mathrm{Gal}(P(\zeta), P)$ *е абелева.*

Доказателство. Ако n е най-малкото естествено число, за което $\zeta^n=1$, то ζ е примитивен n-ти корен на единицата. Очевидно е, че полето $P(\zeta)=K$ съдържа всички n-ти корени на единицата (те са степени на ζ) и K е поле на разлагане на полинома x^n-1. Следователно полето K е простото радикално разширение на P, което отговаря на полинома x^n-1. В този случай можем да положим $\theta=1$. Образът на групата $G=\mathrm{Gal}(K/P)$ при разгледания по-горе мономорфизъм ψ се съдържа в подгрупата B_n на M_n, която е съставена от класовете от вида $[a, 0]$ и която е абелева (понеже е изоморфна на Z_n^*).

§ 7. Циклични разширения

Нормалното разширение K на полето P се нарича *циклично*, ако неговата група на Галоа $\mathrm{Gal}(K/P)$ е циклична.

Нека K е циклично разширение на полето P с група на Галоа $G=\mathrm{Gal}(K/P)=\langle\sigma\rangle=\{\varepsilon+\sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ от ред n и полето P съдържа примитивен n-ти корен ζ на единицата. Целта ни в този параграф ще бъде да покажем, че в този случай K е просто радикално разширение на полето P, което отговаря на неразложим полином $f(x)=x^n-a$ над полето P. В предния параграф доказахме следствие 10, което е обратно на това твърдение.

Определение 8. *Ако b е елемент на полето K,* то елементът (ζ, b) на K, който се определя с равенството

$$(1)\qquad (\zeta, b)=\sum_{k=0}^{n-1}\zeta^k\cdot\sigma^k(b),$$

се нарича *резолвента на Лагранж* на елемента b.

Лема 6. *Ако резолвентата на Лагранж (ζ, b) на елемента b от K е различна от 0, то $K=P(b)$.*

Доказателство. Тъй като $b\in K$, то $P(b)\leqq K$, т. е. $P(b)$ е междинно подполе. На това междинно подполе в съответствието на Галоа отговаря подгрупа $H=\mathrm{Gal}(K/P(b))$ на групата на Галоа $\mathrm{Gal}(K/P)=G$. Тъй като $G=\langle\sigma\rangle$ е циклична група от ред n с образуващ елемент σ, то H е циклична група. Ако m е редът на H и d е индексът на H в G, то $n=md$ и σ^d е пораждащ елемент на H, т. е. $H=\langle\sigma^d\rangle$.

Да допуснем, че $d\neq n$. Тогава $\zeta^d\neq 1$ и

$$\sum_{i=0}^{m-1}\zeta^{id}=1+\zeta^d+\zeta^{2d}+\ldots+\zeta^{(m-1)d}$$

$$=(1-\zeta^{md})\,(1-\zeta^d)^{-1}=(1-\zeta^n)\,(1-\zeta^d)^{-1}=0.$$

Понеже $(\sigma^i)^d=(\sigma^d)^i$ е елемент от H и $b\in P(b)$, а елементите на $P(b)$ са неподвижни относно H, то $\sigma^{id+j}(b)=\sigma^j(b)$ за всички цели числа i и j. Така получаваме

$$(\zeta, b)=\sum_{k=0}^{n-1}\zeta^k\sigma^k(b)=\sum_{i=0}^{m-1}\sum_{j=0}^{d-1}\zeta^{id+j}\sigma^{id+j}(b)$$

$$=\left(\sum_{j=0}^{d-1}\zeta^j\sigma^j(b)\right)\left(\sum_{i=0}^{m-1}\zeta^{id}\right)=0,$$

което противоречи на условието $(\zeta, b)\neq 0$.

Следователно $d=n$ и H е единичната подгрупа $\langle\varepsilon\rangle$ на G.

Тъй като $H=\langle\varepsilon\rangle$ и $P(b)$ е неподвижното поле на H, то $K=P(b)$ и лемата е доказана.

Лема 7. *В полето K съществува поне един елемент b, за който* $(\zeta, b)\neq 0$.

Доказателство. Ако $n=1$, то $(\zeta, 1)=1\neq 0$ и лемата е вярна в този случай. Нека $n>1$. Тогава $\zeta\neq 1$ и

$$(\zeta, 1)=1+\zeta+\ldots+\zeta^{n-1}=(1-\zeta^n)\ (1-\zeta)^{-1}=0.$$

Нормалното разширение K на P е крайно разширение на P и затова $K=P(\theta)$ за някой елемент θ от K. Ще покажем, че поне една от резолвентите (ζ, θ), (ζ, θ^2),..., (ζ, θ^{n-1}) е различна от 0.

Наистина ако тези $n-1$ резолвенти са равни на 0, то ще бъдат изпълнени следните n равенства

$$\begin{vmatrix} 1+\zeta+\zeta^2+\ldots+\zeta^{n-1}=0, \\ \theta+\zeta\sigma(\theta)+\zeta^2\sigma^2(\theta)+\ldots+\zeta^{n-1}\sigma^{n-1}(\theta)=0, \\ \theta^2+\zeta\sigma(\theta)^2+\zeta^2\sigma^2(\theta)^2+\ldots+\zeta^{n-1}\sigma^{n-1}(\theta)^2=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \theta^{n-1}+\zeta\sigma(\theta)^{n-1}+\zeta^2\sigma^2(\theta)^{n-1}+\ldots+\zeta^{n-1}\sigma^{n-1}(\theta)^{n-1}=0, \end{vmatrix}$$

които показват, че $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ образуват ненулево решение на хомогенна линейна система с детерминанта

$$\Delta=\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \theta & \sigma(\theta) & \ldots & \sigma^{n-1}(\theta) \\ \theta^2 & \sigma(\theta)^2 & \ldots & \sigma^{n-1}(\theta)^2 \\ \ldots & \ldots & \ldots & \ldots \\ \theta^{n-1} & \sigma(\theta)^{n-1} & \ldots & \sigma^{n-1}(\theta)^{n-1} \end{vmatrix}.$$

Оттук следва, че $\Delta=0$. Но понеже $\Delta=\prod_{i>j\geq 0}(\sigma^i(\theta)-\sigma^j(\theta))$ и $\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)$ са два по два различни корена на минималния над P полином на θ, то $\Delta\neq 0$. Полученото противоречие показва, че съществува елемент $b\in\{\theta, \theta^2, \ldots, \theta^{n-1}\}$, за който $(\zeta, b)\neq 0$.

Теорема 9. *Нека K е нормално разширение на полето P от степен n и полето P съдържа примитивен n-ти корен ζ на единицата. Групата на Галоа $G=\mathrm{Gal}(K/P)$ е циклична тогава и само тогава, когато K съвпада с простото радикално разширение $P(c)$ на полето P, където c е корен на неразложим полином $f(x)=x^n-a$ над P.*

Доказателство. Ако K е просто радикално разширение на P, което отговаря на полинома $f(x)=x^n-a$, то по следствие 10 групата G е циклична. Затова трябва да докажем само обратното твърдение на теоремата. Нека G е циклична група с пораждащ елемент σ. Тъй като $n=[K:P]=|G|$, то $G=\langle\sigma\rangle=\{\varepsilon, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$.

Според лема 7 в K съществува елемент b, за който $c=(\zeta, b)\neq 0$. За елемента c е изпълнено равенството $\sigma(c)=\zeta^{-1}c$. Наистина, като вземем под внимание, че $\zeta^n=1$, $\sigma^n=\varepsilon$ и $\sigma(\zeta)=\zeta$ (понеже $\zeta\in P$), то получаваме

$$\sigma(c)=\sigma\left(\sum_{k=0}^{n-1}\zeta^k\sigma^k(b)\right)=\sum_{k=0}^{n-1}\sigma(\zeta)^k\sigma^{k+1}(b)=\sum_{k=0}^{n-1}\zeta^k\sigma^{k+1}(b)$$

$$=\zeta^{-1}\sum_{i=1}^{n}\zeta^i\sigma^i(b)=\zeta^{-1}\left(\zeta^n\sigma^n(b)+\sum_{i=1}^{n-1}\zeta^i\sigma^i(b)\right)$$

$$=\zeta^{-1}\left(b+\sum_{i=1}^{n-1}\zeta^i\sigma^i(b)\right)=\zeta^{-1}\sum_{i=0}^{n-1}\zeta^i\sigma^i(b)=\zeta^{-1}c.$$

От равенството $\sigma(c)=\zeta^{-1}c$ с очевидна индукция се получава $\sigma^t(c)=\zeta^{-t}c$ за всяко естествено число t.

Ще докажем, че $K=P(c)$. Понеже K е нормално разширение на P и $P\leqq P(c)\leqq K$, то по твърдение 4 K е нормално разширение на $P(c)$, а групата $H=\mathrm{Gal}(K/P(c))$ е подгрупа на цикличната група $G=\langle\sigma\rangle$. Затова H е циклична и се поражда от някоя степен σ^k $(0\leqq k\leqq n-1)$ на σ. Елементът c се съдържа в неподвижното поле $P(c)$ на H, а $\sigma^k\in H$. Затова $\sigma^k(c)=c$. Но от доказаната по-горе формула получаваме $\sigma^k(c)=\zeta^{-k}c=c$, т. е. $\zeta^{-k}=1$. Последното равенство показва, че n дели k, тъй като ζ е примитивен n-ти корен на единицата. Но тогава $\sigma^k=\varepsilon$ и $H=\langle\varepsilon\rangle$. От съвпадението $H=\langle\varepsilon\rangle$ следва очевидно равенството $K=P(c)$.

Да положим $a=c^n$. Тъй като $c\neq 0$, то и $a\neq 0$. Освен това в сила е равенството $\sigma(a)=\sigma(c^n)=\sigma(c)^n=(\zeta^{-1}c)^n=c^n=a$, т. е. a се съдържа в неподвижното поле P на групата $\langle\sigma\rangle=G$.

Да разгледаме полинома $f(x)=x^n-a$ от $P[x]$. Тъй като c е корен на $f(x)$, $K=P(c)$, $[P(c):P]=|G|=n=\deg f(x)$ и $f(x)$ е със старши коефициент 1, то $f(x)$ е минималният полином на c над P. Затова $f(x)$ е неразложим полином над полето P.

Полето K е поле на разлагане на полинома $f(x)$. Наистина то съдържа поле на разлагане на $f(x)$, понеже $f(x)$ е неразложим над P, K е нормално разширение на P и K съдържа корен c на $f(x)$. От равенството $K=P(c)$ пък следва, че K се съдържа в това поле на разлагане, т. е. K съвпада с него. Теоремата е доказана.

§ 8. Радикални разширения

Ако K е разширение на полето P, то редицата

(1) $$P=L_0\leqq L_1\leqq L_2\leqq\ldots\leqq L_s=K$$

от подполетата на K се нарича *радикален ред* на K, ако $L_i=L_{i-1}(b_i)$, където елементът b_i е корен на полинома

$$f_i(x)=x^{n_i}-a_i,\ a_i\in L_{i-1},\ i=1, 2, \ldots, s.$$

Определение 9. Разширението K на полето P се нарича *радикално разширение* на P, ако K има поне един радикален ред.

Тъй като радикалният ред има краен брой членове, а простите алгебрични разширения са крайни разширения, то всяко радикално разширение е крайно разширение на P. Едно радикално разширение може да има различни радикални редове.

Простите радикални разширения са радикални разширения. Наистина ако F е просто радикално разширение на P, то, както видяхме в § 6, $F=P(\zeta, \theta)$, където θ е корен на полином x^n-a, $a \in P$ и ζ е примитивен n-ти корен на единицата. Но тогава

$$L_0=P \leqq L_1=P(\zeta) \leqq L_2=L_1(\theta)=P(\zeta)(\theta)=F$$

е радикален ред на F.

Радикалното разширение K на полето P не е задължено да бъде нормално разширение на P. Например, както посочихме в § 2, полето $\mathbf{Q}\left(\sqrt[3]{2}\right)$ не е нормално разширение на полето $\mathbf{Q}$ на рационалните числа, но $\mathbf{Q}\left(\sqrt[3]{2}\right)$ е радикално разширение на $\mathbf{Q}$.

Определение 10. Радикалното разширение K на полето P с радикален ред (1) се нарича *полуабелево*, ако за всяко $i\,(1 \leqq i \leqq s)$ полето L_i е нормално разширение на L_{i-1} и неговата група на Галоа $\mathrm{Gal}\,(L_i/L_{i-1})$ е абелева.

Твърдение 19. *Всяко радикално разширение K на полето P може да се вложи в полуабелево разширение F на полето P.*

Доказателство. Нека (1) е радикален ред на K, нека m е най-малкото общо кратно на степените $n_1, n_2, \ldots, n_s$ на полиномите $f_1(x), f_2(x), \ldots, f_s(x)$, нека F е полето на разлагане на полинома x^m-1 над полето K, нека $\delta \in F$ е примитивен m-ти корен на единицата. Тогава $F=K(\delta)$. Ще докажем, че полето F, което съдържа K, е полуабелево разширение на P. Нека $F_0=P$ и $F_{i+1}=L_i(\delta)$ за $i=0, 1, \ldots, s$. Да разгледаме редицата от подполета

$$P=F_0 \leqq F_1 \leqq F_2 \leqq \ldots \leqq F_{s+1}=F. \tag{2}$$

Полето F_1 се получава от полето $F_0=P$ с присъединяване на корен на единицата. Според следствие 11 F_1 е нормално разширение на F_0 с абелева група на Галоа. За $i \geqq 1$ е изпълнено равенството $L_i=L_{i-1}(b_i)$ и

$$F_{i+1}=L_i(\delta)=L_{i-1}(b_i)(\delta)=L_{i-1}(b_i, \delta)=L_{i-1}(\delta)(b_i)=F_i(b_i),$$

където b_i е корен на полинома $f_i(x)=x^{n_i}-a_i$, $a_i \in L_{i-1} \subseteq F_i$. Следователно (2) е радикален ред на F, а F е радикално разширение на полето P.

Понеже n_i дели числото m, а $\delta \in F_i$ е примитивен m-ти корен на единицата, то $\delta^{q_i} \in F_i$ $(m=q_i n_i)$ е примитивен n_i-ти корен на единицата $(1 \leqq i \leqq s)$. Затова полето F_{i+1} е просто радикално разширение на полето F_i, което отговаря на полинома $f_i(x)=x^{n_i}-a_i$ над F_i и по следствие 10 групата на Галоа $\mathrm{Gal}(F_{i+1}/F_i)$ е циклична. Следователно полето F е полуабелево разширение на полето P.

Твърдение 20. *Ако $F_1, F_2, \ldots, F_n$ са полуабелеви разширения на полето P, които се съдържат в полето K, то композитът им $F=F_1F_2 \ldots F_n$ е също полуабелево разширение на полето P.*

Доказателство. Ако $n=1$, то $F=F_1$ и твърдението в този случай е вярно. Нека $n=2$, а F_1 и F_2 са полуабелеви разширения на P съответно с радикални редове

$$P=K_0\leqq K_1\leqq\ldots\leqq K_s=F_1,$$

$$P=L_0\leqq L_1\leqq\ldots\leqq L_t=F_2.$$

Тогава групите $\mathrm{Gal}\,(K_i/K_{i-1})$ и $\mathrm{Gal}\,(L_j/L_{j-1})$ са абелеви за $i=1, 2, \ldots, s$ и $j=1, 2, \ldots, t$. Полагаме $K_{s+j}=F_1L_j$, където $j=1, 2, \ldots, t$. По теорема 6 полето K_{s+j} е нормално разширение на полето $K_{s+j-1}=F_1L_{j-1}$ и $\mathrm{Gal}\,(K_{s+j}/K_{s+j-1})$ е абелева, защото е изоморфна на подгрупа на абелевата група $\mathrm{Gal}\,(L_j/L_{j-1})$, $j=1, 2, \ldots, t$. Освен това $L_j=L_{j-1}(b_j)$, където b_j е корен на полинома $f_j(x)=x^{n_j}-a_j$, $a_j\in L_{j-1}$. Затова $K_{s+j}=K_{s+j-1}(b_j)$ и $a_j\in L_{j-1}\subseteq K_{s+j-1}$. Следователно

$$P=K_0\leqq\ldots\leqq K_s=F_1\leqq K_{s+1}\leqq\ldots\leqq K_{s+t}=F$$

е радикален ред на композита $F=F_1F_2$, в който всяко поле е нормално разширение на предхождащото го с абелева група на Галоа, т. е. F е полуабелево разширение на полето P. Следователно твърдението е вярно за $n=2$.

Нека $n>2$ и твърдението е вярно за $n-1$ междинни подполета. Тогава $F_2'=F_2F_3 \ldots F_n$ е полуабелево разширение на P. По предната част на доказателството $F=F_1F_2'$ е полуабелево разширение на P. С това индукционната стъпка е направена и твърдението е доказано.

