Ръководство за упражнения по висша алгебра

пръстени и полета
полиноми
групи

НАУКА И ИЗКУСТВО

РЪКОВОДСТВО
ЗА УПРАЖНЕНИЯ
ПО ВИСША
АЛГЕБРА

Доц. КИРИЛ ДОЧЕВ
Доц. ДИМИТЪР ДИМИТРОВ
ВЛАДИМИР ЧУКАНОВ

Ръководство за упражнения по висша алгебра

пръстени и полета полиноми групи

ВТОРО ИЗДАНИЕ

ИЗДАТЕЛСТВО „НАУКА И ИЗКУСТВО" СОФИЯ 1976

Тази част от Ръководството за упражнения по висша алгебра съдържа теореми и задачи от следните раздели: теория на числата, пръстени и полета, полиноми на една и повече променливи, групи. Отделните параграфи са предшествувани от кратки обяснителни бележки, имащи справочен характер. Ръководството е предназначено главно за студенти по математика, като е съобразено с лекциите и упражненията по алгебра във Факултета по математика и механика на Софийския университет. То може да се използува като учебно пособие от всички, които желаят да се запознаят по-отблизо с методите на алгебрата. Поради засилващата се в последно време тенденция за проникване на алгебрични методи в най-различни математически и приложни направления в науката, Ръководството може да бъде препоръчано за изучаващите Висша математика физици, инженери химици, икономисти и др.

СЪДЪРЖАНИЕ

ПРЕДГОВОР

Втората част от Ръководството за упражнения по висша алгебра има същата структура, както първата част. И тук задачите и теоремите към отделните параграфи са предшествувани от обяснителни бележки върху използувания теоретичен материал. Подобна структура дава възможност да се правят справки върху разглежданите алгебрични раздели и от онези читатели, които не си поставят за цел да изучават във всички детайли съдържащите се теореми и задачи. Застъпените в Ръководството области от алгебрата: пръстени и полета, полиноми, групи, се предхождат от встъпителна глава, която съдържа необходими за по-нататъшното изложение, а представляващи и самостоятелен интерес сведения от теория на числата. Това е направено с цел при работа с Ръководството читателят да разполага с илюстриращи примери към някои от разглежданите алгебрични теореми и задачи, да бъде изтъкната аналогията между пръстена на целите числа и пръстена на полиномите на една променлива и изобщо за осъществяване на по-тясна връзка между индуктивния и дедуктивния подход към изучаваните въпроси.

При работата си върху Ръководството авторите са се основавали на своя опит като преподаватели по алгебра в Математическия факултет и на новите учебни програми. Разбира се, освен основния учебен материал е застъпен и допълнителен, който е предназначен за студенти с повишен интерес към изучаване на алгебрата. По правило задачите и теоремите с основно значение, а така също и тези с повишена трудност са придружени с решения или упътвания. За контрол на самостоятелната работа на читателя са дадени отговори на почти всички задачи.

По-голямата част от задачите и теоремите са традиционни, като са подредени съобразно структурата на Ръководството и методическите предпочитания на авторите. Известна част от поместените в Ръководството задачи са възникнали в резултат от преподавателската и научна практика на авторите, но това не е изрично посочено на съответно място, за да не се получава излишна за читателя претрупаност с литературни справки. Накрая е дадена литература, която е свързана с разглежданите въпроси. Част от тази литература е използувана от авторите за съставянето на настоящото ръководство.

Изказваме нашата сърдечна благодарност на сътрудниците към сектора по алгебра на ЕЦНПКММ другарите М. Гаврилов, Л. Давидов, Ив. Тонов, Н. Ненов, К. Чакърян за оказаното съдействие при съставянето и обсъждането на тази книга. Особено ценна помощ ни оказа ст. н. с. М. Гаврилов, който положи големи грижи и за редактирането на Ръководството и по същество може да се счита за наш съавтор.

ГЛАВА VI

ЕЛЕМЕНТИ ОТ ТЕОРИЯТА НА ЧИСЛАТА

§ 1. ДЕЛИМОСТ

Нека Z да означава множеството от целите числа, а Z^+ — множеството от естествените числа. Ако $a \in Z$ и $b \in Z$, $b \neq 0$, ще казваме, че b дели a и ще пишем b/a, когато съществува $c \in Z$, такова, че

$$a = bc.$$

Казваме още, че числото a е кратно на b или че b е делител на a. Понеже b/a е равносилно с $|b|/|a|$, достатъчно е да разглеждаме свойствата на релацията делимост в множеството Z^+ на целите положителни числа. В сила са свойствата:

1. От a/b и b/c следва a/c;
2. a/a;
3. От a/b й b/a следва $a=b$;
4. От a/b и a/c следва $a/ub+vc$ при произволни u, $v \in Z$.

(Тук a, b, c означават произволни елементи от Z^+.)

Теорема. За всеки две цели числа a и b, $b>0$ съществуват еднозначно определени числа q и r, такива, че

$$a = bq + r$$

и

$$0 \leq r < b.$$

Числата q и r се наричат съответно *частно и остатък* при делението на a с b. Остатъкът r, получен при делението на a с b, е равен на нула само когато положителното число b дели числото a.

Определение. Под *най-голям общ делител* на целите числа a и b разбираме такова цяло число d, което притежава свойствата:

1. d/a и d/b.
2. От d_1/a и d_1/b следва d_1/d.

Може да се докаже, че най-голям общ делител винаги съществува и е еднозначно определен с точност до знак.

Най-големият общ делител на числата a и b ще означаваме с $d=(a, b)$, при което ще считаме, че $d>0$.

За намиране на най-големия общ делител си служим с т. нар. алгоритъм на Евклид. Той се основава на следното очевидно свойство: ако r е остатъкът от делението на a с b, то всеки общ делител на a и b е общ делител на b и r и обратно. И така

$(a, b)=(b, r)$. Чрез последователно деление ще достигнем до остатък, равен на нула, и последният, различен от нула остатък, ще представлява най-големият общ делител на a и b.

Ако $d=(a, b)$, съществуват цели числа u и v, такива, че

$$d=ua+vb.$$

Когато $(a, b)=1$, казваме, че числата a и b са взаимно прости. Взаимно простите числа нямат други общи делители освен ± 1.

Теорема. Ако $(a, b)=1$ и a/bc, то a/c.

В сила са още следните важни свойства:

а) $(ac, bc)=(a, b)c$.

б) Ако a/c, b/c и $(a, b)=1$, то ab/c.

Определение. Под най-малко общо кратно на числата a и b разбираме число m, притежаващо следните свойства:

1. a/m, b/m;
2. От a/m_1 и b/m_1 следва m/m_1.

С други думи, най-малкото общо кратно е делител на всяко друго общо кратно.

За всеки две цели числа съществува еднозначно определено с точност до знак най-малко общо кратно. Най-малкото общо кратно m на числата a и b ще означаваме с $[a, b]$, при което ще считаме, че $m>0$.

Теорема. За всеки две естествени числа a и b е в сила равенството: $(a, b)\,[a, b]=ab$.

Определение. Едно естествено число p се нарича *просто*, когато $p>1$ и p няма нетривиални делители (различни от ± 1 и $\pm p$).

Теорема. Ако p е просто число и p дели произведението на числата a, b, то p дели поне един от множителите, т. е. от p/ab следва p/a или p/b.

Всяко цяло число $\neq 0$ и $\neq \pm 1$ притежава поне един прост делител. Съществуват безбройно много прости числа.

Основна теорема на аритметиката. Всяко естествено число $n>1$ еднозначно се представя (с точност до реда на множителите) като произведение от прости множители:

$$n=p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_s^{\lambda_s} \tag{1}$$

($s\geq 1$, $p_1, p_2, \ldots, p_s$ — различни прости числа, $\lambda_1, \lambda_2, \ldots, \lambda_s$ — естествени числа).

Функция на Ойлер $\varphi(n)$. Под $\varphi(n)$ разбираме броя на естествените числа, които са по-малки от n и са взаимно прости с n. При $n=1$ полагаме $\varphi(1)=1$.

При $(n, m)=1$ имаме

$$\varphi(mn)=\varphi(m)\,\varphi(n).$$

Ако естественото число n е зададено посредством каноничното си разлагане на прости множители с равенството (1), то

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_s}\right).$$

В частност:

$$\varphi(p^\lambda)=p^\lambda-p^{\lambda-1}.$$

1. Покажете, че ако m, n, p и q са цели числа и $mn+pq$ се дели на $m-p$, то и $mq+np$ се дели на $m-p$.

2. Покажете, че ако m е произволно цяло число, числото m^5-m се дели на 30.

3. Покажете, че при произволно естествено число n, числото $(n+1)(n+2)\ldots(n+n)$ се дели на 2^n, но не се дели на 2^{n+1}.

4. Покажете, че числото $2^{2^n}+1$ при $n>1$ окончава на 7.

5. Покажете, че каквото и да бъде естественото число n, числото n^2+3n+5 не се дели на 121.

Упътване: Използувайте равенствата

$$n^2+3n+5=(n+7)(n-4)+33 \text{ и } (n+7)-(n-4)=11.$$

6. Покажете, че ако k е нечетно число, а n е произволно естествено число, числото $k^{2^n}-1$ се дели на 2^{n+2}.

7. Покажете, че ако петзначното число $\overline{abcde}$ се дели на 41, то всяко от числата

$$\overline{bcdea},\ \overline{cdeab},\ \overline{deabc},\ \overline{eabcd}$$

също се дели на 41.

8. Покажете, че сумата от квадратите на пет последователни цели числа не е квадрат на цяло число.

9. Покажете, че числото $3m^2+2$ не е квадрат на цяло число при никое цяло m.

10. Нека $f(x)$ е полином с цели коефициенти, такъв, че числата $f(2)$ и $f(3)$ се делят на 6. Покажете, че числото $f(5)$ също се дели на 6.

11. Покажете, че ако $n>1$ е произволно естествено число, числото

$$S=\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}$$

не е цяло.

Решение. Нека k е най-голямото естествено число, за което $2^k\leq n$, и P е произведението от всички естествени нечетни числа, ненадминаващи n. Числото $2^{k-1}PS$ е сума, всички събираеми на която освен $2^{k-1}P\cdot\frac{1}{2^k}$ са цели числа. Следователно числото S не е цяло.

12. Покажете, че каквото и да бъде естественото число n, числото

$$S=\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{2n+1}$$

не е цяло.

Решение. Нека k е най-голямото цяло положително число, за което $3^k \leq 2n+1$ и P е произведението на всички взаимно прости с 6 числа, ненадминаващи $2n+1$. Числото $3^{k-1}PS$ е сума, всички събираеми на която освен събираемото $3^{k-1}P \cdot \frac{1}{3^k}$ са цели числа.