Лема 8. *Ако K е поле, $L\leqq M\leqq K$, M е нормално разширение на L и σ е автоморфизъм на K, то полето $\sigma(M)$ е нормално разширение на $\sigma(L)$ и $\mathrm{Gal}\,(M/L)\cong\mathrm{Gal}\,(\sigma(M)/\sigma(L))$.*

Доказателство. Ако M е нормално разширение на полето L, то M е поле на разлагане на полином

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n,\ a_i\in L,$$

с корени $b_1, b_2, \ldots, b_n$ от M и $M=L(b_1, b_2, \ldots, b_n)$. Полагаме $c_0=\sigma(a_0), c_1=\sigma(a_1), \ldots, c_n=\sigma(a_n), d_1=\sigma(b_1), d_2=\sigma(b_2), \ldots, d_n=\sigma(b_n)$. Тогава полиномът $g(x)=c_0x^n+c_1x^{n-1}+\ldots+c_n$ е с коефициенти от полето $L_1=\sigma(L)$, а корените му $d_1, \ldots, d_n$ са от $M_1=\sigma(M)$. Освен това $M_1=\sigma(L(b_1, \ldots, b_n))=L_1(d_1, \ldots, d_n)$, т. е. M_1 е поле на разлагане на $g(x)$ над L_1 и затова M_1 е нормално разширение на L_1. Нека $G_1=\mathrm{Gal}\,(M_1/L_1)$. Ако $\tau_1\in G_1$, то $\sigma^{-1}\tau_1\sigma=\tau$ е елемент на групата $G=\mathrm{Gal}\,(M/L)$. Лесно се проверява, че изображението $\tau_1\to\sigma^{-1}\tau_1\sigma$ е изоморфизъм на G_1 върху G. Лемата е доказана.

Следствие 12. *Ако K е поле, $P\leqq F\leqq K$, σ е автоморфизъм*

на K над P и F е радикално или полуабелево разширение на P, то образът му $\sigma(F)$ е съответно радикално или полуабелево разширение на P.

Доказателство. Нека F е радикално разширение на P с радикален ред

$$P=L_0\leqq L_1\leqq\ldots\leqq L_s=F,$$

където $L_i=L_{i-1}(b_i)$ и b_i е корен на $f_i(x)=x^{n_i}-a_i$, $a_i\in L_{i-1}$ $i=1, 2, \ldots, s$. Полагаме $\sigma(F)=F_1$ и $M_i=\sigma(L_i)$. Тъй като $M_i=M_{i-1}(d_i)$, където $d_i=\sigma(b_i)$ е корен на полинома $g_i(x)=x^{n_i}-c_i$, $c_i=\sigma(a_i)\in M_{i-1}=\sigma(L_{i-1})$, то редът

$$P=M_0\leqq M_1\leqq\ldots\leqq M_s=F_1$$

е радикален ред на F_1. Следователно полето F_1 е радикално разширение на полето P.

Ако радикалното разширение F е полуабелево разширение на P, то по предната лема M_i е нормално разширение на M_{i-1} и $\mathrm{Gal}(M_i/M_{i-1})$ е абелева, защото е изоморфна на абелевата група $\mathrm{Gal}(L_i/L_{i-1})$. Това показва, че F_1 е също полуабелево разширение на P. Следствието е доказано.

Твърдение 21. *Всяко полуабелево разширение F на полето P може да се вложи в нормално полуабелево разширение K на P.*

Доказателство. Полуабелевото разширение F на полето P е крайно разширение на P. Затова $F=P(\theta)$ за подходящ елемент θ от F. Нека $p(x)$ е минималният полином на θ над P, а K е полето на разлагане на $p(x)$ над F. Ако $\theta=\theta_1, \theta_2, \ldots, \theta_n$ са корените на $p(x)$ в K, то $K=P(\theta_1, \ldots, \theta_n)$ и K съдържа $F=P(\theta)$. Ще докажем, че нормалното разширение K на P е полуабелево разширение на P. Да положим $F_i=P(\theta_i)$, $i=1, 2, \ldots, n$. Очевидно е, че $F_1=F$ и че полето K съвпада с композита $F_1F_2\ldots F_n$. Тъй като елементите $\theta_1=\theta$ и θ_i са спрегнати над P, то според твърдение 3 в $\mathrm{Gal}(K/P)$ съществува такъв автоморфизъм σ_i, че $\sigma_i(\theta)=\theta_i$. Тогава $\sigma_i(F)=F_i$ и според предното следствие полето F_i е полуабелево разширение на P, $i=1, 2, \ldots, n$. Тогава композитът $K=F_1F_2\ldots F_n$ по твърдение 20 е полуабелево разширение на полето P. Твърдението е доказано.

Теорема 10. *Групата на Галоа на всяко нормално радикално разширение е разрешима.*

Доказателство. Нека K е нормално радикално разширение на полето P. Според твърдения 19 и 21 полето K може да се вложи в нормално полуабелево разширение F на P. Тъй като K е нормално междинно подполе на разширението F на полето P, то от теорема 5 следва, че $G=\mathrm{Gal}(K/P)$ е хомоморфен образ на $H=\mathrm{Gal}(F/P)$. Ще докажем, че $H=\mathrm{Gal}(F/P)$ е разрешима. Нека

$$P=L_0\leqq L_1\leqq\ldots\leqq L_s=F$$

е радикален ред на F с абелеви групи на Галоа $\mathrm{Gal}(L_i/L_{i-1})$, $i=1, 2, \ldots, s$. В съответствието на Галоа на междинното подполе L_i съответствува подгрупа $H_i=\mathrm{Gal}(F/L_i)$ на групата H, а L_i е неподвижното подполе на подгрупата H_i. Да разгледаме тройката полета $L_{i-1}\leqq L_i\leqq F$. В нея F е нормално разширение на L_{i-1} и L_i, а L_i е нормално разширение на L_{i-1} с абелева група на Галоа $A_i=\mathrm{Gal}(L_i/L_{i-1})$. Затова подгрупата $H_i=\mathrm{Gal}(F/L_i)$ е нормален делител на $H_{i-1}=\mathrm{Gal}(F/L_{i-1})$, а фактор-групата H_{i-1}/H_i по теорема 5 е изоморфна на комутативната група A_i $(i=1, 2, \ldots, s)$. Следователно

$$H=H_0\geqq H_1\geqq \ldots \geqq H_s=\mathrm{Gal}(F/F)=\langle\varepsilon\rangle$$

е нормален ред на H с абелеви фактори, т. е. групата H е разрешима, а тогава по твърдение 11 и нейният хомоморфен образ $G=\mathrm{Gal}(K/P)$ е разрешима група. Теоремата е доказана.

Теорема 11. *Всяко нормално разширение K на полето P, което има разрешима група на Галоа, може да се вложи в нормално радикално разширение L на полето P.*

Доказателство. Нека n е редът на групата $G=\mathrm{Gal}(K/P)$, а M е поле на разлагане на полинома x^n-1 над полето K. Нека ζ е примитивен n-ти корен на единицата от M, а $L_1=P(\zeta)$. Ще докажем, че композитът $L=KL_1$ е търсеното нормално радикално разширение на полето P. Тъй като K и L_1 са нормални разширения на полето P, то от теорема 6 и твърдение 5 следва, че композитът $L=KL_1$ е нормално разширение на K и на L_1, а $H=\mathrm{Gal}(L/L_1)$ е изоморфна на подгрупа на разрешимата група G. Затова редът m на H дели реда n на G и освен това според твърдение 10 групата H е разрешима. Според теорема 7 в H има нормален ред

$$H=H_0\geqq H_1\geqq \ldots \geqq H_s=\langle e\rangle \tag{3}$$

с циклични фактори H_{i-1}/H_i, $i=1, 2\ldots, s$. Редовете $n_i=|(H_{i-1}/H_i)|$ на тези фактори делят реда m на H и затова те са делители на реда n на G. Да разгледаме редицата

$$P=L_0\leqq L_1=P(\zeta)\leqq L_2\leqq \ldots \leqq L_{s+1}=L \tag{4}$$

от подполета на L, където L_{i+1} е неподвижното поле K^{H_i} на подгрупата H_i за $i=0, 1, 2, \ldots, s$. Ще докажем, че редът (4) е радикален. Полето L_1 е просто алгебрично разширение на L_0, което отговаря на полинома x^n-1 над L_0. Нека $i\geqq 1$ и да разгледаме тройката полета $L_i\leqq L_{i+1}\leqq L$. Тъй като $[L:L_i]=|H_{i-1}|$, $[L:L_{i+1}]=|H_i|$ и $[L:L_i]=[L:L_{i+1}]\,[L_{i+1}:L_i]$, то степента на L_{i+1} над L_i е равна на реда n_i на фактора H_{i-1}/H_i. Полето L_i съдържа примитивен n_i-ти корен на единицата, тъй като $\zeta\in L_i$ и n_i е делител на n. Освен това полето L_{i+1} е нормално разширение на полето L_i, защото е неподвижното поле на нормален делител H_i на групата на Галоа $\mathrm{Gal}(L/L_i)=H_{i-1}$. Групата $\mathrm{Gal}(L_{i+1}/L_i)$ е циклична от ред n_i, тъй като тя е изоморфна на фактор-групата H_{i-1}/H_i. Тогава според теорема 9 е изпълнено равенството $L_{i+1}=L_i(b_{i+1})$, където b_{i+1} е корен на

полином от вида $x^{n_i}-a_i$, $a_i \in L_i$, $i=1, 2, \ldots, s$. Следователно редът (4) е радикален, а L е радикално разширение на P_s което по построение съдържа полето K. Теоремата е доказана.

§ 9. Решимост на уравнения в радикали

В този и в следващия параграф ще приложим развитата в предните параграфи теория към някои от задачите, които са свързани с решаването на алгебрични уравнения в радикали. С помощта на теорията на Галоа се получава пълно и точно обяснение на съществуването на познатите формули за корените на полиномите от степен 2, 3 и 4 (виж § 9 на глава II), а така също и доказателството на това, че при по-високите степени такива формули не съществуват. Задачите за построение с линия и пергел намират също своята естествена трактовка в рамките на теорията на Галоа. Целите на настоящия учебник не ни позволяват да разгледаме много от възхитителните по своята дълбочина задачи и приложения на теорията на Галоа.

Определение 11. Ще казваме, че неразложимият полином $f(x)$ над полето P е *решим в радикали* (или *решим с радикали*), ако съществува радикално разширение K на полето P, в което $f(x)$ има поне един корен.

Теорема 12. *Неразложимият полином $f(x)$ над полето P е решим в радикали тогава и само тогава, когато групата на Галоа $\mathrm{Gal}(K/P)=G$ на неговото поле K на разлагане е разрешима. Освен това ако $f(x)$ е решим в радикали, то съществува нормално радикално разширение на P, което съдържа полето K.*

Доказателство 1. Ако групата G е разрешима, то по теорема 11 полето K се влага в нормално радикално разширение L на полето P. Следователно $f(x)$ е решим с радикали, а полето K на разлагане над P се съдържа в нормално радикално разширение на P.

2. Нека $f(x)$ е решим в радикали и нека M е радикално разширение на P, което съдържа корен на $f(x)$. Според твърдение 19 радикалното разширение M на P може да се вложи в полуабелево разширение F на полето P, а от твърдение 21 следва, че F може да се вложи в нормално радикално разширение L на полето P. Тъй като неразложимият над P полином $f(x)$ има корен в $M \leqq L$, то той се разлага на линейни множители над L. Нека K_1 е полето на разлагане на $f(x)$ над P, което се съдържа в L и $G_1=\mathrm{Gal}(K_1/P)$.

Тъй като G_1 е хомоморфен образ на групата $H=\mathrm{Gal}(L/P)$, която според теорема 10 е разрешима, то G_1 е разрешима група. Но групата $G=\mathrm{Gal}(K/P)$ е изоморфна на групата $G_1=\mathrm{Gal}(K_1/P)$, тъй като полетата K и K_1 са изоморфни над P (теорема 9 и следствие 8 на глава VIII). Следователно групата G е разрешима. Теоремата е доказана.

Ако полиномът $f(x)$ над P е разложим над P, то естествено

е да считаме, че $f(x)$ е решим с радикали, когато всеки неразложим над P делител на $f(x)$ е решим с радикали. Прието е също групата на Галоа $\mathrm{Gal}(K/P)$ на полето на разлагане K на $f(x)$ над P да се нарича *група на Галоа на* $f(x)$ *над* P или *на уравнението* $f(x)=0$. Предната теорема може да се обобщи по следния начин.

Теорема 13. *Ако* $f(x)$ *е произволен полином над полето* P, *то уравнението* $f(x)=0$ *е решимо с радикали тогава и само тогава, когато неговата група на Галоа е разрешима.*

Доказателство. Нека K е поле на разлагане на полинома $f(x)$ над P, $G=\mathrm{Gal}(K/P)$ е групата му на Галоа, а $p_1(x)$, $p_2(x), \ldots, p_n(x)$ са различните неразложими над P делители на $f(x)$.

Ако $n=1$, то $f(x)=p_1^r(x)$, където $p_1(x)$ е неразложим полином над P. Тогава $f(x)=0$ е решимо в радикали точно тогава, когато е решимо в радикали уравнението $p_1(x)=0$. Очевидно е, че K е поле на разлагане и на $p_1(x)$ над P, т. е. G е групата на Галоа и на $p_1(x)$. По теорема 12 уравнението $f(x)=0$ е решимо в радикали тогава и само тогава, когато групата G е разрешима, т. е. при $n=1$ теоремата е вярна.

Ще проведем доказателството с индукция по n. Нека $n>1$ и да допуснем, че теоремата е вярна за полиноми с по-малко от n различни неразложими делители. Полиномът $f(x)$ се представя във вида $f(x)=p_1^r(x)q(x)$, където $p_1(x)$ не дели полинома $q(x)$, а $q(x)$ има $n-1$ различни неразложими делителя над P. Полето K съдържа поле M на разлагане на $q(x)$ над P, а групата на Галоа $F=\mathrm{Gal}(M/P)$ на $q(x)$ е изоморфна на фактор-групата $G/\mathrm{Gal}(K/M)$. Нека L е подполето на K, което е поле на разлагане на неразложимия полином $p_1(x)$ над P, а $H=\mathrm{Gal}(L/P)$. Тъй като $K=LM$, то от теорема 6 следва, че групата $\mathrm{Gal}(K/M)$ е изоморфна на подгрупа на групата H.

Нека сега $f(x)=0$ е решимо с радикали. Тогава $p_1(x)=0$ и $q(x)=0$ са решими в радикали и затова групите им на Галоа H и F са разрешими. Но тогава и групата $\mathrm{Gal}(K/M)$ е разрешима. По твърдение 12 G е също разрешима група.

Ако пък G е разрешима група, то полето K се влага в радикално разширение на P (теорема 11) и $f(x)$ е решим с радикали. С това индукционната стъпка е направена и теоремата е доказана.

Ако $f(x)$ е произволен полином над полето P, а $a_1, a_2, \ldots, a_n$ са различните корени на $f(x)$ в полето му K на разлагане над P, то $K=P(a_1, a_2, \ldots, a_n)$ и $f(x)$ се разлага над K във вида

$$f(x)=a(x-a_1)^{l_1}(x-a_2)^{l_2}\ldots(x-a_n)^{l_n},$$

където $a\in P$, $l_i\geqq 1$, $i=1, 2, \ldots, n$.

От следствие 2 знаем, че всеки автоморфизъм σ от групата $G=\mathrm{Gal}(K/P)$ на $f(x)$ се определя еднозначно от действието си върху елементите $a_1, a_2, \ldots, a_n$, а $\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)$ е една пермутация на тези елементи. Следователно групата G е подгрупа на симетричната група на множеството от различните корени на

$f(x)$. За опростяване на разглежданията можем да считаме, че G е подгрупа на симетричната група S_n, т. е. елементите на G ще пермутират индексите на елементите a_i. По този начин автоморфизмът $\sigma \in G$, за който имаме $\sigma(a_1)=a_{i_1}$, $\sigma(a_2)=a_{i_2}, \ldots, \sigma(a_n)=a_{i_n}$, се отъждествява със субституцията

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}.$$

Така интерпретирана, групата G действува на множеството от числата $1, 2, \ldots, n$ и то се разбива на орбити относно нейното действие. Ако числата $j_1, j_2, \ldots, j_r$ образуват една орбита относно действието на G, то $a_{j_1}, a_{j_2}, \ldots, a_{j_r}$ са корените на неразложим над P делител $p(x)$ на полинома $f(x)$. Наистина ако $p(x)$ е онзи неразложим делител на $f(x)$, на който a_{j_1} е корен, то, понеже $a_{j_k}=\sigma(a_{j_1})$ за някой автоморфизъм σ от G, то a_{j_k} е корен на $p(x)$. Ако b е корен на $p(x)$, то a_{j_1} и b са спрегнати над P и по твърдение 3 съществува такова $\tau \in G$, че $b=\tau(a_{j_1})$, т. е. $b=a_{j_k}$ за някое k, $1 \leqq k \leqq r$. Орбитата $\{j_1, j_2, \ldots, j_r\}$ относно действието на групата G (а така също множеството от корените $a_{j_1}, a_{j_2}, \ldots, a_{j_r}$) се нарича област на транзитивност на групата G.