13. Докажете, че всичките биномни коефициенти $\binom{n}{s}$ са нечетни тогава и само тогава, когато n има вида $n=2^k-1$.

Решение. При $n \leq 8$ твърдението се проверява непосредствено. Нека n е произволно естествено число и да допуснем, че твърдението е вярно за всички естествени числа, по-малки от n. Очевидно биномните коефициенти

$$(1) \qquad \frac{n}{1}, \frac{n(n-1)}{1.2}, \frac{n(n-1)(n-2)}{1.2.3}, \ldots, \frac{n(n-1)(n-2)\ldots 3.2}{1.2.3\ldots(n-1)}$$

ще бъдат всичките нечетни тогава и само тогава, когато крайните (които са равни на n) са нечетни и числата, които се получават от останалите биномни коефициенти, като премахнем нечетните множители в числителите и знаменателите, са също нечетни. Да положим $n=2m+1$. В такъв случай биномните коефициенти (1) без крайните се представят с числата от редицата

$$\frac{m}{1}, \frac{m(m-1)}{1.2}, \frac{m(m-1)(m-2)}{1.2.3}, \ldots, \frac{m(m-1)(m-2)\ldots 3.2}{1.2.3\ldots(m-1)}.$$

Оттук съгласно индуктивното предположение последните биномни коефициенти, а следователно и биномните коефициенти (1) ще бъдат нечетни тогава и само тогава, когато m има вида $m=2^k-1$, т. е. когато $n=2(2^k-1)+1=2^{k+1}-1$. С това твърдението е доказано.

14. Намерете всички двойки естествени числа a, b, такива, че

$$(a, b)=24 \text{ и } [a, b]=2496.$$

Отг. $a=24$, $b=2496$ и $a=192$, $b=132$.

15. Нека $a_1, a_2, \ldots, a_k$ са дадени цели числа, поне едно от които е различно от нула. С M да означим множеството на всички числа от вида $u_1a_1+u_2a_2+\ldots+u_ka_k$, където $u_1, u_2, \ldots, u_k$ са произволни цели числа. Покажете, че съществува цяло число $a \in M$, такова, че всички числа от M са кратни на a.

Решение. Нека a е най-малкото естествено число, което се съдържа в M. Имаме $a=u_1^0a_1+u_2^0a_2+\ldots+u_k^0a_k$, където u_1^0, u_2^0, u_k^0 са някакви цели числа. Ще покажем, че всеки елемент x от M се дели на a. Наистина нека $x=u_1a_1+u_2a_2+$ $+\ldots+u_ka_k$ и да разделим x на a. Получаваме

$$x=aq+r,$$

където $0 \leq r < a$. От последното равенство имаме

$$r=x-aq=(u_1-u_1^0q)\,a_1+(u_2-u_2^0q)\,a_2+\ldots+(u_k-u_k^0q)a_k.$$

Очевидно $r \in M$ и ако $r \neq 0$, стигаме до противоречие с избора на a. Следователно $r=0$ и за числото $x \in M$ имаме $x=aq$.

16. Като използувате резултата от предната задача, докажете съществуването на най-голям общ делител d на произволна система числа $a_1, a_2, \ldots, a_k$, т. е. такова естествено число d, което е общ делител на дадените числа и се дели на всеки друг

техен общ делител. Докажете, че числото d може да се представи във вида

$$d=u_1a_1+u_2a_2+\dots+u_ka_k,$$

където $u_1, u_2, \dots, u_k$ са цели числа.

Решение. Разглеждаме множеството M от предната задача. С d да означим най-малкото цяло положително число от M. Имаме

$$d=u_1a_1+u_2a_2+\dots+u_ka_k.$$

От последното равенство непосредствено следва, че всеки общ делител на $a_1, a_2, \dots, a_k$ дели d. Числата $a_1, a_2, \dots a_k$ очевидно принадлежат на M и съгласно предната задача всяко от тях се дели на d. Следователно d е най-голям общ делител на числата, $a_1, a_2, \dots, a_k$.

17. Докажете, че ако числата a, b са взаимно прости и a дели произведението bc, то a дели c.

Решение. Понеже числата a, b са взаимно прости, т. е. техният най-голям общ делител е равен на 1, ще бъде в сила равенството

$$ua+vb=1,$$

където u и v са цели числа. Като умножим двете страни на последното равенство с c, получаваме

$$uac+vbc=c,$$

откъдето твърдението на задачата следва непосредствено.

18. Нека a е число, което е взаимно просто с всяко от числата b и c. Докажете, че a е взаимно просто и с произведението bc.

Решение. Понеже $(a, b)=1$ и $(a, c)=1$, ще бъдат в сила равенства от вида

$$u_1a+v_1b=1, \qquad u_2a+v_2c=1,$$

където u_1, v_1, u_2, v_2 са цели числа. Като умножим почленно двете равенства, ще получим равенство от вида

$$ax+bcy=1,$$

откъдето твърдението на задачата следва непосредствено.

19. Нека a и b са взаимно прости числа, всяко от които дели числото c. Покажете, че произведението ab също дели c.

20. Нека p е просто число. Покажете, че a е взаимно просто с числото p тогава и само тогава, когато p не дели a.

21. Покажете, че ако простото число p дели произведението ab на целите числа a и b, то p дели поне един от множителите.

Решение. Твърдението следва непосредствено от зад. 17 и зад. 20. Ще приведем директно доказателство на това твърдение. Да допуснем, че твърдението не е вярно и нека a е най-малкото цяло положително число, такова, че за някое цяло число b да имаме: p дели ab, p не дели a и p не дели b. Като разделим p на a, ще получим $p=aq+r$, където q и r са съответно частното и остатъкът при това деление. Ако $r=0$, ще имаме $p=aq$ и понеже числото p е просто, то $p=a$. Последното обаче противоречи на предположението, че p не дели a. И така остатъкът r е различен от нула. От очевидното равенство $pb=abq+rb$ следва, че p дели rb. По такъв начин достигнахме до противоречие с избора на числото a, понеже $0<r<a$.

22. Нека $a_1, a_2, \ldots, a_n$ са цели числа и с $(a_1, a_2, \ldots, a_n)$ да означим най-големия техен общ делител. Докажете, че

$$(a_1, a_2, \ldots, a_n)=((a_1, a_2, \ldots, a_{n-1}), a_n).$$

23. Покажете, че ако a, b и c са нечетни числа, то

$$(a, b, c)=\left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right).$$

24. Докажете, че броят на числата от редицата

$$a, 2a, 3a, \ldots, ba,$$

които са кратни на b, е равен на (a, b).

25. Нека a и b са взаимно прости естествени числа. Докажете, че сумата от частните на числата

$$a, 2a, 3a, \ldots, (b-1)a$$

с числото b е равна на $\frac{(a+1)(b-1)}{2}$.

26. Проверете равенството:

а) $(a, bc)=(a, b)(a, c)$ при $(a, b, c)=1$;

б) $(a, b)=(a+b, [a, b])$;

в) $(a, [b, c])=[(a, b), (a, c)]$;

г) $[a, (b, c)]=([a, b], [a, c])$;

д) $[(a, b), (b, c), (c, a)]=([a, b], [b, c], [c, a])$.

27. Нека a и b са взаимно прости числа. Покажете, че най-големият общ делител на числата a^3-b^3 и $(a-b)^3$ е равен на $a-b$ или на $3(a-b)$.

28. Нека $(a, b)=1$. Покажете, че $(a\pm b, ab)=1$.

29. Покажете, че при произволно цяло число a числата $\frac{1}{2}a(a+1)$ и $2a+1$ са взаимно прости.

30. Покажете, че ако числата a, b, c са две по две взаимно прости, то $(abc, ab+bc+ca)=1$.

31. Покажете, че ако a и b са две взаимно прости числа от различна четност, то при произволно естествено число n числата $(a+b)^n$ и $(a-b)^n$ са взаимно прости.

32. Нека $(a, b)=1$. Покажете, че

$$(11a+2b, 18a+5b)=1 \text{ или } 19.$$

33. Покажете, че при произволни цели числа a, b, c числото $(a, b, c)^2$ дели числото (ab, bc, ca).

34. Покажете, че при произволни цели числа a, b, c имаме $(a, bc)=(a, (a, b)(a, c))$.

35. Покажете, че каквито и да бъдат целите числа a, b, c, то:

а) $(a, b)=(5a+3b, 13a+8b)$;

б) $(a, b)=(a+bc, a+b(c-1))$.

36. Покажете, че най-малкото общо кратно на три последователни числа е равно на произведението им или на полупроизведението им.

37. Докажете, че при произволно естествено число n е в сила равенството

$$[1, 2, 3, \ldots, 2n]=[n+1, n+2, n+3, \ldots, 2n].$$

38. Нека $a_1, a_2, \ldots, a_n$ са естествени числа. Докажете, че

$$m=[a_1, a_2, \ldots, a_n]=\frac{a}{d},$$

където $a=a_1a_2\ldots a_n$, $d=\left(\frac{a}{a_1}, \frac{a}{a_2}, \ldots, \frac{a}{a_n}\right)$.

Решение. Да положим $\frac{a}{d}=x$, $\frac{a}{a_i}=q_i$, $i=1, 2, \ldots, n$. Тогава ще имаме

(1) $$x=a_1\frac{q_1}{d}=a_2\frac{q_2}{d}=\ldots=a_n\frac{q_n}{d},$$

откъдето непосредствено следва, че всяко от числата $a_1, a_2, \ldots, a_n$ дели числото x. Следователно x представлява общо кратно на числата $a_1, a_2, \ldots, a_n$ и ще се дели на най-малкото им общо кратно m, т. е. ще имаме $x=mq$, където $q\geq 1$. Равенствата (1) при $x=mq$ могат да се запишат във вида

$$\frac{m}{a_1}q=\frac{q_1}{d}, \frac{m}{a_2}q=\frac{q_2}{d}, \ldots, \frac{m}{a_n}q=\frac{q_n}{d},$$

откъдето непосредствено следва, че q е общ делител на взаимно простите числа $\frac{q_1}{d}, \frac{q_2}{d}, \ldots, \frac{q_n}{d}$. Следователно $q=1$ и $\frac{a}{d}=m$, с което твърдението е доказано.

39. Докажете, че ако a, b и c са естествени числа, то

$$[a, b, c]=\frac{abc}{(ab, ac, bc)}.$$

Упътване. Твърдението е частен случай на твърдението от предната задача.