Ясно е, че броят на различните области на транзитивност е равен на броя на различните неразложими делители на полинома $f(x)$. Полиномът $f(x)$ е степен на неразложим полином над P тогава и само тогава, когато числата $1, 2, \ldots, n$ образуват област на транзитивност на G, т. е. когато G действува транзитивно на множеството $\{1, 2, \ldots, n\}$. В този случай ще казваме, че групата G на Галоа е *транзитивна*.

Задача. Докажете, че всеки полином над полето P, чиято степен е не по-голяма от 4, е решим с радикали.

Упътване. Използувайте факта, че S_n при $n \leqq 4$ е разрешима група.

Ясно е, че нерешими в радикали полиноми трябва да бъдат търсени сред полиномите от степен, по-голяма или равна на 5. При това възможността за намиране на такива полиноми зависи от основното поле P. Ако P е алгебрически затворено, то неразложимите над P полиноми са от степен 1 и затова всеки полином над P е решим в радикали. Също така ако $P=R$ е полето на реалните числа, то неразложимите полиноми над R са от степен 1 или 2 и всеки полином над R е решим в радикали. Тъй като всеки полином над P, неразложимите делители на който са от степен, не по-голяма от 4, е решим с радикали, то необходимо условие за съществуването на нерешими в радикали полиноми над P е да има неразложими полиноми над P от степен, по-голяма или равна на 5. Едно такова поле е полето на рационалните числа, над което има неразложими полиноми от произволна степен (виж § 7 на глава II).

Лема 9. *Нека q е просто число, а G е транзитивна подгрупа на симетричната група S_q. Тогава всеки неединичен нор-*

мален делител H на G е също транзитивна подгрупа на S_q.

Доказателство. Неединичният нормален делител H на групата G действува на множеството от числата $1, 2, \ldots, q$ и го разбива на орбити. Нека $O(i)$ и $O(j)$ са две орбити относно действието на H и $r=|O(i)|$, $s=|O(j)|$. Ще покажем, че $r=s$, т. е. че всеки две орбити относно действието на H имат еднакъв брой елементи. Наистина, тъй като G е транзитивна, то $j=g(i)$ за някой елемент g от G. Полагаме $g(O(i))=\{g(k)|\ k\in O(i)\}$. Ясно, е че множеството $g(O(i))$ има $r=|O(i)|$ елемента. Нека $k\in O(i)$. Тогава $k=h(i)$ за някое h от H, а елементът ghg^{-1} е от H, понеже H е нормален делител на G. Елементът $g(k)$ от $g(O(i))$ се записва във вида $g(k)=gh(l)=ghg^{-1}g(i)=ghg^{-1}(j)$, което показва, че $g(k)\in O(j)$. Следователно множеството $g(O(i))$ се съдържа в орбитата $O(j)$. Това доказва неравенството $r\leqq s$. Обратното неравенство се получава аналогично с използуване на g^{-1} и $i=g^{-1}(j)$. Следователно $r=s$.

Тъй като броят на елементите на всеки две орбити е едно и също число r, то r е делител на простото число q. Орбитите не могат да бъдат едноелементни, тъй като H е неединична подгрупа на S_q. Следователно $r>1$ и от това, че q е просто число, следва равенството $r=q$. Но това означава, че H е транзитивна подгрупа на S_q. Лемата е доказана.

Нека q е просто число. Тогава пръстенът $Z_q=Z/qZ$ е поле с q елемента $[1], [2], \ldots, [q-1]$ и $[q]=[0]$. За нас ще бъде удобно сега да означаваме тези елементи с $1, 2, \ldots, q$ и да считаме, че симетричната група S_q действува на елементите на полето Z_q.

Разбира се, след тази смяна на означенията всички пресмятания с елементите $1, 2, \ldots, q$ на Z_q се извършват по модул q. Ако a е ненулев елемент на Z_q $(a\neq q)$, то a е обратим в Z_q и $a^{-1}=c$, $1\leqq c\leqq q-1$, където $ac\equiv 1 \pmod q$, т. е. $ac=1$ в Z_q. Ако a, $b\in Z_q$ и $a\neq 0$, то изображението $\sigma(a, b): Z_q\to Z_q$, което се определя с формулата $\sigma(a, b)(x)=ax+b$, е взаимно еднозначно изображение на Z_q, т. е. $\sigma(a, b)$ е елемент на симетричната група S_q, която действува на елементите на полето Z_q. Всяка субституция от този вид се нарича линейна. Две линейни субституции $\sigma(a, b)$ и $\sigma(c, d)$ съвпадат тогава и само тогава, когато $a=c$ и $b=d$. Наистина ако $\sigma(a, b)=\sigma(c, d)$, то от $\sigma(a, b)(0)=\sigma(c, d)(0)$ се получава $b=d$, а тогава от $\sigma(a, b)(1)=a+b=\sigma(c, d)(1)=c+d$ следва $a=c$. Линейните субституции образуват подмножество L_q на групата S_q, което съдържа точно $(q-1)q$ елемента. От равенствата $\sigma(a, b)\ \sigma(c, d)(x)=\sigma(a, b)(cx+d)=a(cx+d)+b=acx+ad+b=\sigma(ac, ad+b)(x)$ следва формулата

$$\sigma(a, b)\sigma(c, d)=\sigma(ac, ad+b), \tag{1}$$

която показва, че произведение на линейни субституции е линейна субституция. Очевидно е, че тъждествената субституция е съвпада с линейната субституция $\sigma(1, 0)$, а от формула (1) се получава равенството

$$\sigma(a, b)^{-1}=\sigma(a^{-1}, -a^{-1}b), \tag{2}$$

т. е. обратната на линейна субституция е също линейна субституция. Следователно множеството L_q на линейните субституции е подгрупа на симетричната група S_q.

На всяка линейна субституция $\sigma(a, b)$ съответствува елемент $[a, b]$ на групата M_q, която построихме в § 5. Тъй като на различни линейни субституции отговарят различни елементи на M_q и M_q има $\varphi(q)\,q=(q-1)\,q$ елемента, то това съответствие е взаимно еднозначно. От формула (1) и от определението на умножението в M_q следва, че съответствието е изоморфизъм между групите L_q и M_q. Понеже групата M_q е разрешима (твърдение 17), то и групата L_q е разрешима. Така получихме следното

Твърдение 22. *Ако q е просто число, то линейните субституции от симетричната група S_q, която действува на елементите на полето Z_q, образуват разрешима подгрупа L_q на S_q, която е изоморфна на групата M_q.*

В § 5 видяхме, че M_q съдържа цикличен нормален делител N_q, който се поражда от елемента $[1, 1]$. Тъй като простото число q е взаимно просто с реда $q-1$ на фактор-групата M_q/N_q, то всеки елемент от M_q от ред q ще се съдържа в нормалния делител N_q, т. е. ще бъде от вида $[1, b]=[1, 1]^b$, където $1\leqq t\leqq q-1$. Следователно линейната субституция $\sigma(1, 1)$ има ред q и поражда цикличен нормален делител на L_q. Освен това всяка линейна субституция от ред q е степен на $\sigma(1, 1)$.

Определение 12. Подгрупата G на симетричната група S_q (q е просто число) се нарича *линейна*, ако елементите на G са линейни субституции и $\sigma(1, 1)\in G$.

Тъй като подгрупите на разрешима група са разрешими групи, то от предното твърдение се получава следното

Следствие 13. *Ако q е просто число, то всяка линейна подгрупа на симетричната група S_q е разрешима група.*

Лема 10. *Ако q е просто число, $F\lhd H\leqq S_q$ и F е линейна подгрупа на S_q, то H е също линейна подгрупа на S_q.*

Доказателство. Тъй като F е линейна подгрупа, то в F се съдържа линейната субституция $\sigma=\sigma(1, 1)$. Нека $\tau\in H$. Тогава $\tau\sigma\tau^{-1}$ е също елемент на нормалния делител F. Тъй като σ е от ред q, то и линейната субституция $\tau\sigma\tau^{-1}$ е от ред q. Понеже всяка линейна субституция от ред q е степен на $\sigma(1, 1)=\sigma$, то $\tau\sigma\tau^{-1}=\sigma^a$, където $1\leqq a\leqq q-1$. Следователно $\tau\sigma=\sigma^a\tau$. Ако $y\in Z_q$, то $\tau\sigma(y)=\sigma^a\tau(y)$, т. е.

$$\tau(y+1)=\tau(y)+a. \tag{3}$$

От (3) следва, че $\tau(y+2)=\tau(y+1)+a=\tau(y)+2a$ и изобщо $\tau(y+x)=\tau(y)+xa$. При $y=0$ и $b=\tau(0)$ получаваме $\tau(x)=ax+b$ за всяко $x\in Z_q$, т. е. τ е линейна субституция. Следователно групата H се състои само от линейни субституции. Тъй като $\sigma=\sigma(1, 1)\in H$, то H е линейна подгрупа на S_q.

Теорема 14. *Нека $f(x)$ е неразложим полином над полето*

P от степен q, където q е просто число. Ако групата G на Галоа на полинома $f(x)$ над P е разрешима, то G е линейна подгрупа на симетричната група S_q.

Доказателство. Тъй като $f(x)$ е неразложим полином над P и разглежданите полета са с характеристика 0, то $f(x)$ има точно q различни корена в полето си K на разлагане над P. Затова групата G е транзитивна подгрупа на симетричната група S_q. Нека G е разрешима група. По теорема 7 групата G има нормален ред с циклични фактори от прости редове

$$G=G_0>G_1>\ldots>G_{s-1}>G_s=\langle e\rangle. \tag{4}$$

Можем да считаме, че G_{s-1} е неединична циклична подгрупа от прост ред d с пораждащ елемент σ. Понеже G_1 е неединичен нормален делител на транзитивната група G, то по лема 9 G_1 е също транзитивна. Като приложим отново същата лема, получаваме, че $G_2, G_3, \ldots, G_{s-1}$ са транзитивни. Тъй като $G_{s-1}=\langle\sigma\rangle$ е от прост ред d, то $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{d-1}(1)$ са всевъзможните образи на 1 относно действието на G_{s-1}. Затова $d=q$ и можем да изберем така номерацията на корените $a_1, a_2, \ldots, a_q$ на полинома $f(x)$, че $a_2=\sigma(a_1), a_3=\sigma^2(a_1), \ldots, a_q=\sigma^{q-1}(a_1)$. Тогава редицата $1, 2, \ldots, q$ ще съвпада точно с редицата $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{q-1}(1)$ при приетото отъждествяване на автоморфизмите от $G=\mathrm{Gal}(K/P)$ със съответните субституции от S_q. Оттук следва, че пораждащият елемент σ на подгрупата G_{s-1} съвпада с линейната субституция $\sigma(1, 1)(x)=x+1$. Следователно G_{s-1} е линейна подгрупа на S_q. Но G_{s-1} е нормален делител на G_{s-2}. Тогава по лема 10 G_{s-2} е също линейна подгрупа на S_q. След неколкократно прилагане на същата лема получаваме, че всички членове на реда (5) са линейни подгрупи на S_q. В частност, групата на Галоа G на $f(x)$ е линейна подгрупа на S_q.

Теорема 15. *Нека $f(x)$ е неразложим полином над полето P от проста степен q, K е полето на разлагане на $f(x)$ над P $G=\mathrm{Gal}(K/P)$ е групата на Галоа на $f(x)$. Ако групата G е разрешима, то полето K се получава от полето P с присъединяване на два произволни различни корена на $f(x)$.*

Доказателство. Нека $a_1, a_2, \ldots, a_q$ са корените на $f(x)$ от K. Тъй като $f(x)$ е неразложим полином над P и P е с нулева характеристика, то $a_i\neq a_j$ при $i\neq j$. Да означим с F подполето $P(a_i, a_j)$, $i\neq j$, на полето K. Нека $H=\mathrm{Gal}(K/F)$ е подгрупата на G, която съответствува на това подполе. Знаем, че редът на H съвпада със степента $[K:F]$. Ако $\tau\in H$, то $\tau(a_i)=a_i$ и $\tau(a_j)=a_j$, т. е. $\tau(i)=i$, $\tau(j)=j$ при отъждествяването на G с подгрупа на S_q. Нека G е разрешима група. По предната теорема G е линейна подгрупа и затова субституцията τ от H съвпада с някоя линейна субституция $\sigma(a, b)$, т. е. $\tau(x)=ax+b$ за всяко $x\in Z_q$. Оттук следва, че $i=\tau(i)=ai+b$, $j=\tau(j)=aj+b$, където $i\neq j$. Ако $a\neq 1$, то $i(1-a)=b=j(1-a)$ влече $i=j$, което е невъзможно. Следователно $a=1$. Но тогава $b=0$ и $\tau=\sigma(1, 0)=\varepsilon$ е тъждествената суб-

ституция. Това показва, че H е единичната подгрупа на G и $[K:F]=1$. Следователно $K=F=P(a_i, a_j)$. Теоремата е доказана.

Следствие 14. *Нека полето P е подполе на полето* R *на реалните числа, а $f(x)$ е неразложим полином от проста нечетна степен q над P. Ако $f(x)$ е решим в радикали над полето P, то или всички негови корени са реални числа, или $f(x)$ има само един реален корен.*

Доказателство. Полиномът $f(x)$ е с реални коефициенти и е от нечетна степен. Затова той има поне един реален корен (глава VIII, лема 2). От теоремата на Даламбер (глава VIII, теорема 15) следва, че полето **C** на комплексните числа съдържа поле K на разлагане на $f(x)$ над реалното поле P. Нека $G=\mathrm{Gal}(K/P)$ е групата на Галоа на $f(x)$ над P. Понеже $f(x)$ е решим в радикали, то групата G е разрешима, а полето K ще се получава от P с присъединяване на кои да са два различни корена на $f(x)$. Ако $f(x)$ има поне два реални корена a_1, a_2, то полето $K=P(a_1, a_2)$ е подполе на полето R на реалните числа и корените на $f(x)$ ще са реални числа, защото те се съдържат в K. Следствието е доказано.

От доказаното следствие се получава, че *всеки неразложим полином от степен* 5 *над полето* **Q** *на рационалните числа, който има точно три реални корена, е нерешим в радикали над* **Q**. А да се построят цели серии от такива полиноми не представлява трудност. Например ако p е произволно просто число, то от критерия на Айзенщайн—Шьонеман (теорема 9 на глава II) следва, че полиномът $f_p(x)=x^5-5px-p$ е неразложим над полето **Q**. Този полином има 5 различни корена в полето **C** на комплексните числа и сред тях нечетен брой са реалните, защото коефициентите на $f_p(x)$ са реални. Елементарни съображения за графиката на функцията $f_p(x)$ ни показват, че ако реалните корени са 5, то производната на $f_p(x)$ ще има 4 реални корена, което не е вярно, тъй като тази производна има точно два реални корена $-\sqrt[4]{p}$ и $\sqrt[4]{p}$. От друга страна, $f_p(x)$ има поне три реални корена, тъй като лесно се намират три интервала, в краищата на които функцията $f_p(x)$ приема стойности с различни знаци — например интервалите $(-p, -1)$, $(-1, 0)$, $(0, p)$. Следователно полиномът $f_p(x)$ има точно 3 реални корена и според предното следствие той е нерешим в радикали над полето **Q**.

Следствие 15. *За всяко естествено число $n\geqq 5$ съществува полином от степен n с рационални коефициенти, който е нерешим в радикали над полето* **Q** *на рационалните числа.*

Наистина достатъчно е да умножим полинома $x^5-10x-2$ с x^{n-5}, за да получим полином от степен n, който е нерешим в радикали над полето **Q**.

§ 10. Теорема на Руфини — Абел

Преди да се заемем с основния въпрос на този параграф, ще изучим с помощта на теорията на Галоа един пример, свързан с полето от рационални функции.