40. Докажете, че съществуват безбройно много прости числа.

Решение. Ще изложим доказателството на Евклид. Нека $p_1, p_2, \ldots, p_k$ са k прости числа. Да разгледаме числото

$$P=p_1p_2\ldots p_k+1.$$

Числото P притежава поне един прост делител p_{k+1}, който очевидно не съвпада с никое от простите числа $p_1, p_2, \ldots, p_k$.

41. Покажете, че всяко нечетно просто число може да се представи във вида $4k-1$ или $4k+1$, където k е цяло число.

42. Покажете, че всяко просто число $p>3$ може да се представи във вида $6k-1$ или $6k+1$, където k е цяло число.

43. Докажете, че съществуват безбройно много прости числа от вида $4k-1$.

Упътване. Разгледайте числото $P=4p_1 p_2 \ldots p_s-1$, където $p_1, p_2, \ldots, p_s$ са прости числа от вида $4k-1$, и използувайте, че произведението на числа от вида $4l+1$ е число от същия вид.

44—45. Докажете, че съществуват безбройно много прости числа от вида $6k-1$.

Забележка. Зад. 44 и зад. 45 са частни случаи от важната **теорема на Дирихле:**

Всяка безкрайна аритметична прогресия, в която първият член и разликата са взаимно прости числа, съдържа безбройно много прости числа.

46. Покажете, че ако $n>2$ е цяло число, числата 2^n-1 и 2^n+1 не могат да бъдат едновременно прости.

Решение. Очевидно 3 не дели 2^n, откъдето следва, че при $n>2$ числото 2^n е от вида $3k+1$ или $3k-1$. В първия случай числото 2^n-1 се дели на 3, а във втория числото 2^n+1 се дели на 3.

47. Намерете всички прости числа p, за които числата $p+10$ и $p+20$ са също прости.

Решение. Очевидно, ако p е такова просто число, то $p>2$. Следователно простото число p е равно на 3 или има вида $3k\pm1$.

При $p=3$ за $p+10$ и $p+20$ получаваме съответно 13 и 23, които числа са прости.

При $p=3k+1$ за $p+10$ и $p+20$ имаме съответно $3k+11$ и $3k+21$, от които второто число е съставно.

При $p=3k-1$ за $p+10$ и $p+20$ получаваме съответно $3k+9$ и $3k+19$, от които първото число е съставно.

И така условието на задачата е удовлетворено само при $p=3$.

48. Намерете всички прости числа p, за които числата $p+4$ и $p+14$ са също прости.

Отг. $p=3$.

49. Намерете всички прости числа p, за които числото $8p^2+1$ е просто.

Отг. $p=3$

50. Покажете, че ако числата p и $8p-1$ са едновременно прости, числото $8p+1$ е съставно.

51. Покажете, че ако числата p и $8p^2+1$ са едновременно прости, числото $8p^2-p+2$ е съставно.

52. Намерете всички прости числа p, за които числата $4p^2+1$ и $6p^2+1$ са също прости.

Отг. $p=5$.

53. Покажете, че ако числата p и $2p+1$ са едновременно прости, числото $4p+1$ при $p>3$ е съставно.

54. Покажете, че ако числата $8n+1$ и $24n+1$ са квадрати на цели числа, числото $8n+3$ при $n>1$ е съставно.

55. Покажете, че от всички числа от вида $2p+1$, където p е просто, само числото 27 е куб на цяло число.

56. Нека p е просто число, по-голямо от 5. Покажете, че остатъкът при делението на p^2 с 30 е равен на 1 или на 19.

Решение. Да представим числата от естествения ред по следния начин;

$$30k,\ 30k\pm1,\ 30k\pm2, \dots, 30k\pm15.$$

От тях прости могат да бъдат само числата:

$$30k\pm1,\ 30k\pm7,\ 30k\pm11,\ 30k\pm13.$$

По-нататък решението е ясно.

57. Покажете, че ако p и q са прости числа, по-големи от 3, числото p^2-q^2 се дели на 24.

Решение. Да представим p^2-q^2 във вида

$$(1)\qquad p^2-q^2=(p-1)(p+1)-(q-1)(q+1).$$

Понеже p и q са нечетни, всяко от числата $(p-1)(p+1)$ и $(q-1)(q+1)$ като произведение на две последователни четни числа се дели поне на 8. От друга страна, всяко от числата $(p-1)\,p(p+1)$ и $(q-1)\,q\,(q+1)$ като произведения на три последователни числа се дели на 3. Но съгласно условието на задачата $(p, 3)=1$ и $(q, 3)=1$. Следователно 3 дели числата $(p-1)(p+1)$ и $(q-1)(q+1)$. Накрая, като вземем пред вид още, че $(8, 3)=1$ и равенството (1), непосредствено следва, че p^2-q^2 се дели на 24.

58. Покажете, че нечетното число n е просто тогава и само тогава, когато се представя по единствен начин като разлика от квадратите на две естествени числа.