Нека $x_1, x_2, \ldots, x_n$ са независими променливи и M е произволно поле с характеристика 0. Пръстенът $A = M[x_1, x_2, \ldots, x_n]$ от полиномите на $x_1, x_2, \ldots, x_n$ с коефициенти от M е област на цялостност, а неговото поле $L = M(x_1, x_2, \ldots, x_n)$ от частните се нарича поле от рационалните функции на $x_1, x_2, \ldots, x_n$. На всяка субституция σ от симетричната група S_n съответствува автоморфизъм на полето L, който изобразява рационалната функция $f(x_1, x_2, \ldots, x_n)$ в рационалната функция $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. Лесно се вижда, че това съответствие е мономорфизъм на групата S_n в групата $\mathrm{Aut}\, L$ на автоморфизмите на L. Затова можем да разглеждаме S_n като подгрупа на $\mathrm{Aut}\, L$, като отъждествяваме субституцията σ със съответния автоморфизъм на L. Неподвижното подполе S на L относно S_n се нарича *поле на симетричните рационални функции* с коефициенти от M. Тъй като S_n е крайна група от ред $n!$, то от теорема 3 следва, че L е нормално разширение на S, а от твърдение 4 знаем, че $[L : S] = n!$. При това S_n е групата на Галоа $\mathrm{Gal}(L/S)$ на L над S. Ще се стремим да получим по-точни сведения за полето S на симетричните рационални функции и за неговото сечение $B = S \cap A = S \cap M[x_1, x_2, \ldots, x_n]$ с пръстена на полиномите над M, т. е. за пръстена B на симетричните полиноми на $x_1, x_2, \ldots, x_n$. Ясно е, че $M \leqq S \cap A$. Да разгледаме полинома $g(t) = (t - x_1) \ldots (t - x_n) = t^n + a_1 t^{n-1} + \ldots + a_n$ на променливата t над полето L. Коефициентите a_i на $g(t)$ са с точност до знак елементарните симетрични полиноми на $x_1, x_2, \ldots, x_n$, т. е. $a_i = (-1)^i \sum x_1 x_2 \ldots x_i$ $i = 1, 2, \ldots, n$. Ясно е, че $a_1, a_2, \ldots, a_n$ се съдържат в пръстена $B = A \cap S$. Тъй като $M \leqq S$ и $a_1, a_2, \ldots, a_n \in S$, то подполето $T = M(a_1, a_2, \ldots, a_n)$ се съдържа в S. Ще докажем, че $S = T$.

Действително, понеже $T \leqq S \leqq L$ и $[L : S] = n!$, то $[L : T] \geqq n!$. Да разгледаме редицата

$$T = T_n \leqq T_{n-1} \leqq T_{n-2} \leqq \ldots \leqq T_1 \leqq T_0 = L \tag{1}$$

от подполета на L, където $T_i = T(x_{i+1}, x_{i+2}, \ldots, x_n) = T_{i+1}(x_{i+1})$. Тъй като $T_{i-1} = T_i(x_i)$, то за да се убедим, че $[T_{i-1} : T_i] \leqq i$ за $i = 1, 2, \ldots, n$, трябва да покажем, че степента на алгебричност на x_i над подполето T_i е не по-голяма от i. Да разгледаме полиномите

$$h_i(t) = \frac{g(t)}{(t - x_{i+1}) \ldots (t - x_n)} = \frac{h_{i+1}(t)}{t - x_{i+1}}$$

за $i<n$ и $h_n(t)=g(t)$. Ако извършим делението на $g(t)=t^n+a_1t^{n-1}+\ldots+a_n$ с полинома $(t-x_{i+1})(t-x_{i+2})\ldots(t-x_n)=t^{n-i}+\ldots$ по известното правило за деление на полиноми, то ще видим, че $h_i(t)$ е полином от степен i със старши коефициент единица, а останалите му коефициенти са полиноми на $a_1, a_2, \ldots, a_n, x_{i+1}, x_{i+2}, \ldots, x_n$, при което коефициентите на тези полиноми са цели числа. Затова $h_i(t)$ е полином с коефициенти от полето T_i. Но x_i е корен на $h_i(t)$ и минималният полином на x_i над T_i ще бъде делител на $h_i(T)$. Следователно степента на алгебричност на x_i над T_i е не по-голяма от i, т. е. $[T_{i-1}:T_i]\leqq i$. Но тогава

$$[L:T]=[T_0:T_1][T_1:T_2]\ldots[T_{n-1}:T_n]\leqq n!$$

и следователно $[L:T]=n!$. Полученото равенство показва, че $[S:T]=1$, което е равносилно на равенството $S=T$. Така получихме, че $S=M(a_1, a_2, \ldots, a_n)$, т. е. полето на симетричните рационални функции съвпада с полето от рационалните функции на елементарните симетрични полиноми на $x_1, x_2, \ldots, x_n$. Освен това от равенството $[S:T]=n!$ следват равенствата $[T_{i-1}:T_i]=i$, $i=1, 2, \ldots, n$. Затова полиномът $h_i(t)$ ще бъде минималният полином на x_i над подполето T_i, а $1, x_i, x_i^2, \ldots, x_i^{i-1}$ е базис на T_{i-1} над T_i и следните $n!$ еднočлена

$$x_1^{\nu_1}x_2^{\nu_2}\ldots x_n^{\nu_n},\quad 0\leqq\nu_i\leqq i-1 \tag{2}$$

образуват базис на полето L над подполето S.

Тъй като x_1 е корен на полинома $h_1(t)$, който е от степен 1 и старши коефициент 1, то x_1 се изразява като полином с цели коефициенти на $a_1, a_2, \ldots, a_n, x_2, x_3, \ldots, x_n$. Понеже $h_2(t)$ е полином със старши коефициент единица, то x_2^2 се изразява като полином с цели коефициенти на $a_1, a_2, \ldots, a_n, x_2, x_3, \ldots, x_n$ в който x_2 участвува най-много в първа степен. Тогава всички степени на x_2 ще се изразяват като целочислени полиноми на $a_1, \ldots, a_n, x_2, \ldots, x_n$, където x_2 е от степен $\leqq 1$. Също така от $h_3(x_3)=0$ получаваме, че всички степени на x_3 се изразяват като полиноми на $a_1, a_2, \ldots, a_n, x_3, \ldots, x_n$, в които x_3 участвува най-много във втора степен. Изобщо от $h_i(x_i)=0$ получаваме, че степените на x_i са полиноми с цели коефициенти на $a_1, a_2, \ldots, a_n, x_i, x_{i+1}, \ldots, x_n$, в които x_i участвува най-много в $(i-1)$-ва степен. Нека сега $g(x_1, x_2, \ldots, x_n)\in A$ е произволен полином на $x_1, x_2, \ldots, x_n$ над полето M. Като заместим в $g(x_1, x_2, \ldots, x_n)$ степените на променливите x_i със съответното им изразяване като полиноми на $a_1, \ldots, a_n, x_i, x_{i+1}, \ldots, x_n$ и извършим приведение, получаваме, че $g(x_1, x_2, \ldots, x_n)$ е линейна комбинация от елементите на базиса (2) с коефициенти, които са полиноми на $a_1, a_2, \ldots, a_n$, т. е. с коефициенти от пръстена $M[a_1, a_2, \ldots, a_n]$. Ако $g(x_1, x_2 \ldots, x_n)$ е от $B=A\cap S$, то, от една страна, $g(x_1, x_2, \ldots, x_n)$ се записва като тривиална линейна комбинация.

на базисните елементи от (2), т. е. в тази линейна комбинация коефициентът пред базисния елемент $1=x_1^0, x_2^0, \ldots, x_n^0$ е равен на $g(x_1, \ldots, x_n)$ и останалите коефициенти са равни на нула, а, от друга страна, всички коефициенти на тази линейна комбинация са полиноми на $a_1, a_2, \ldots, a_n$. Следователно симетричният полином $g(x_1, \ldots, x_n)$ се изразява като полином на $a_1, a_2, \ldots, a_n$ с коефициенти от M, т. е. $B=A\cap S\leqq M[a_1, a_2, \ldots, a_n]$. Обратното е очевидно — всеки полином на $a_1, \ldots, a_n$ е симетричен полином на $x_1, x_2, \ldots, x_n$. Следователно пръстенът $B=A\cap S$ съвпада с пръстена $M[a_1, a_2, \ldots, a_n]$, който е пръстенът от полиномите на елементарните симетрични полиноми на променливите $x_1, x_2, \ldots, x_n$. Полученото твърдение е точно основната теорема за симетричните полиноми на $x_1, x_2, \ldots, x_n$ над полето M.

Нека $u_1, u_2, \ldots, u_n$ са независими променливи, а $P=M(u_1, u_2, \ldots, u_n)$ е полето от рационалните функции на $u_1, u_2, \ldots, u_n$ над полето M.

Определение 13. Полиномът

$$f(x)=x^n+u_1x^{n-1}+u_2x^{n-2}+\ldots+u_{n-1}x+u_n$$

и уравнението $f(x)=0$ се наричат съответно *общ полином* и *общо уравнение* от n-та степен над полето P от рационалните функции на $u_1, u_2, \ldots, u_n$.

Интересуваме се от въпроса, дали общото уравнение от n-та степен е решимо в радикали над полето P. За получаването на отговор на този въпрос ще приложим теорията на Галоа. За целта трябва да намерим групата на Галоа на общото уравнение от n-та степен и да установим дали тя е разрешима група или не.

Нека K е поле на разлагане на общия полином $f(x)$ от n-та степен над полето P. Тогава

$$f(x)=(x-\xi_1)(x-\xi_2)\ldots(x-\xi_n) \tag{3}$$

и $K=P(\xi_1, \xi_2, \ldots, \xi_n)$. Коефициентите на $f(x)$ съвпадат с точност до знак със съответните елементарни симетрични полиноми на елементите $\xi_1, \xi_2, \ldots, \xi_n$, т. е.

$$u_i=(-1)^i\sum\xi_1\,\xi_2\ldots\xi_i,\quad i=1, 2, \ldots, n.$$

Нека $G_n=\mathrm{Gal}(K/P)$ е групата на Галоа на общото уравнение от n-та степен. Ако $n\leqq 4$, то $f(x)$ има не повече от 4 различни корена, а G_n е изоморфна на подгрупа на една от разрешимите симетрични групи S_1, S_2, S_3, S_4. Затова G_n при $n\leqq 4$ е разрешима група и общото уравение в тези четири случая е решимо в радикали. Всъщност този факт е известен и без прилагане на теорията на Галоа, тъй като познаваме формули, които изразяват в радикали корените на общото уравнение от степен $n\leqq 4$.

Ще докажем, че групата G_n е изоморфна на симетричната група S_n.

Да разгледаме пръстените $E=M[u_1, u_2, \ldots, u_n]$ и $B=$

$=M[a_1, a_2, \ldots, a_n]<L=M(x_1, x_2, \ldots, x_n)$. Тъй като $u_1, u_2, \ldots, u_n$ са независими променливи, то съществува хомоморфизъм ψ на E върху B, който на полином $h(u_1, u_2, \ldots, u_n)$ от E съпоставя елемента $h(a_1, a_2, \ldots, a_n)$ от B. За да докажем, че ψ е изоморфизъм, ще разглеждаме също подпръстена $F=M[x_1, x_2, \ldots, x_n]$ на полето L и подпръстена $H=M[\xi_1, \xi_2, \ldots, \xi_n]$ на полето K. Нека φ е хомоморфизъм на F върху H, който съпоставя на полинома $g(x_1, x_2, \ldots, x_n)$ от F елемента $g(\xi_1, \xi_2, \ldots, \xi_n)$ от H. Тъй като $a_1, a_2, \ldots, a_n$ са полиноми на $x_1, x_2, \ldots, x_n$, то B е подпръстен на F. По аналогични причини пръстенът E е подпръстен на H. Нека полиномът $h(u_1, u_2, \ldots, u_n)$ е от ядрото $\ker\psi$ на хомоморфизма ψ. Тогава $\psi(h(x_1, x_2, \ldots, x_n))=h(a_1, a_2, \ldots, a_n)=0$ в пръстена B, който е подпръстен на F. Затова

$$0=\varphi(h(a_1, a_2, \ldots, a_n)=h(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n)).$$

Да забележим сега, че

$$\varphi(a_i)=\varphi\left((-1)^i \sum x_1 x_2 \ldots x_i\right)=(-1)^i \sum \xi_1\xi_2 \ldots \xi_i = u_i,$$

където $i=1, 2, \ldots, n$. Оттук получаваме равенството $0=h(u_1, u_2, \ldots, u_n)$ в пръстена E. Това показва, че $\ker\psi=(0)$ и ψ е изоморфизъм на пръстена E върху пръстена B на симетричните полиноми на $x_1, x_2, \ldots, x_n$. Изоморфизмът $\psi: E=M[u_1, u_2, \ldots, u_n]\to B=M[a_1, \ldots, a_n]$ се разширява до изоморфизъм $\bar{\psi}$ на полето $P=M(u_1, u_2, \ldots, u_n)$ от частни на E върху полето $S=M(a_1, a_2, \ldots, a_n)$ от частни на пръстени B. Тъй като при изоморфизма ψ на полинома $f(x)$ от (3) съответствува полиномът $g(x)=x^n+a_1x^{n-1}+\ldots+a_n$, а K е полето на разлагане на $f(x)$ над P и L е полето на разлагане на $g(x)$ над S, то по теорема 7 на глава VIII изоморфизмът $\bar{\psi}$ се разширява до изоморфизъм τ на полето K върху полето L. При този изоморфизъм корените на полинома $f(x)$ ще преминават в корените на полинома $g(x)$, т. е. след евентуална преномерация на корените на полинома $f(x)$ ще имаме $\tau(\xi_i)=x_i$ за $i=1, 2, \ldots, n$. Ограничението на изоморфизма τ върху пръстена H е изоморфизъм (над полето M) на H върху F, който изобразява множеството $\{\xi_1, \xi_2, \ldots, \xi_n\}$ върху множеството $\{x_1, x_2, \ldots, x_n\}$. Така ние получихме следните две твърдения:

1. *Елементарните симетрични полиноми на независимите променливи $x_1, x_2, \ldots, x_n$ са алгебрично независими над полето M.*

2. *Корените $\xi_1, \xi_2, \ldots, \xi_n$ на общия полином от n-та степен са алгебрично независими над полето M.*

Забележка. Сега вече е очевидно, че разглежданият по-горе хомоморфизъм φ е изоморфизъм.

Лесно се проверява, че съответствието, което на всяко σ от групата G_n съпоставя $\tau\sigma\tau^{-1}$, който е елемент на групата S_n (отъждествена по посочения по-горе начин с подгрупа на групата

Aut L от автоморфизмите на полето L), е изоморфизмът на G_n върху S_n. Така доказахме следната

Теорема 16. *Групата на Галоа на общото уравнение от n-та степен е изоморфна на симетричната група* S_n.

От теорема 8 и теорема 13 тогава се получава прочутата теорема на Руфини — Абел:

Теорема 17 (Руфини — Абел). *Ако характеристиката на разглежданите полета е нула и* $n \geqq 5$, *то общото уравнение от n-та степен е нерешимо в радикали.*

ДОПЪЛНЕНИЕ

§ 1. Множества. Операции над множества

Понятието множество е едно от основните понятия в математиката. Затова за него не може да бъде дадено строго определение. Обикновено понятието множество се пояснява с примери, а след това се посочват правилата за използуването му в математическите разсъждения. Този подход към термина множество се нарича интуитивен.

Теорията на множествата е тази част от математиката, която изследва общите свойства на множествата независимо от природата на тяхните елементи. Създаването на тази теория е дело на Георг Кантор и се отнася към годините 1871—1883. Той се е придържал именно към интуитивния подход към понятието множество. Този подход обаче се е оказал ненадежден. Свободното боравене с понятието множество, основано само на интуицията, е довело твърде бързо до появата на тъй наречените *антиномии* (противоречия) в теорията на множествата. Те се отстраняват в аксиоматичната теория на множествата. Понастоящем съществуват различни методи за аксиоматизация на теорията на множествата, но тяхното разглеждане би ни отвело твърде далеч от целта ни да изложим основите на съвременната алгебра.

За нашата цел ще бъде достатъчно да използуваме само интуитивния подход и да застанем на позициите на тъй наречената „наивна теория на множествата".

Когато разглеждаме някои обекти или понятия, които имат дадено общо свойство, то мислено можем да образуваме нов обект — множеството M на тези обекти. За разглежданите обекти казваме, че са *елементи* на множеството M или че *принадлежат* на M. Съждението, че елементът a принадлежи на множеството M (или M *съдържа* a), ще записваме чрез $a \in M$ (или $M \ni a$). Ако b не принадлежи на множеството M (т. е. b не е елемент на M), то ще записваме $b \notin M$ (или $M \not\ni b$).