Решение. За всяко естествено нечетно число n е в сила равенството

$$(1)\qquad n=\left(\frac{n+1}{2}\right)^2-\left(\frac{n-1}{2}\right)^2.$$

Нека n е просто число, за което да имаме $n=u^2-v^2$, където u и v са цели положителни числа. От разлагането $n=(u-v)(u+v)$ следва $u-v=1$, $u+v=n$, т. е. $u=\frac{n+1}{2}$ и $v=\frac{n-1}{2}$. И така, ако n е просто, представянето (1) е единственото представяне на n като разлика от квадрати на естествени числа. Обратно, нека n е съставно. Тогава ще съществуват естествени числа a, b, при това нечетни, така че $n=ab$ и $1<a\leq b<n$. Очевидното равенство

$$n=\left(\frac{a+b}{2}\right)^2-\left(\frac{a-b}{2}\right)^2$$

ни дава друго представяне (различно от (1)) на съставното число n като разлика от квадрати на естествени числа.

59. Да се докаже, че не съществува полином $f(x)$ с цели коефициенти, за който числото $f(n)$ да е просто при всяка цяла стойност на n.

Решение. Нека $f(x)$ е произволен полином с цели коефициенти и $x=x_0$ да е цяла стойност на x, за която числото $f(x_0)=p$ е просто. Да образуваме стойността $f(x_0+py)$ на полином $f(x)$ при $x=x_0+py$, където y е произволно цяло число. Ще имаме

$$f(x_0+py)=f(x_0)+pg(y)=p[1+g(y)].$$

Очевидно $g(y)$ е полином с цели коефициенти. Ако числото $f(x_0+py)$ е просто при всяко цяло y, би трябвало $1+g(y)=1$, а това би означавало, че уравнението $g(y)=0$ има безбройно много корени, което е невъзможно.

60. Нека $2^m-1=ab$, където m, a, b са естествени числа, по-големи от 1. Докажете, че $a+b=2^k a_1$, $b-1=2^k b_1$ и числата k, a_1, b_1 са нечетни.

Упътване. Използувайте равенството

$$2^m=(a+1)(b-1)+(a+1)-(b-1).$$

61. Докажете, че ако числото 2^k+1 е просто, то $k=0$ или $k=2^n$ $(n=0, 1, 2,\ldots)$.

62. Докажете, че ако a, b, m и n са естествени числа, за които числото a^m+b^n е просто, то най-големият общ делител на m и n е равен на 1 или е степен на 2.

63. Всички прости числа, ненадминаващи простото число p, разделяме на две групи $p_1, p_2,\ldots, p_k$ и $q_1, q_2,\ldots,q_s$, така че $1<p_1p_2\ldots p_k-q_1q_2\ldots q_s<p^2$. Покажете, че числото $p_1 p_2\ldots p_k-q_1q_2\ldots q_s$ е просто.

64. Докажете, че ако a и b са взаимно прости естествени числа, то $\varphi(ab)=\varphi(a)\varphi(b)$, (тук $\varphi(n)$ означава функцията на Ойлер).

Решение. Ще използуваме следното свойство: едно число е взаимно просто с произведението ab тогава и само тогава, когато това число е взимно просто поотделно с a и с b. Оттук следва, че задачата се свежда до намиране броя на естествените числа, по-малки от ab и взаимно прости както с a, така и с b. За целта да подредим естествените числа от 1 до ab в следната таблица

$$\begin{matrix} 1 & 2\ \ldots & k\ \ldots & b \\ b+1 & b+2\ \ldots & b+k\ \ldots & 2b \\ 2b+1 & 2b+2\ \ldots & 2b+k\ \ldots & 3b \\ \ldots & \ldots & \ldots & \ldots \\ (a-1)b+1 & (a-1)b+2\ \ldots & (a-1)b+k\ \ldots & ab \end{matrix}$$

Числата от кой да е стълб на таблицата се различават помежду си със събираемо кратно на b. Оттук следва, че те имат с b един и същ най-голям общ делител, който е равен на най-големия общ делител на b и числото, стоящо на първо място в съответния стълб. Следователно броят на стълбовете, съставени от числа, взаимно прости с b, е равен на броя на естествените числа от 1 до b, които са взаимно прости с b, т. е. на $\varphi(b)$.

Да разгледаме сега произволен стълб, например

$$(1)\qquad k,\ b+k,\ 2b+k,\ \ldots,\ (a-1)b+k,$$

и с $r_0, r_1, r_2,\ldots,r_{a-1}$ да означим остатъците от делението на числата от този стълб с a. Понеже $(a, b)=1$, непосредствено се проверява, че $r_i\neq r_j$ при $i\neq j$. Следователно остатъците $r_0, r_1,\ldots, r_{a-1}$ са числата $0, 1, 2,\ldots, a-1$, но изобщо в някакъв друг ред. Като вземем пред вид още, че $(sb+k, a)=(r_s, a)$, $s=0,1,\ldots,a-1$, е ясно, че числото $sb+k$ е тогава и само тогава взаимно просто с a, когато r_s е взаимно просто с a.

Следователно броят на числата (1), взаимно прости с a, е равен на $\varphi(a)$. По такъв начин се убеждаваме, че всеки стълб на таблицата съдържа $\varphi(a)$ на брой числа, взаимно прости с a. И така таблицата съдържа $\varphi(b)$ стълба, числата на които са взаимно прости с b, и всеки стълб съдържа $\varphi(a)$ числа, взаимно прости с a. Оттук непосредствено следва, че броят на числата, по-малки от ab и взаимно прости както с a, така и с b, е равна на $\varphi(a)\varphi(b)$, т. е.

$$\varphi(ab)=\varphi(a)\varphi(b).$$

Доказаното свойство остава в сила и за случая на произведение от произволен краен брой два по два взаимно прости множители.