Удобно е да се въведе понятието празно множество, т. е. множество, което не съдържа никакъв елемент. Празното множество ще бележим със знака $\emptyset$. Например множеството от всички реални корени на уравнението $x^2+1=0$ е празно. Примери за множества са множествата N, Z, Q, R и C съответно на естествените, целите, рационалните, реалните и комплексните числа.

Две множества A и B се наричат *равни* тогава и само тогава, когато те са съставени от едни и същи елементи, т. е. когато елементите на A са елементи на B и обратно. Ако множествата A, B са равни, то това записваме като $A=B$

Ако всеки елемент на множеството A е елемент на множеството B, то A се нарича *подмножество* на B и записваме $A \subseteq B$ или $B \supseteq A$. За подмножеството A на множеството B казваме също, че A *се съдържа в* B.

Очевидно празното множество $\emptyset$ е подмножество на всяко множество. Всяко множество A е подмножество на себе си, т. е. $A \subseteq A$.

Множеството M, на което всички елементи са $a_1, a_2, \ldots, a_n$, ще означаваме с $M = \{a_1, a_2, \ldots, a_n\}$.

Ако A е множество, а $E(x)$ е някакво свойство, то елементите от A, които притежават свойството $E(x)$, образуват подмножество M на A, което се бележи с

$$M = \{a \mid a \in A,\ E(a)\}.$$

Например $\{x \mid x \in \mathbf{N},\ 10 < x\}$ е множеството от естествените числа, по-големи от 10.

Всички подмножества на дадено множество A образуват също множество, което се бележи с $P(A)$.

Задача. Докажете, че ако множеството A има n елемента, то $P(A)$ има 2^n различни елемента.

Ако $A = \emptyset$, то $P(A)$ е едноелементното множество $\{\emptyset\}$, чийто единствен елемент е празното множество $\emptyset$. Ако A е едноелементно множество, то A и $\emptyset$ са елементите на $P(A)$.

Обединение, или *сума*, $A \cup B$ на множествата A и B се нарича множеството от всички елементи, които принадлежат на поне едно от дадените множества A, B, т. е.

$$A \cup B = \{x \mid x \in A \text{ или } x \in B\}.$$

Обединението на произволен брой множества се определя по аналогичен начин.

Сечение, или *обща част*, $A \cap B$ на две множества A и B се нарича множеството от всички елементи, които едновременно се съдържат в A и B, т. е.

$$A \cap B = \{x \mid x \in A,\ x \in B\}.$$

По същия начин се определя и *сечението на произволен брой множества.*

Разбира, се сечението $A \cap B$ може да бъде празното множество. Ако $A \cap B = \emptyset$, то казваме, че A и B са *непресичащи се* или че A и B *са чужди* помежду си.

Разлика $A \setminus B$ на множествата A и B се определя с формулата

$$A \setminus B = \{x \mid x \in A,\ x \overline{\in} B\}.$$

От това определение следват непосредствено следните равенства

$$A \setminus A = \emptyset,\ A \setminus \emptyset = A,\ \emptyset \setminus A = \emptyset.$$

Когато множеството B се съдържа в A, то разликата $A \setminus B$ се нарича *допълнение* на B в A и се бележи с $C_A(B)$. За допъл-

нението на B в A са изпълнени равенствата $A=B\cup C_A(B)$ и $B\cap C_A(B)=\varnothing$.

Ако A, B, C са произволни множества, то за така въведените операции са изпълнени следните закони:

1. $A\cup A=A$, $A\cap A=A$ — *идемпотентност на обединението и сечението;*

2. $A\cup B=B\cup A$, $A\cap B=B\cap A$ — *комутативност;*

3. $(A\cup B)\cup C=A\cup(B\cup C)$, $(A\cap B)\cap C=A\cap(B\cap C)$ — *асоциативност;*

4. $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$, $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ — *дистрибутивност на обединението спрямо сечението и дистрибутивност на сечението спрямо обединението;*

5. $A\setminus(B\cup C)=(A\setminus B)\cap(A\setminus C)$, $A\setminus(B\cap C)=(A\setminus B)\cup(A\setminus C)$ — разликата „антиразделя“ обединението и сечението;

6. *Ако* $B\subseteq A$, *то* $C_A(C_A(B))=B$.

Доказателството на всеки един от тези закони използува само дадените по-горе определения. Като пример ще приведем само доказателството на първото равенство от 5.

Нека $x\in A\setminus(B\cup C)$. Тогава $x\in A$ и $x\overline{\in}B\cup C$, т. е. $x\in A$, $x\overline{\in}B$ и $x\overline{\in}C$. Но $x\in A$ и $x\overline{\in}B$ означава, че $x\in A\setminus B$. Аналогично $x\in A$ и $x\overline{\in}C$ означава, че $x\in A\setminus C$, т. е. $x\in(A\setminus B)\cap(A\setminus C)$. Тъй като x е произволен елемент от $A\setminus(B\cup C)$, то доказахме включването

$$A\setminus(B\cup C)\subseteq(A\setminus B)\cap(A\setminus C).$$

Обратно, ако y е елемент от сечението $(A\setminus B)\cap(A\setminus C)$, то $y\in A\setminus B$ и $y\in A\setminus C$. Затова $y\in A$, $y\overline{\in}B$ и $y\overline{\in}C$. Тъй като $y\overline{\in}B$ и $y\overline{\in}C$ то $y\overline{\in}B\cup C$. Но $y\in A$ и $y\overline{\in}B\cup C$ влекат $y\in A\setminus(B\cup C)$, т. е. имаме включването

$$(A\setminus B)\cap(A\setminus C)\subseteq A\setminus(B\cup C).$$

От определението за равенство на две множества получаваме

$$A\setminus(B\cup C)=(A\setminus B)\cap(A\setminus C).$$

Останалите закони се доказват по подобен начин.

§ 2. Декартово произведение. Двучленни релации. Изображения

Ако x и y са два обекта, то можем да образуваме нов обект (x, y), които се нарича *наредена двойка* с *първа компонента (проекция)* x и *втора компонента (проекция)* y.

Две наредени двойки (x, y) и (z, t) се наричат *равни* тогава и само тогава, когато $x=z$ и $y=t$. В общия случай наредената двойка (x, y) не е равна на наредената двойка (y, x). Например $(0, 1)\neq(1, 0)$. Следва да различаваме наредената двойка (x, y) от множеството $\{x, y\}$; елементите на което са x и y.

Определение 1. *Декартово произведение* $A\times B$ на множе-

ствата A, B наричаме множеството от всички наредени двойки с първа компонента (проекция) — елемент от A, и втора компонента — елемент от B, т. е.

$$A\times B=\{(a,\ b)\,|\,a\in A,\ b\in B\}.$$

Например, ако $A=\{0,\ 1\}$ и $B=\{1,\ 3\}$ то

$$A\times B=\{(0,\ 1),\ (0,\ 3),\ (1,\ 1),\ (1,\ 3)\}.$$

Ако $B=A$, то декартовото произведение $A\times A$ се бележи с A^2 и се нарича *декартов квадрат* на множеството A.

Задача. Докажете, че ако A има $m\geqq 1$ елемента, а B има $n\geqq 1$ елемента, то декартовото произведение $A\times B$ се състои от mn елемента.

Задача. Нека A и B са непразни множества. Докажете, че $A\times B=B\times A$ тогава и само тогава, когато $A=B$.

За декартовото произведение на множества не е изпълнен асоциативният закон, т. е. ако A, B и C са множества, то множествата $(A\times B)\times C$ и $A\times(B\times C)$ не са задължени да съвпадат.

Задача. а) Докажете, че декартовото произведение $A\times B$ на множествата A, B е празното множество тогава и само тогава, когато $A=\emptyset$ или $B=\emptyset$.

б) Докажете, че за множествата A, B, C имаме равенството $(A\times B)\times C=A\times(B\times C)$ точно тогава, когато поне едно от A, B, C е празното множество.

В математиката често се налага да се разглеждат *твърдения (релации)*, в които участвуват неизвестни, след заместването на които с конкретни обекти се получава вярно или невярно твърдение. Например $x=y$ и $x<y$ са две релации, които зависят от две неизвестни, а $0<x$ е релация, която зависи от една променлива. Релациите, които зависят от една променлива, се наричат *унарни (едноместни)*, а тези, които зависят от две променливи се наричат *бинарни (двуместни)*.

Ако ρ е бинарна релация, която зависи от променливите x и y, и при всяко заместване на x и y с елементи на множеството A се получава вярно или неверно твърдение, то ще казваме, че ρ е определена в множеството A. Ще казваме, че елементът a от A е в релация ρ с елемента b от A, и ще записваме $a\rho b$, ако след заместването $x=a$, $y=b$ се получава от ρ вярно твърдение. Ако за елементите a, b от A е вярно поне едно от твърденията $a\rho b$ и $b\rho a$, то казваме, че a и b *са сравними относно (по модул) релацията* ρ. На бинарната релация ρ можем да съпоставим подмножеството $M(\rho)$ на скаларния квадрат A^2, което се определя с формулата

$$M(\rho)=\{(a,\ b)\,|\,(a,\ b)\in A^2,\ a\rho b\}.$$

Ако познаваме елементите на подмножеството $M(\rho)$, то знаем точно за кои двойки $(a,\ b)\in A^2$ е вярно твърдението $a\rho b$ и следователно познаваме и релацията ρ. Така между подмножествата на A^2 и бинарните релации в множеството A се получава взаимно

еднозначно съответствие. Поради това съответствие често под бинарна релация ρ в множеството A се разбира подмножество M на скаларния квадрат A^2, като се подразбира, че $a\rho b$ е вярно точно тогава, когато $(a, b) \in M$.

Примери

1. На релацията „равенство“ $(x = y)$ отговаря диагоналът $M(=) = \{(a, b) \ (a, b) \in A^2, \ a = b\} = \{(a, a) \mid a \in A\}$ на скаларния квадрат A^2.

2. На релацията $x + y = 0$ в множеството $\mathbf{Z}$ на целите числа отговаря подмножеството $\{(n, -n) \mid n \in \mathbf{Z}\}$ на декартовия квадрат $\mathbf{Z}^2$, а на същата релация в множеството от неотрицателните цели числа отговаря едноелементното подмножество $\{(0, 0)\}$.

Понятието *изображение (функция, съответствие)* на множеството A в множеството B (глава IV, § 2) е частен случай на бинарна релация. Наистина съответствието f на A в B може да се определи като бинарна релация на множеството $C = A \cup B$ със свойствата:

1) ако за $x, y \in C$ е изпълнено xfy, то $x \in A$ и $y \in B$;

2) за всяко $x \in A$ съществува един-единствен елемент $y \in B$, така че xfy.

Посоченият подход към изображенията обаче не е удобен за записване и работа със самите изображения.

Нека ρ е бинарна релация в множеството A. Ще казваме, че ρ е *рефлексивна релация*, ако за всяко a от A е в сила $a\rho a$. Релацията ρ се нарича *симетрична*, ако за всички $x, y \in A$ от $x\rho y$ следва $y\rho x$, а ρ се нарича *антисиметрична*, ако от едновременното изпълнение на $x\rho y$ и $y\rho x$ следва равенството $x = y$. Релацията ρ се нарича *транзитивна*, ако за всички $x, y, z \in A$ от $x\rho y$ и $y\rho z$ следва $x\rho z$. Посочените свойства могат да се определят и с помощта на подмножеството $M = M(\rho)$ на A^2;

1. *Рефлексивност:* $(a, a) \in M$ *за всяко* $a \in A$.

2. *Симетричност: от* $(x, y) \in M$ *следва* $(y, x) \in M$ *за всички* x, y от A.

3. *Антисиметричност: ако* $(x, y) \in M$ *и* $(y, x) \in M$, то $x = y$.

4. *Транзитивност: ако* $(x, y) \in M$ *и* $(y, z) \in M$, *то* $(x, z) \in M$.

§ 3. Релации на еквивалентност

Определение 2. Бинарната релация ρ на множеството A се нарича *релация на еквивалентност*, ако тя е рефлексивна, симетрична и транзитивна, т. е. ако за всички a, b, c от A са в сила твърденията

1) $a\rho a$,

2) от $a\rho b$ следва $b\rho a$,

3) от $a\rho b$ и $b\rho c$ следва $a\rho c$.

Примери:

1. Релацията равенство е релация на еквивалентност.

2. Скаларният квадрат $A^2 = A \times A$ определя релация на еквивалентност на A.

3. Ако A е множеството от всички прави в тримерното пространство, то подмножеството

$$M=\{(x, y) \mid x, y \in A, \ : \| y \text{ или } x=y\}$$

определя релация на еквивалентност на A, която се бележи с $\|$ и се нарича „обобщена успоредност на прави".

4. *Разбиване* на множеството A се нарича всяко представяне на A като обединение на непресичащи се подмножества на A. Ако $A=\bigcup_{i \in I} A_i$ е произволно разбиване на множеството A, то подмножествата A_i на A се наричат *класове* на разбиването. С помощта на дадéното разбиване на A се определя релация ρ:

$x \rho y$ е вярно точно тогава, когато елементите x и y се съдържат в един и същ клас A_i на разбиването.

Така дефинираната релация ρ е релация на еквивалентност. За тази релация ще казваме, че тя *отговаря на даденото разбиване* на A.

5. Ако $f: A \to B$ е изображение на множеството A в някое множество B, то да означим с ρ_f релацията, която се определя по следния начин:

$x \rho_f y$ е вярно тогава и само тогава, когато $f(x)=f(y)$.

Релацията ρ_f е релация на еквивалентност.

Всъщност, както ще видим по-нататък, примерите 4 и 5 са *универсални*, т. е. *всяка релация на еквивалентност ρ на A може да се получи по начините, описани в тези примери.*

Определение 3. Ако ρ е релация на еквивалентност на множеството A и a е елемент на A, то подмножеството на A от всички елементи x със свойството $a \rho x$ ще бележим с $[a]$ и ще го наричаме *клас на еквивалентност по модул* ρ, който е определен от a.

Твърдение 1. *Нека ρ е релация на еквивалентност на множеството A. Тогава*

а) *всеки елемент $a \in A$ се съдържа в класа $[a]$;*

б) *ако $b \in [a]$, то $[b]=[a]$;*

в) *два класа на еквивалентност по модул ρ или съвпадат или са непресичащи се.*

Доказателство. а) Понеже ρ е рефлексивна релация, то за всяко $a \in A$ е изпълнено $a \rho a$ и затова $a \in [a]$.

б) Нека $b \in [a]$. Тогава е изпълнено $a \rho b$, а това влече $b \rho a$, понеже релацията е симетрична.

Ако $x \in [a]$, то $a \rho x$ е изпълнено. От транзитивността на ρ и от $b \rho a$, $a \rho x$ следва $b \rho x$, т. е. $x \in [b]$. Следователно изпълнено е включването $[a] \subseteq [b]$. Обратното включване се получава аналогично, т. е. $[a]=[b]$.

в) Нека класовете $[a]$ и $[b]$ се пресичат и нека $c \in [a] \cap [b]$. Тогава от твърдение б) следва, че $[a]=[c]=[b]$, т. е. $[a]=[b]$. Твърдението е доказано.

Теорема 1. *Ако ρ е релация на еквивалентност на множеството A, то различните класове на еквивалентност по модул ρ определят разбиване на множеството A, а релацията, която отговаря на това разбиване, съвпада с релацията ρ.*

Доказателство От твърдение 1 знаем, че всеки елемент a от A се съдържа точно в един клас на еквивалентност по модул ρ, а именно в класа $[a]$. Затова различните класове на еквивалентност по модул ρ определят разбиване на A.

Ако σ е релацията, която отговаря на това разбиване, то от определението на σ знаем, че $x\sigma y$ е изпълнено точно тогава, когато x и y се съдържат в един и същи клас $[a]$. От $x\in[a]$ и $y\in[a]$ следват $a\rho x$ и $a\rho y$. Като използуваме симетричността и транзитивността на ρ, получаваме $x\rho y$.

Ако пък $x\rho y$ е изпълнено, то $y\in[x]$ и от твърдение 1 имаме $x\in[x]=[y]\ni y$, което показва, че $x\sigma y$ е също изпълнено. Следователно двете релации σ и ρ съвпадат. Теоремата е доказана.

Ако ρ е релация на еквивалентност на множеството A, то класовете на еквивалентност по модул ρ образуват множество, което се означава с A/ρ и се нарича *фактор-множество* на A по релацията на еквивалентност ρ. Изображението φ на A във фактор-множеството A/ρ, което съпоставя на всяко a от A класа на еквивалентност $[a]$, се нарича *канонично изображение*. Елементът a от A се нарича *представител* на класа $\varphi(a)=[a]$.

Задача. а) Докажете, че каноничното изображение $\varphi: A\to A/\rho$ е изображение на A върху A/ρ.

б) Докажете, че φ е взаимно еднозначно изображение на A върху A/ρ тогава и само тогава, когато релацията ρ съвпада с релацията равенство на A.

в) Докажете, че релацията ρ_φ (пример 5) съвпада с релацията ρ

§ 4. Естествени числа. Математична индукция

Множеството $\mathbf{N}=\{1, 2, \ldots, n, \ldots\}$ на естествените числа е един от най-важните обекти в математиката. Неговото строго математично определение и доказателството на основните свойства на естествените числа се постигат със системата от аксиоми на Д. Пеано (1858—1932). Тъй като разглеждането на този кръг от въпроси излиза вън от рамките на настоящия учебник, то ще се базираме върху знанията, придобити в училищния курс по математика. Като начало ще изброим някои от основните свойства на естествените числа

1) *Ако* $a, b\in\mathbf{N}$, *то* $a+b\in\mathbf{N}$, *т. е. множеството на естествените числа е затворено относно операцията събиране.*

2) *Ако* $a, b\in\mathbf{N}$, *то* $a+b=b+a$ (*комутативност на събирането*).

3) *Ако* $a, b, c\in\mathbf{N}$, *то* $(a+b)+c=a+(b+c)$ (*асоциативност на събирането*).

4) *Ако* $a, b\in\mathbf{N}$, *то* $ab\in\mathbf{N}$, *т. е. множеството на естествените числа е затворено относно операцията умножение.*

5) *Ако* $a, b\in\mathbf{N}$, *то* $ab=ba$ (*комутативност на умножението*).

6) *Ако* $a, b, c\in\mathbf{N}$, *то* $a(bc)=(ab)c$ (*асоциативност на умножението*).

7) Ако $a, b, c \in \mathbf{N}$, то $(a+b)c=ac+bc$ (дистрибутивен закон, който свързва операциите събиране и умножение).

По-нататък с $\mathbf{N}(+, .)$ ще означаваме множеството на естествените числа, разглеждано заедно с операциите събиране и умножение. По аналогичен начин въвеждаме и означението $\mathbf{N}(+)$ или $\mathbf{N}(.)$. Всяко множество $S(+, .)$, което удовлетворява условията 1)—7), се нарича *комутативен полупръстен*. Следователно, вместо подробно да изброяваме, че множеството на естествените числа удовлетворява условията от 1) до 7), накратко ще казваме, че $\mathbf{N}(+, .)$ е комутативен полупръстен.

Ще посочим още някои свойства на естествените числа.

8) ***Ако $a, b, c \in \mathbf{N}$ и $a+c=b+c$, то $a=b$ (закон за съкращаване при събирането).***

Ако $a, b, c \in \mathbf{N}$ и $ac=bc$, то $a=b$ (закон за съкращаване при умножението).

Разлика на естествените числа a и b се нарича такова естествено число $k \in \mathbf{N}$, за което $a=b+k$.

Лесно се вижда, че ако съществува разлика на естествените числа a и b, то тя е единствена. Действително ако $a=b+k$ и $a=b+r$, то $b+k=b+r$, откъдето съгласно свойството 8) следва, че $k=r$.

Единственото естествено число k, което е разлика на $a, b \in \mathbf{N}$, се означава с $k=a-b$.

Очевидно е, че не всеки две естествени числа притежават разлика в $\mathbf{N}$. Нещо повече, ако a и b имат разлика в $\mathbf{N}$, то b и a нямат разлика в $\mathbf{N}$. Този „дефект“ на $\mathbf{N}$ е първата причина да се търси разширение на множеството на естествените числа.

Ако за естествените числа a и b съществува число $k \in \mathbf{N}$, за което $a+k=b$, то ще казваме, че „*a е по-малко от b*“, и записваме $a<b$. В този случай се казва още, че „*b е по-голямо от a*“, и записваме $b>a$.

10) *За всеки две естествени числа a и b е изпълнено точно едно от следните три условия:*

$a<b$, $a=b$ или $a>b$ (закон за трихотомия на релацията $<$).

11) *Ако $a, b, c \in \mathbf{N}$, то $a<b$ тогава и само тогава, когато $a+c<b+c$ (или $ac<bc$).*

12) *Всяко непразно подмножество на $\mathbf{N}$ притежава най-малък елемент.*

Нека още един път отбележим, че посочените свойства на естествените числа следват от три аксиоми на Пеано, но ние ги приемаме като интуитивно ясни. Без да се впускаме в повече подробности, накрая ще покажем как от свойството 12) следва много често използуваният принцип на пълната индукция, въведем в математиката от Б. Паскал (1623—1662) и Я. Бернули (1654—1705).

Теорема 2. (Принцип на пълната индукция). *Ако твърдението $\mathcal{A}(n)$ удовлетворява условията:*

1) *$\mathscr{A}(k)$ е вярно за $n=1$ и*

2) *от допускането, че то е вярно за всяко $n \leqq k-1$, следва вярността му за $n=k$,*

то това твърдение е вярно за всяко $n \in \mathbf{N}$.

Доказателство. Да допуснем, че множеството

$$S=\{s \mid s \in \mathbf{N},\ A(s) \text{ е невярно твърдение}\}$$

от естествени числа е непразно. Съгласно свойство 12) S притежава минимален елемент k, при което $k>1$, защото $\mathscr{A}(1)$ е вярно твърдение. Тогава твърдението $\mathscr{A}(k)$ е невярно, а всички твърдения $\mathscr{A}(1), \mathscr{A}(2), \ldots, \mathscr{A}(k-1)$ са верни, понеже числата $1, 2, \ldots, k-1$ не принадлежат на S. Но това противоречи на условието 2). Следователно S е празно подмножество на $\mathbf{N}$ и $\mathscr{A}(n)$ е вярно твърдение за всяко $n \in \mathbf{N}$. Теоремата е доказана.

Тук нямаме възможност по-подробно да обсъждаме принципа на пълната математична индукция, но ще отбележим, че той допуска и други еквивалентни формулировки и с успех може да се прилага за доказване на твърдения, които зависят не от едно, а едновременно от няколко естествени числа. Например *принципът на двойната индукция се състои в следното:*

Нека на всеки две естествени числа m и n е съпоставено твърдението $\mathscr{A}(m, n)$, при което:

1) *$\mathscr{A}(m, 1)$ и $\mathscr{A}(1, n)$ са верни твърдения за всички $m, n \in \mathbf{N}$*

2) *ако $\mathscr{A}(k-1, l)$ и $\mathscr{A}(k, l-1)$ са верни, то $\mathscr{A}(k, l)$ е също вярно твърдение. Тогава $\mathscr{A}(m, n)$ е вярно твърдение за всички естествени числа m и n.*

Често пъти се налага по индукция да се доказват твърдения $\mathscr{A}(n)$, които са верни не за всяко $n \in \mathbf{N}$, а само при $n \geqq r$, където $r \in \mathbf{N}$ е дадено число. Тогава, за да приложим теоремата вместо твърдението $\mathscr{A}(1)$, необходимо е да проверим верността на твърдението $\mathscr{A}(r)$.

Пример. Да се покаже, че за всяко естествено число $n \geqq 2000$ е изпълнено неравенството $n^3-4>1000\,n^2+3n$.

Непосредствено се проверява, че при $n=2000$ неравенството е изпълнено. Да допуснем, че то е изпълнено при някое $n=k \geqq 2000$. Ако в даденото неравенство положим $n=k+1$, то в лявата част на неравенството при $n=k$ ще се добави изразът $3k^2+3k+1$, а в дясната част ще се добави $2000\,k+1003$. Всичко ще бъде доказано, ако докажем верността на помощното неравенство $3k^2+3k+1 \geqq 2000\,k+1003$ при $k \geqq 2000$. Последното неравенство лесно се доказва също по метода на пълната индукция.

Този пример показва, че понякога условието (2) е също целесъобразно да се проверява чрез пълна индукция. При това може да възникне верига от индуктивни доказателства на твърдения, всяко от които е по-просто от предхождащото го.

§ 5. Пръстен на целите числа

Вече споменахме, че не всеки две естествени числа имат разлика в N, т. е. уравнението $a=b+x$ ($a, b \in \mathbf{N}$) невинаги има решение в N.

Комутативен полупръстен $S(+, .)$, в който уравнението $a=b+x$ има единствено решение в S за всяко $a, b \in S$, се нарича *комутативен пръстен*. Единственото решение на уравнението $a=b+x$ се нарича *разлика* на елементите a и b и се означава с $a-b$.

Очевидно е, че всеки пръстен е същевременно и полупръстен.

Нашата задача е да докажем, че съществува такъв комутативен пръстен $\mathbf{Z}(\oplus, \odot)$ с операции $\oplus$ и $\odot$, който притежава следните свойства:

А) *полупръстенът* $\mathbf{N}(+, .)$ *се влага в полупръстена* $\mathbf{Z}(\oplus, \odot)$;

В) *всеки елемент от* $\mathbf{Z}$ *може да се представи като разлика на елементи от образа на* N *в* Z.

Ще поясним какво по-точно означават условията А) и В).

Условието А) означава, че Z притежава такова подмножество $\overline{\mathbf{N}}$, за което $\overline{\mathbf{N}}(\oplus, \odot)$ е полупръстен, и освен това съществува такова взаимно еднозначно изображение $\varphi: \mathbf{N} \to \overline{\mathbf{N}}$ на N върху $\overline{\mathbf{N}}$, което е съгласувано с операциите в N и $\overline{\mathbf{N}}$, т. е.

$$\varphi(a+b)=\varphi(a) \oplus \varphi(b), \quad \varphi(ab)=\varphi(a) \odot \varphi(b)$$

за всички $a, b \in \mathbf{N}$.

Условието В) означава, че за всяко $z \in \mathbf{Z}$ могат да се намерят елементи $a, b \in \mathbf{N}$, за които $z=\varphi(a) \ominus \varphi(b)$.

Всеки пръстен, който притежава свойствата А) и В), се нарича *пръстен на целите числа*, а неговите елементи — *цели числа*.

Ще докажем следната

Теорема 3. *Съществува поне един пръстен на целите числа.*

Доказателство. В множеството $\mathbf{N} \times \mathbf{N}=\{(a, b) \mid a, b \in \mathbf{N}\}$ въвеждаме релация $\sim$ по следния начин: $(a, b) \sim (c, d)$ тогава и само тогава, когато $a+d=c+b$.

Непосредствена проверка показва, че релацията $\sim$ е релация на еквивалентност на $\mathbf{N} \times \mathbf{N}$, т. е.

1) $(a, b) \sim (a, b)$;

2) ако $(a, b) \sim (c, d)$, то $(c, d) \sim (a, b)$ и

3) ако $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$, то $(a, b) \sim (e, f)$.

Съгласно теорема 1 релацията $\sim$ разбива множеството $\mathbf{N} \times \mathbf{N}$ на непресичащи се класове от еквивалентни помежду си наредени двойки. Нека Z е фактор-множеството $(\mathbf{N} \times \mathbf{N}) / \sim$. С $[a, b]$ ще бележим класа на еквивалентност с представител (a, b).

В множеството Z дефинираме операции събиране $\oplus$ и умножение $\odot$, като полагаме

$$(1)\qquad \begin{aligned}[a, b]\oplus[c, d]&=[a+c, b+d].\\ [a, b]\odot[c, d]&=[ac+bd, ad+bc].\end{aligned}$$

Тук най-напред трябва да докажем, че операциите $\oplus$ и $\odot$ не зависят от избора на представителите на съответните класове. Действително нека $[a, b]=[a_1, b_1]$ и $[c, d]=[c_1, d_1]$. Необходимо е да се провери, че

$$(2)\qquad [a+c, b+d]=[a_1+c_1, b_1+d_1],$$

$$(3)\qquad [ac+bd, ad+bc]=[a_1c_1+b_1d_1, a_1d_1+b_1c_1[.$$

Наистина от $[a, b]=[a_1, b_1]$ следва, че $(a, b)\sim(a_1, b_1)$ и $a+b_1=a_1+b$. По същия начин получаваме, че $c+d_1=c_1+d$. Като съберем почленно тези две равенства, стигаме до извода, че $(a+c, b+d)\sim(a_1+c_1, b_1+d_1)$, с което верността на равенството (2) е проверена. За да установим и равенството (3), трябва да покажем, че наредените двойки $\alpha=(ac+bd, ad+bc)$ и $\alpha_1=(a_1c_1+b_1d_1, a_1d_1+b_1c_1)$ са еквивалентни. Но това следва от факта, че те поотделно са еквивалентни на наредената двойка $\beta=(ac_1+bd_1, ad_1+bc_1)$. Действително $\alpha\sim\beta$ точно тогава, когато е изпълнено условието $ac+bd+ad_1+bc_1=ac_1+bd_1+ad+bc$, а то следва от равенствата $c+d_1=c_1+d$ и $c_1+d=c+d_1$, като ги умножим съответно с a и b, а след това почленно ги съберем. По аналогичен начин се проверява и релацията $\alpha_1\sim\beta$.

За да покажем, че $Z(\oplus, \odot)$ е комутативен полупръстен, необходимо е да се докаже, че елементите на Z и операциите $\oplus$ и $\odot$ удовлетворяват условията 1) —7) от предния параграф, което се извършва без затруднения, като вместо знаците за събиране и умножение на естествени числа поставим съответно $\oplus$ и $\odot$ и използуваме тяхното определение от (1).

Нека $[a, b]$ и $[c, d]$ са произволни елементи от Z. Ще покажем, че уравнението

$$(4)\qquad [a, b]=[c, d]\oplus x$$

има едно-единствено решение в Z.

С непосредствена проверка се вижда, че $x_1=[a+d, b+c]$ е решение на (4). Ако $x_2=[u, v]\in Z$ е произволно решение на (4), то от равенството $[a, b]=[c, d]\oplus[u, v]$ следва, че наредените двойки (a, b) и $(c+u, d+v)$ са еквивалентни, т. е. $a+d+v=c+b+u$. Но това равенство показва, че наредените двойки (u, v) и $(a+d, b+c)$ също са еквивалентни, поради което $x_2=[u, v]=[a+d, b+c]=x_1$, т. е. x_1 е единствено решение на (4), а полупръстенът $Z(\oplus, \odot)$ е комутативен пръстен.

Единственото решение на уравнението (4) се нарича *разлика* на елементите $[a, b]$ и $[c, d]$, което ще означаваме $[a, b]\ominus[c, d]$. Следователно

$$(5)\qquad [a, b]\ominus[c, d]=[a+d, b+c].$$

Остава да се докаже, че пръстенът $Z(\oplus, \odot)$ притежава свойствата A) и B). За тази цел полагаме

$$\bar{\mathbf{N}}=\{(a+1,1)\mid a\in\mathbf{N}\}\subset Z.$$

Тъй като

(6) $[a+1,\ 1]\oplus[b+1,\ 1]=[a+b+2,\ 2]=[a+b+1,\ 1]\in\bar{\mathbf{N}}$,

(7) $[a+1,\ 1]\odot[b+1,\ 1]=(ab+a+b+2,\ a+b+2]=[ab+1,\ 1]\in\bar{\mathbf{N}}$,

то подмножеството **N** е затворено относно операциите $\oplus$ и $\odot$. Останалите условия от 1) до 7) (вж. предишния параграф) също, се удовлетворяват от елементите на $\bar{\mathbf{N}}$, защото те се удовлетворяват от всички елементи на **Z**.

Нека $\varphi:\mathbf{N}\to\bar{\mathbf{N}}$ е изображение на **N** в $\bar{\mathbf{N}}$, при което $\varphi(a)=[a+1,\ 1]$ за всяко $a\in\mathbf{N}$. Лесно се проверява, че φ е взаимно еднозначно изображение на **N** върху $\bar{\mathbf{N}}$. Тогава

$$\varphi(a+b)=[a+b+1,\ 1]=[a+1,\ 1]\oplus[b+1,\ 1]=\varphi(a)\oplus\varphi(b),$$

където второто равенство следва от (6). По същия начин от (7) получаваме, че $\varphi(ab)=\varphi(a)\odot\varphi(b)$. Следователно изображението φ е съгласувано с операциите в **N** и $\bar{\mathbf{N}}$. С това е установено, че **Z** притежава свойството А). За да покажем, че **Z** притежава и свойството В), достатъчно е да се отбележи, че съгласно (5) произволен елемент $[a,\ b]\in\mathbf{Z}$ може да се запише във вида

8) $$[a,\ b]=[a+1,1]\ominus[b+1,1]=\varphi(a)\ominus\varphi(b).$$

Теоремата е доказана.

С някои допълнителни разсъждения може да се докаже, че пръстенът на целите числа в известен смисъл е единствен.

Задача. а) Докажете, че за всяко $[a,\ b]\in\mathbf{Z}$ елементът $[1,\ 1]$ е единственото решение на уравнението $[a,\ b]\oplus x=[a,\ b]$, т. е. $[1,\ 1]$ е неутрален относно събирането и се нарича нулев елемент на **Z**. Докажете, че $[1,\ 1]$ е единствен нулев елемент в **Z**.