65. Нека p е просто число, а λ е произволно естествено число. Покажете, че

$$\varphi(p^{\lambda})=p^{\lambda}\left(1-\frac{1}{p}\right).$$

Решение. Трябва да пресметнем броя на естествените числа, по-малки от p^{λ} и взаимно прости с p^{λ}. Очевидно

$$p,\ 2p,\ 3p,\ldots,p^{\lambda-1}p$$

са всичките числа, ненадминаващи p^{λ} и които не са взаимно прости с p^{λ}. Понеже броят на тези числа е равен на $p^{\lambda-1}$, за $\varphi(p^{\lambda})$ ще имаме

$$\varphi(p^{\lambda})=p^{\lambda}-p^{\lambda-1}=p^{\lambda}\left(1-\frac{1}{p}\right).$$

66. Нека $n=p^{\lambda}q^{\mu}\ldots r^{\nu}$ е каноничното разлагане на естественото число n на прости множители. Покажете, че

$$\varphi(n)=n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\ldots\left(1-\frac{1}{r}\right).$$

Упътване. Използувайте резултатите от зад. 64 и зад. 65.

67. Намерете броя на естествените числа, по-малки от 4320 и взаимно прости с 4320.

Отг. 1152

68. Намерете броя на естествените числа, по-малки от 120 не взаимно прости с 30.

Отг. 88.

69. За естественото число a знаем, че $\varphi(a)=3600$ и $a=3^{\alpha}5^{\beta}7^{\gamma}$. Намерете a.

Отг. 7875.

70. Дадено е, че $\varphi(a)=120$ и $a=pq$, където p и q са различни прости числа. Намерете a, ако $p-q=2$.

Отг. $a=143$.

71. Намерете естественото число a, ако е известно, че $\varphi(a)=11\,424$ и $a=p^2q^2$, където p и q са различни прости числа.

Отг. $a=14\,161$.

72. Нека S е сумата на всички естествени числа, по-малки от m и взаимно прости с m. Покажете, че

$$S=\frac{1}{2}m\varphi(m).$$

Упътване. Използувайте, че ако $(a, m)=1$, то $(a, m-a)=1$.

73. Като използувате резултата от предната задача, пресметнете сумата S за числото m, където

а) $m=28$; б) $m=46$; $m=375$.

Отг. а) $S=168$; б) $S=506$; в) $S=375\,000$.

74. Покажете, че броят на положителните несъкратими правилни дроби, знаменателят на които не надминава естественото число n, е равен на $\varphi(2)+\varphi(3)+\ldots+\varphi(n)$.

75. Като използувате резултата от предната задача, намерете броя на всички положителни несъкратими правилни дроби, знаменателят на които не надминава n, където:

а) $n=5$; б) $n=10$; в) $n=15$.

Отг. а) 9; б) 31; в) 71.

76. Покажете, че за произволни естествени числа n и k е в сила равенството

$$\varphi(n^k)=n^{k-1}\varphi(n).$$

77. Нека d и m са съответно най-големият общ делител и най-малкото общо кратно на естествените числа a и b. Покажете, че

$$\varphi(ab)=d\varphi(m).$$

78. Нека n и d са дадени естествени числа, като d не надминава n. Намерете броя на естествените числа, ненадминаващи n, най-големият общ делител на които с n е равен на d.

Решение. С $\varphi_d(n)$ да означим търсения брой. Очевидно $\varphi_1(n)=\varphi(n)$. Произволно число от интересуващите ни числа ще има вида dq, където $q\leq\frac{n}{d}$. От условието $(n, dq)=d$ получаваме $\left(\frac{n}{d}, q\right)=1$, откъдето следва $\varphi_d(n)=\varphi_1\left(\frac{n}{d}\right)=$ $=\varphi\left(\frac{n}{d}\right)$.

79. В означенията на предната задача пресметнете:

а) $\varphi_{12}(660)$; б) $\varphi_{20}(580)$; в) $\varphi_{17}(595)$.

Отг. а) 40; б) 28; в) 24.

80. Нека n е естествено число и със $\sum\limits_{d/n}\varphi(d)$ да означим сумата от индикаторите на всички делители на n. Докажете, че

$$\sum_{d/n}\varphi(d)=n.$$

81. Решете уравненията:

а) $\varphi(x)=12$;
б) $\varphi(2x)=\varphi(3x)$;
в) $\varphi(x)=\frac{1}{2}x$;

Отг. а) $x=13, 21, 26, 28, 42, 36$;
б) $x=2^{\lambda}y$, където $(6, y)=1$;
в) $x=2^{\lambda}$;

г) $\varphi(x)=-\frac{2}{3}x$; г) $x=3^{\lambda}$;

д) $\varphi(x)=\frac{1}{3}x$; д) $x=2^{\lambda}3^{\mu}$;

е) $\varphi(x)=\frac{1}{4}x$. е) уравнението няма решение.

Определение. Цяла част $[x]$ на реалното число x се нарича най-голямото цяло число, което не надминава x. Например $[-3,4]=-4$, $[5,3]=5$, $[\sqrt{10}]=3$, $[2]=2$ и т. н.

82. Докажете следните свойства на функцията $[x]$:

а) $[x+y]\geq[x]+[y]$;

б) $[x+n]=[x]+n$, където n е произволно цяло число;

в) $[2x]+[2y]\geq[x]+[x+y]+[y]$;

г) $\left[\frac{[x]}{n}\right]=\left[\frac{x}{n}\right]$, където n е произволно естествено число;

д) $[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\ldots+\left[x+\frac{n-1}{n}\right]=[nx]$,

където n е произволно естествено число.