б) Докажете, че за всяко $[a,\ b]\in\mathbf{Z}$ елементът $[b,\ a]$ е единственото решение на уравнението $[a,\ b]\oplus x=[1,\ 1]$. Това решение се нарича противоположен елемент на елемента $[a,\ b]$ и се означава с $x=\ominus[a,\ b]$, т. е. $\ominus[a,\ b]=[b,\ a]$.

в) Докажете, че $\ominus(\ominus[a,\ b])=[a,\ b]$.

г) Докажете, че елементът $e=[a+1,\ a]$ е единственият неутрален елемент относно умножението.

Обстоятелството, че съществува взаимно еднозначно съответствие между елементите на $\bar{\mathbf{N}}$ и **N**, зададено с равенството $\varphi(a)=[a+1,\ 1]$ за всяко $a\in\mathbf{N}$, ни позволява да отъждествяваме съответните елементи на **N** и $\bar{\mathbf{N}}$, т. е. $[a+1,\ 1]=a\ (a\in\mathbf{N})$. При това можем да заменим и знаците за съответните операции. Тогава равенството (8) придобива вида $[a,\ b]=a-b$.

Следствие 1. *За всяко цяло число $z\in\mathbf{Z}$ е изпълнено точно едно от следните три условия:* $z\in\mathbf{N}$, $z=0$, $-z\in\mathbf{N}$.

Действително ако $z=a-b\ (a,\ b\in\mathbf{N})$, то съгласно закона за трихотомията в **N** (свойство 10) и определението на релацията $<$

за естествените числа a и b възможен точно един от следните три случая: 1) $a=b+c$ ($c\in\mathbf{N}$, 2) $a=b$ и 3) $b=a+d$ ($d\in\mathbf{N}$), което е еквивалентно съответно на условията: 1) $z=a-b=c\in\mathbf{N}$; 2) $z=a-b=0$ и 3) $-z=b-a=\in\mathbf{N}$.

Доказаното следствие позвва, че пръстенът на целите числа може да се представи като обединение $\mathbf{Z}=\mathbf{N}\cup\{0\}\cup(-\mathbf{N})$, т. е. $\mathbf{Z}=\{0, \pm1, \pm2, \ldots\}$.

С $\mathbf{N}_0$ ще означаваме обединението $\mathbf{N}\cup\{0\}$.

Задача. Докажете, че ако $a\neq0$ и $ab=ac$, то $b=c$ ($a, b, c\in\mathbf{Z}$)

§ 6. Делимост на цел числа. НОД и НОК

Нека a и b са цели числа, т. е. $a, b\in\mathbf{Z}$. Ще казваме, че b *дели* a, ако $a=bq$ за някое $q\in\mathbf{Z}$. В такъв случай ще казваме още, че *a се дели на b* или *a е кратно на b*, и ще записваме $b|a$. В противен случай се казва че *b не дели a*, *a не се дели на b* или *a не е кратно на b*, се записва $b\nmid a$. От определението за делимост лесно се получават следните свойства на целите числа:

1) $a|a$ *за всяко* $a\in\mathbf{Z}$;
2) $a|0$ ($a\in\mathbf{Z}$);
3) *ако* $0|a$, *то* $a=0$;
4) *ако* $a|b$ и $b|c$, *то* $a|c$;
5) *ако* $b|a$, *то* $b|ac$ *за всяко* $c\in\mathbf{Z}$;
6) *ако* $b|a$, *то* $bc|ac$ *за всяко* $c\in\mathbf{Z}$;
7) *ако* $c|a$ *и* $c|b$, *то* $c|(a\pm b)$;
8) *ако* $bc|ac$ *и* $c\neq0$, *то* $b|a$;
9) *ако* $a|(b+c)$ *и* $a|b$, *то* $a|c$;
10) *ако* $a|b$ и $c|d$, то $ac|bd$.

Следващите свойства на делимостта се получават от някои специфични особености на естествените числа.

11) *Ако a и b са естествени числа и $ab=1$, то $a=b=1$.*

Доказателство. Ако едно от двете числа a и b е равно на 1, то и другото число е равно на 1. Да допуснем, че $a>1$ и $b>1$. Съгласно определението на релацията $>$ съществуват естествени числа k, $l\in\mathbf{N}$, за които $a=k+1$ и $b=l+1$. Тогава $ab=kl+k+l+1=1$ и $kl+k+l=0$. Но тъй като $\mathbf{N}(+,.)$ е полупръстен, то от последното равенство следва, че $0\in\mathbf{N}$, което не е вярно.

12) *Ако цялото число a дели 1 то $a=\pm1$.*

Доказателство. От $a|1$, следва, че $1=aq$ ($q\in\mathbf{Z}$). Тогава $a^2q^2=1$, където a^2 и q^2 са естествени числа. Съгласно 11) оттук се получава, че $a^2=1$. Следователно изпълнени са равенствата $a.a=1$ и $(-a)(-a)=1$. Понеже едно от двете числа a и $-a$ е естествено, то пак от 11) следва, че a или $-a$ е равно на 1.

13) *Ако $a|b$ и $b|a$, то $a=\pm b$.*

Доказателство. От условието следва, че $a=bq$, $b=aq_1$ ($q, q_1\in\mathbf{Z}$) и $a=aqq_1$. Ако $a=0$, то от $0|b$ получаваме $b=0$ и твър-

дението е вярно. Ако $a \neq 0$, то $q_1 = 1$ и $q = \pm 1$, поради което $a = \pm b$.

С $|a|$ ще бележим абсолютната стойност на числото a, т. е. $|a| = a$ при $a \geqq 0$ и $|a| = -a$ при $a < 0$.

14) *Ако* $b|a$ *и* $a \neq 0$, *то* $|b| \leqq |a|$.

Доказателство. Нека $a = bq$ $(q \in Z)$. Тогава $|a| = |b| \cdot |q|$, където $|a|$, $|b|$ и $|q|$ са естествени числа. Тъй като $|q| = 1 + k$ $(k \geqq 0)$, то $|a| = |b| + |b|k$ и $|b|k \geqq 0$. Сега твърдението следва от определението на релацията $>$.

Нека $a, b \in Z$ $b \neq 0$. Да разделим числото a на числото b с остатък означава да представим a във вида $a = bq + r$, където q, $r \in Z$ и $0 \leqq r < |b|$. При това q се нарича непълно частно, а r—остатък от делението на a с b. Както показва следващата теорема, делението с остатък е винаги възможно, а непълното частно q и остатък r са еднозначно определени от делимото a и делителя b.

Теорема 4. *За всеки две цели числа* a *и* b *при* $b \neq 0$ *съществува единствена двойка цели числа* q *и* r, *за които*

$$a = bq + r, \quad 0 \leqq r < |b|.$$

Доказателство. Да разгледаме най-напред случая, когато $b = |b|$. Подмножеството $S = \{a - bs \mid s \in Z, a - bs \geqq 0\}$ на множеството $N_0 = N \cup \{0\}$ не е празно. Действително ако $a = s = 0$, то $0 = a - bs \in S$. Ако $a \neq 0$ и $s = -a^2$, то $a - bs = a + ba^2 \in S$, защото $a|ba^2$, $ba^2 \in N$, $|a| \leqq ba^2$ съгласно 14) и затова $a + ba^2 \geqq 0$. Следователно подмножеството S съдържа най-малък елемент и нека той е $r = a - bq$ $(q \in Z)$. По условие $r \geqq 0$. Ако предположим, че $r \geqq b$, то елементът $r - b = a - b(q + 1)$ е също от S и ще бъде по-малък от r, а това противоречи на избора на r. Полученото противоречие показва, че $0 \leqq r < b$, при което $a = bq + r$.

Ако $b < 0$, то $|b| > 0$ и, както вече доказахме, съществуват такива q_1, $r_1 \in Z$, че $a = |b|q_1 + r_1$ и $0 \leqq r_1 < |b|$. Но $|b| = -b$ и следователно $a = b(-q_1) + r_1$.

Нека q', r' е друга двойка от цели числа, за които $a = bq' + r'$ и $0 \leqq r' < |b|$. Тогава $bq + r = bq' + r'$ и $b(q - q') = r' - r$. Тъй като $|r' - r| < |b|$ и $|b| / |r' - r|$, то последното равенство е възможно само тогава, когато $q = q' = 0$ (вж. свойство 14)). Следователно $q = q'$ и $r = r'$. Теоремата е доказана.

Изложеното просто доказателство на теоремата дава същевременно удобен алгоритъм за намиране на непълното частно q и остатъка r при делението на a с b. Действително, понеже $\varphi(s) = a - bs$ при $b > 0$ е намаляваща линейна функция относно s, то q е най-голямото цяло число, за което $r = \varphi(q) \geqq 0$. Във важността на тази теорема ще имаме възможност да се убеждаваме при многобройните нейни приложения.

Цялото число d се нарича *общ делител* на целите числа a и b, ако $d|a$ и $d|b$. *Най-голям общ делител* (НОД) на a и b се нарича такъв техен общ делител, който се дели на всеки друг

общ делител на a и b. С НОД(a, b) ще означаваме множеството на най-големите общи делители на a и b. Следователно $d \in$ НОД(a, b) точно тогава, когато са изпълнени условията:

1) d/a и d/b;

2) ако d_1/a и d_1/b, то d_1/d.

Забележка: Често понятието НОД(a, b) се въвежда като най-голямото от целите числа d със свойството d/a и d/b. Това определение е неприложимо за числата $a=0$ и $b=0$. Освен това *то не може да бъде пренесено за алгебрични обекти, в които няма релация наредба.*

Ще отбележим някои основни свойства на НОД.

1). НОД$(0, 0)=\{0\}$.

Действително всяко цяло число е общ делител на числата $a=0$ и $b=0$. Но единственото число d, което се дели на всяко цяло число, е $d=0$.

2). Ако a/b, то $a \in$ НОД(a, b)

3). Ако $d, d_1 \in$ НОД(a, b), то $d=\pm d_1$.

Наистина d/d_1, защото d е общ делител на a и b, а d_1 е техен НОД. По същия начин получаваме, че d_1/d. От 13) следва, че $d=\pm d_1$.

4). НОД$(a, b)=$НОД$(|a|, |b|)$.

Теорема 5. *Всеки две цели числа притежават поне един* НОД.

Доказателство. Поради посочените вече свойства 1), 2) и 4) достатъчно е да разгледаме случая, когато $a>0$ и $b>0$. Доказателството на теоремата представлява определен начин за намирането на НОД на две числа, известен като алгоритъм на Евклид (III в. пр. н. е.). Алгоритъмът се състои в последователното прилагане на теорема 3 за намиране на равенствата

$$
\begin{aligned}
a &= bq_1 + r_1, \quad 0 \leqq r_1 < b, \\
b &= r_1 q_2 + r_2, \quad 0 \leqq r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 \leqq r_3 < r_2, \\
&\cdots\cdots\cdots\cdots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, \quad 0 \leqq r_k < r_{k-1}, \\
r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 \leqq r_k < r_{k-1}, \\
r_{k-1} &= r_k q_{k+1} + r_{k+1}, \quad 0 \leqq r_{k+1} < r_k,
\end{aligned} \tag{1}
$$

където $q_1, q_2, \ldots, q_{k+1}$ са непълни частни, а $r_1, r_2, \ldots, r_{k+1}$ са съответните остатъци. Тъй като $b > r_1 > r_2 > \ldots > r_{k+1} \geqq 0$, то след краен брой стъпки ще стигнем до първия остатък $r_{k+1}=0$. Тогава r_k е НОД на a и b. Действително, разглеждайки посочените равенства от последното към първото, ние последователно намираме, че r_k дели $r_{k-1}, r_{k-2}, \ldots, b, a$, т. е. r_k е общ делител на a и b. Ако d_1 е произволен общ делител на a и b, то като разглеждаме същите равенства от първото до последното, стигаме до извода, че d_1 дели $r_1, r_2, \ldots, r_k$. Следователно $r_k \in$ НОД(a, b). Теоремата е доказана.

От доказаната теорема и свойство 3) следва, че всеки две

цели числа a и b притежават един единствен неотрицателен НОД, който ще означаваме с (a, b). Очевидно е, че $(a, b) = r_k$, където r_k е последният ненулев остатък в равенствата (1).

Теорема 6. *Ако a и, b са произволни цели числа; то съществуват такива цели числа u и $v \in \mathbf{Z}$, че $(a, b) = ua + vb$.*

Доказателство. Достатъчно е да разгледаме случая, когато $a > 0$, $b > 0$, и да докажем, че последният ненулев остатък в равенствата (1) е линейна комбинация на a и b, с цели коефициенти.

От (1) следва, че

$$r_i = r_{i-2} - r_{i-1} q_i \quad (i = 1, 2, \ldots, k), \tag{2}$$

където $r_0 = b$ и $r_{-1} = a$. Тогава в израза за r_k от (2) заместваме r_{k-1} (също определено от (2)) и получаваме, че r_k се изразява линейно чрез r_{k-2} и r_{k-3} с цели коефициенти. След това по същия начин изключваме r_{k-2} и т. н. Така ще получим, че r_k се изразява линейно чрез a и b.

Две цели числа a и b се наричат *взаимно прости*, ако $(a, b) = 1$.

Следствие 2. *Числата a и b са взаимно прости тогава и само тогава, когато съществуват такива цели числа u и v, че $ua + vb = 1$.*

Сега вече можем да докажем някои по-съществени твърдения за делимост на цели числа.

Твърдение 2. *Ако a/bc и $(a, b) = 1$, то a/c.*

Доказателство. Тъй като $(a, b) = 1$, то съществуват такива цели числа u и v, за които $ua + vb = 1$. Умножаваме това равенство с c и получаваме $c = (uc)a + v(bc)$. Понеже a дели двете събираеми $(uc)a$ и $v(bc)$, то a/c.

Твърдение 3. *Ако a/c, b/c и $(a, b) = 1$, то ab/c.*

Доказателство. Тъй като a/c, то $c = aq$ $(q \in \mathbf{Z})$. Тогава b/aq, $(b, a) = 1$ и от твърдение 2 се получава, че $q = bq_1$ $(q_1 \in \mathbf{Z})$. Следователно $c = aq = abq_1$ и ab/c.

Твърдение 4. *Ако $(a, c) = 1$ и $(b, c) = 1$, то $(ab, c) = 1$.*

Доказателство. От условието следва, че за някои цели числа u, v, u_1, v_1 са изпълнени равенствата $ua + vb = 1$ и $u_1 b + v_1 c = 1$. Като умножим почленно тези равенства, ще получим, че $1 = wab + zc$, където $w = uu_1$ и $z = vu_1 b + vv_1 c + uv_1 a$. Следователно числата ab и c са взаимно прости.

От това твърдение и следствие 2 се получава.

Следствие 3. *Произведенията $a_1 a_2 \ldots a_k$ и $b_1, b_2 \ldots b_r$ са взаимно прости тогава и само тогава, когато $(a_i, b_j) = 1$ за всяко $i = 1, 2, \ldots, k$ и $j = 1, 2, \ldots, r$. В частност $(a^k, b^r) = 1$ тогава и само тогава, когато $(a, b) = 1$.*

Твърдение 5. *Ако a и b са цели числа и $d \in \mathbf{N}_0$, то $d = (a, b)$* тогава и само тогава, когато

$$a = da_1, \; b = db_1, \quad (a_1, b_1) = 1, \; a_1, b_1 \in \mathbf{Z}. \tag{3}$$

Доказателство. Нека са изпълнени равенствата (3). От тях се вижда, че d е общ делител на a и b. За да докажем, че $d=(a, b)$, остава да се покаже, че d се дели на всеки друг общ делител на a и b. За тази цел използуваме равенството $(a_1, b_1)=1$. От него следва, че $1=ua_1+vb_1$ за някои цели числа u и v. Като умножим равенството с d, ще получим, че $d=ua+vb$, а оттук веднага се вижда, че общите делители на a и b делят d.

Обратно, да допуснем, че $d=(a, b)$. Трябва да докажем, че са изпълнени условията (3).

Ако $d=0$, то $0/a$, b и затова $a=b=0$. Тогава можем да положим $a_1=b_1=1$. Ако $d>0$, то от условието d/a, b следва, че за някои a_1, $b_1\in Z$ са изпълнени равенствата $a=da_1$, $b=db_1$. Но от теорема 5 следва, че $d=ua+vb$ $(u, v\in Z)$. Като заместим в това равенство a и b с техните равни и съкратим на d, ще получим равенството $1=ua_1+vb_1$, което показва, че $(a_1, b_1)=1$. Предложението е доказано.

Понятието НОД на две цели числа по същия начин *се пренася и за повече от две цели числа* $a_1, a_2, \ldots, a_n$. При това теорема 5 остава вярна за неотрицателния най-голям общ делител $(a_1, a_2, \ldots, a_n)$. Не е трудно да се покаже, че *ако* $(a_1, a_2)=d_1$, $(d_1, a_3)=d_2, \ldots, (d_{n-2}, a_n)=d_{n-1}$, *то* $(a_1, a_2, \ldots, a_n)=d_{n-1}$.

Наистина общите делители на числата a_1 и a_2 са делителите на техния най-голям общ делител $d_1=(a_1, a_2)$ и само те. Следователно общите делители на числата a_1, a_2 и a_3 са общи делители на d_1 и a_3. В частност $(a_1, a_2, a_3)=(d_1, a_3)$. По същия начин общите делители на a_1, a_2, a_3 и a_4 са общи делители на $d_2=(d_1, a_3)$ и a_4, поради което $(a_1, a_2, a_3, a_4)=(d_2, a_4)$. По-нататък разсъжденията следват с индукция.

Числото m се нарича *общо кратно* на числата $a_1, a_2, \ldots, a_n$, ако m се дели на всяко едно от тях. *Най-малко общо кратно* $[a_1, a_2, \ldots, a_n]$ на ненулевите цели числа $a_1, a_2, \ldots, a_n$ наричаме най-малкото естествено число, което едновременно се дели на $a_1, a_2, \ldots, a_n$. Ако поне едно от тези числа е равно на нула, тогава полагаме $[a_1, a_2, \ldots, a_n]=0$.

Твърдение 6. *Ако* $a, b\in Z$, *то* $(a, b)\,[ab]=|ab|$ *и общите кратни на числата* a *и* b *съвпадат с кратните на* $[a, b]$.

Доказателство. Ако поне едно от числата a и b е равно на нула, то $[a, b]=|a\,b|=0$ и равенството, което трябва да докажем, в този случай е изпълнено. Освен това в този случай единственото общо кратно на a и b е само числото 0.

Нека a и b са ненулеви цели числа и m е произволно тяхно общо кратно. От a/m следва, че $m=aq$ $(q\in Z)$. Но m е кратно и на b, поради което $\frac{aq}{b}\in Z$. Нека $d=(a, b)$ и $a=da_1$, $b=db_1$, където $(a_1, b_1)=1$. Тогава $\frac{aq}{b}=\frac{da_1q}{db_1}=\frac{a_1}{b_1}q\in Z$ и затова b_1/q, т. е. $q=b_1t=\frac{b}{d}t$ $(t\in Z)$. Следователно $m=aq=\frac{ab}{d}t=\frac{|ab|}{(a, b)}\varepsilon t$, където $\varepsilon=1$

при $ab>0$ и $\varepsilon=-1$ при $ab<0$. Оттук следва, че общите кратни на a и b съвпадат с кратните на числото $\frac{|ab|}{(a, b)}$, а то от своя страна е тяхното най-малко общо кратно. Твърдението е доказано.

Следствие 4. *Ако a/c и b/c, то $[a, b]/c$.*

Втората част на твърдение 6 ни дава възможност да намираме най-малкото общо кратно на няколко числа. Действително общите кратни на числата a_1 и a_2 са кратни на числото $[a_1, a_2]$. Тогава общите кратни на a_1, a_2 и a_3 съвпадат с кратните на $[a_1, a_2]$ и a_3. В частност $[a_1, a_2, a_3]=[[a_1, a_2], a_3]$. Така по индукция може да се докаже, че

$$[a_1, a_2, \ldots, a_{n-1}, a_n]=[[a_1, a_2, \ldots, a_{n-1}], a_n] \tag{4}$$

и общите кратни на числата $a_1, a_2, \ldots, a_n$ съвпадат с кратните на тяхното най-малко общо кратно $[a_1, a_2, \ldots, a_n]$. Следователно ако числата $a_1, a_2, \ldots, a_n$ делят числото c, то и $[a_1, a_2, \ldots, a_n]/c$.

Твърдение 7. *Ако $a_1, a_2, \ldots, a_n$ са произволни цели числа, то равенството*

$$[a_1, a_2, \ldots, a_n]=|a_1\ a_2 \ldots a_n| \tag{5}$$

е изпълнено тогава и само тогава, когато числата $a_1, a_2, \ldots, a_n$ са две по две взаимно прости или някое от тях е равно на нула.

Доказателство. Ако някое a_i $(1\leqq i\leqq n)$ е равно на нула то равенството (5) е изпълнено, понеже и двете му части са равни на нула. Нека $a_1, a_2, \ldots, a_n$ са ненулеви две по две взаимно прости цели числа. С индукция ще докажем, че за тях е изпълнено равенството (5). При $n=2$ твърдението следва от твърдение 6. Да допуснем, че равенството (5) е вярно при $n=k$. Тогава, като приложим последователно равенството (4), индукционното предположение и следствие 3, ще получим

$$[a_1, a_2, \ldots, a_k, a_{k+1}]=[[a_1, a_2, \ldots, a_k], a_{k+1}]$$
$$=[|a_1\ a_2 \ldots a_k|, a_{k+1}]=|a_1 a_2 \ldots a_k\ a_{k+1}|,$$

т.е. равенството (5) е вярно и при $n=k+1$. Следователно равенството (5) е вярно за всяко n.

Обратно, нека за числата $a_1, a_2, \ldots, a_n$ е изпълнено равенството (5). Трябва да докажем, че те са две по две взаимно прости някое от тях е равно на нула. Ако $[a_1, a_2, \ldots, a_n]=|a_1, a_2, \ldots, a_n|=0$, то поне едно от числата $a_1, a_2, \ldots, a_n$ е равно на нула твърдението е доказано.

Да разгледаме случая, когато всяко от числата $a_1, a_2, \ldots, a_n$ е различно от нула. Да допуснем, че някои две от тях не са взаимно прости, и нека например $(a_1, a_2)=d>1$, където $a_1=da_1'$, $a_2=da_2'$. Тогава числото $|a_1' a_2' d a_3 \ldots a_n|$ също е общо кратно на числата $a_1, a_2, \ldots, a_n$ и е по-малко от $|a_1 a_2 \ldots a_n|$. С полученото противоречие доказателството е завършено.

§ 7. Прости числа

Естественото число $p>1$ се нарича *просто*, ако неговите единствени положителни делители са числата 1 и p. Единствените числа, които имат повече от два положителни делителя, се наричат **съставни. Числото 1 не е нито просто, нито съставно.**

Тези определения са свързани с традицията да се разглежда обикновено делимостта само на естествените числа. По-нататък, когато разглеждаме теорията на делимостта и за други обекти, понятието **просто число** се обобщава с понятието *прост елемент.* Така например числото -5 не е просто число, но то е в известен смисъл прост елемент в пръстена на целите числа. Прости числа са 2, 3, 5, 7 и т. н. Числата 4, 6, 8, 9 и т. н. са съставни. За отрицателните числа -4, -6, -8, -9 и т. н. също ще казваме, че са съставни, а числата -2; -3, -5, -7 и т. н. ще наричаме прости елементи на пръстена Z. Числата -1, 0 и 1 не са нито прости, нито съставни.

Твърдение 8. *Ако p е просто число и $p\nmid a$, то $(a, p)=1$.*

Доказателство. Общите положителни делители на a и p са сред числата 1 и p. Тъй като $p\nmid a$, то 1 е единственият техен общ положителен делител и затова $(a, p)=1$.

Твърдение 9. *Всяко цяло число $a\neq\pm1$ се дели поне на едно просто число.*

Доказателство. Ако $a=0$, то a се дели на всяко просто число. Ако $a\neq0$, то $|a|>1$ и $|a|\mid a$. Следователно числото a се дели поне на едно естествено число, по-голямо от 1. Нека p е най-малкият от положителните делители на a, които са по-големи от 1. Тогава p е просто число, защото противното допускане, че $p=p_1p_2$, води до противоречието, че a има делители $p_1>1$ и $p_2>1$ които са по-малки от p. Твърдението е доказано.

Следната интересна теорема е била доказана от Евклид около три века преди новата ера.

Теорема 7. *Множеството на простите числа е безкрайно*

Доказателство. Да допуснем, че съществуват само краен брой прости числа $p_1, p_2, \ldots, p_k$. Тогава числото $a=p_1p_2\ldots p_k+1$ съгласно предното твърдение притежава поне един прост делител p. Тъй като $p_1, p_2, \ldots, p_k$ са единствените прости числа, то $p=p_i$ за някое $i\ (1\leqq i\leqq k)$. Но от $p\mid a$ и $p\mid p_1p_2\ldots p_k$ следва, че $p\mid1$, което е невъзможно. Теоремата е доказана.

Съществуват и много други интересни доказателства на теорема 7. Например Ойлер е дал едно такова доказателство, като е доказал, че сумата от реципрочните стойности на всички прости числа е безкрайна. Най-интересното е обаче, че сумата от реципрочните стойности на известните досега на науката прости числа не надминава $\frac{1}{4}$. По времето на Ойлер през XVIII век най-голямото известно просто число е било числото $2^{31}-1=2\,147\,483\,647$. В 1883 г. руският самоук математик И. М. Первушин

е доказал, че числото $2^{61}-1$ е също просто. Днес благодарение на съвременните електронни сметачни машини са известни всички прости числа, по-малки от 10^7. В същото време са открити и много големи прости числа от специален вид. Едно такова число е например числото $2^{11213}-1$, което се записва с 3376 цифри.

Задача. Докажете, че всеки две различни числа от редицата с общ член $a_n=2^{2^n}+1$ са взаимно прости. Като следствие оттук изведете друго доказателство на теорема 7.

Решение. Числото $(2^{2^k}+1)-2$ се дели на числото $2^{2^s}+1$ за всяко $s<k$, защото

$$(2^{2^k}+1)-2=2^{2^k}-1=(2^{2^s})^{2^{k-s}}-1=(2^{2^s}+1)q,\ q\in Z.$$

Следователно остатъкът от делението на $2^{2^k}+1$ с $2^{2^s}+1$ е равен на 2. Тъй като $2^{2^s}+1$ е нечетно число, то неговият остатък при делението на 2 е равен на 1. Оттук следва, че $(2^{2^k}+1, 2^{2^s}+1)=1$ за всяко $k\neq s$. Ако допуснем, че простите числа са краен брой, например равен на n, то не биха съществували повече от $n+1$ на брой две по две взаимно прости числа.

Твърдение 10. *Ако простото число p дели произведението $a_1a_2\ldots a_n$ на целите числа $a_1, a_2, \ldots, a_n$, то p дели поне едно от тях.*

Доказателство. Твърдението ще докажем с индукция спрямо n. Ако $n=2$ и $p\nmid a_1$, то $(p, a_1)=1$ и от твърдение 2 следва, че p/a_2. Да допуснем, че предложението е доказано за всяко $n\leq k$. Тогава от $p/a_1a_2\ldots a_ka_{k+1}$ следва, че $p/a_1a_2\ldots a_k$ или p/a_{k+1}. При положение че $p/a_1a_2\ldots a_k$, от индукционното предположение следва, че p дели някое от числата $a_1, a_2, \ldots a_k$.

Следващата теорема е основна теорема в аритметиката на целите числа.

Теорема 8. *Всяко естествено число $a>1$ се разлага като произведение на прости числа, което е единствено с точност до наредбата на простите множители.*

Доказателство. Ако $a=2$, то теоремата е вярна, защото 2 е просто число. Да допуснем, че теоремата е доказана за всяко естествено число $a\leq k$, и нека $a=k+1$. Съгласно твърдение 9 числото $k+1$ има поне един прост делител p_1. Ако $k+1=p_1q$ $(q\in N)$, то $q\leq k$ и затова q се разлага като произведение $q=p_2p_3\ldots p_n$ на простите числа $p_2, p_3, \ldots, p_n$, което е единствено с точност до наредбата на множителите. Следователно $k+1=p_1p_2\ldots p_n$, т. е. $k+1$ е също произведение на прости множители. Да допуснем, че съществува и второ такова разлагане $k+1=q_1q_2\ldots q_m$, където $q_1, q_2, \ldots, q_m$ са прости числа. Тъй като $p_1/(k+1)$, то съгласно предложение 17 p_1/q_i за някое i $(1\leq i\leq m)$. След евентуална преномерация на числата $q_1, q_2, \ldots, q_m$ можем да считаме, че p_1/q_1, т. е. $i=1$. Тъй като p_1 и q_1 са прости числа, то $p_1=q_1$. Оттук следва, че $q=p_2p_3\ldots p_n=q_2q_3\ldots q_m$. Понеже разлагането на q е единствено, то $n=m$ и след евентуална преномерация на числата $q_2, q_3, \ldots q_m$

ще имаме $p_2=q_2$, $p_3=q_3, \ldots, p_n=q_n$. С това теоремата е доказана и за числото $k+1$.

Ясно е, че в разлагането на едно естествено число като произведение на прости множители някои от тези множители могат да се повторят. Ако $p_1, p_2, \ldots, p_k$ са всичките различни прости делители на дадено естествено число a, то a има представянето $a=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, където $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbf{N}$ (т. е. множителят p_i в разлагането на a се повтаря α_i пъти). Това представяне е единствено с точност до номерацията на числата $p_1, p_2, \ldots, p_k$ и се нарича *каноничен вид* (или *каноничко представяне*) на числото a.

Задача. Намерете (a, b) и $[a, b]$, ако са известни каноничните представяния на числата a и b.

ЛИТЕРАТУРА

1. Артин, Е. Теория на Галоа. Наука и изкуство, София, 1972.
2. Артин, Э. Геометрическая алгебра. Наука. Москва, 1969.
3. Бухштаб, А. А. Теория чисел. Учпедгиз. Москва, 1960.
4. Ван дер Варден, Б. Л. Алгебра. Наука. Москва, 1976.
5. Виноградов, И. М. Основы теории чисел. Гостехиздат. Москва, 1949.
6. Гаврилов, М., Д. Димитров, Ив. Димовски. Съвременна аритметика. Народна просвета. София, 1975.
7. Гельфанд, И. М. Лекции по линейной алгебре. Наука. Москва, 1966.
8. Калужнин, Л. А. Введение в общую алгебру. Наука. Москва, 1973.
9. Каргаполов, М. И., Ю. И. Мерзляков. Основы теории групп. Наука. Москва, 1972.
10. Кострикин, А. И. Введение в алгебру. Наука. Москва, 1973.
11. Куликов, Л. Я. Алгебра и теория чисел. Высшая школа. Москва, 1979
12. Курош, А. Г. Лекции по общей алгебре. Наука. Москва, 1973.
13. Курош, А. Г. Теория групп. Наука. Москва, 1967.
14. Курош, А. Г. Курс по висша алгебра. Наука и изкуство. София, 1968.
15. Кэртис, Ч., И. Райнер. Теория представлений конечных групп и ассоциативных алгебр. Наука. Москва, 1969.
16. Ленг, С. Алгебра. Мир. Москва, 1968.
17. Мальцев, А. И. Алгебрические системы. Наука. Москва, 1970.
18. Манин, Ю. А. О разрешимости задач на построение с помощью циркуля и линейки. Энциклопедия элементарной математики, Т. IV. Гос. изд. физ-мат. литературы. Москва, 1963.
19. Обрешков, Н. Теория на числата. Наука и изкуство. София, 1965.
20. Обрешков, Н. Висша алгебра. Наука и изкуство. София, 1962.
21. Постников, М. М. Теория Галуа. Гос. изд. физ-мат. литературы. Москва, 1963.
22. Проскуряков, И. В. Сборник задач по линейной алгебре. Наука. Москва, 1967.
23. Рашова, Х. Елементи на теорията на множествата. Наука и изкуство, София, 1972.
24. Скорняков, Л. А. Лекции по алгебре. МГУ. Москва, 1963.

Георги Генов
Стоил Миховски
Тодор Моллов

АЛГЕБРА С ТЕОРИЯ НА ЧИСЛАТА

Второ допълнено издание
Рецензенти
Стефан Додунеков, Керопе Чакърян
Редактор
Николай Божинов
Художник
Таня Николова
Художествен редактор
Кремена Филчева
Технически редактор
Богомил Биджев
Коректор
Теменужка Балабанова

Дадена за набор на 17. VII. 1990 г. Подписана за печат на 28. XI. 1990 г. Излязла от печат през декември 1990 г. Печатни коли 24,25. Издателски коли 24,25. Условно издателски коли 27,12. Формат 16/60/90. Тираж 2070. Цена 1,54. Издателски № 30627. КОД 02953462151 1/4805—424—91

Издателство „Наука и изкуство“ — София
Печатница „Георги Димитров“ — Ямбол