Решение.

а) Реалното число x можем да представим във вида $x=[x]+\alpha$, където $0\leq\alpha<1$. Аналогично за y имаме $y=[y]+\beta$, където $0\leq\beta<1$. От почленното събиране на двете равенства получаваме $x+y=[x]+[y]+\alpha+\beta$, от което равенство следва, че цялото число $[x]+[y]$ не надминава $x+y$. Но тъй като $[x+y]$ е най-голямото число с това свойство, то $[x+y]\geq[x]+[y]$.

б) От очевидните неравенства $x+n-1<[x+n]\leq x+n$ получаваме $x-1<[x+n]-n\leq x$, откъдето следва, че $[x+n]-n\leq[x]$, т. е. $[x+n]=[x]+n$.

в) Съгласно свойство б), ако увеличим x и y с цели числа, двете страни на неравенството ще се увеличат с едно и също число. Следователно без ограничение на общността можем да предполагаме, че $0\leq x<1$, $0\leq y<1$. При това предположение трябва да покажем, че е в сила неравенството

$$[2x]+[2y]\geq[x+y].$$

Ако $[x+y]=0$, последното неравенство очевидно е изпълнено. Ако $[x+y]\geq1$, то $x+y\geq1$, откъдето следва, че поне едно от числата x и y, например x, е по-голямо от $\frac{1}{2}$. Следователно $[2x]+[2x]\geq[2x]\geq1=[x+y]$.

г) Да представим x във вида $x=[x]+\alpha$, където $0\leq\alpha<1$. С q и r да означим съответно частното и остатъка при делението на $[x]$ с n. Ще имаме

$$[x]=nq+r,\ 0\leq r\leq n-1.$$

Оттук получавме

$$\frac{[x]}{n}=q+\frac{r}{n},$$

откъдето $\left[\frac{[x]}{n}\right]=q$.

Да пресметнем сега $\left[\frac{x}{n}\right]$. Имаме

$$x=[x]+\alpha=nq+r+\alpha=nq+r_1,$$

където $r_1=r+\alpha<n$. Оттук получаваме

$$\frac{x}{n}=q+\frac{r_1}{n},$$

откъдето следва $\left[\frac{x}{n}\right]=q=\left[\frac{[x]}{n}\right]$, което трябваше да докажем.

д) Съгласно свойство б) достатъчно е да разгледаме случая $0\leq x<1$. При $x=0$ равенството очевидно е вярно. Нека $x>0$. В такъв случай съществува естествено число $m\leq n$, такова, че да са в сила неравенствата

$$x+\frac{m-1}{n}<1\leq x+\frac{m}{n}. \tag{1}$$

Неравенствата (1) могат да се запишат още във вида

$$n-nx\leq m<n-nx+1,$$

откъдето следва, че $m=[n-nx]=n-[nx]$. Следователно дясната страна $[nx]$ на интересуващото ни равенство е $[nx]=n-m$.

От друга страна, съгласно неравенствата (1) имаме

$$\left[x+\frac{k}{n}\right]=\begin{cases}0, & \text{при } 0\leq k<m;\\ 1, & \text{при } m\leq k\leq n,\end{cases}$$

откъдето непосредствено следва, че лявата страна на интересуващото ни равенство е също равно на $n-m$.

83. Покажете, че ако p и q са взаимно прости числа, то

$$\sum_{k=1}^{q-1}\left[\frac{kp}{q}\right]=\sum_{l=1}^{p-1}\left[\frac{lq}{p}\right]=\frac{1}{2}(p-1)(q-1).$$

84. Нека σ_k означава броя на положителните делители на естественото число n, а s_k означава сумата на тези делители. Докажете равенствата

а) $\sigma_1+\sigma_2+\ldots+\sigma_n=\left[\frac{n}{1}\right]+\left[\frac{n}{2}\right]+\ldots+\left[\frac{n}{n}\right]$;

б) $s_1+s_2+\ldots+s_n=\left[\frac{n}{1}\right]+2\left[\frac{n}{2}\right]+\ldots+n\left[\frac{n}{n}\right]$.

Решение. Ще приложим метода на пълната математическа индукция. При $n=1$ равенствата очевидно са верни. Да предположим, че те са верни при $n=m$. При това предположение ще покажем, че те остават в сила и при $n=m+1$. При доказателството ще използваме следните равенства, които се проверяват непосредствено:

$$\left[\frac{m+1}{k}\right]=\left[\frac{m}{k}\right], \text{ ако } k \text{ не дели } m;$$

$$\left[\frac{m+1}{k}\right]=\left[\frac{m}{k}\right]+1, \text{ ако } k \text{ дели } m.$$

Оттук следва, че

а) $\left[\frac{m+1}{1}\right]+\left[\frac{m+1}{2}\right]+\ldots+\left[\frac{m+1}{m+1}\right]=\left[\frac{m}{1}\right]+\ldots+\left[\frac{m}{m}\right]+\sigma_{m+1}$, т. е. ако

$$\left[\frac{m}{1}\right]+\left[\frac{m}{2}\right]+\ldots+\left[\frac{m}{m}\right]=\sigma_1+\sigma_2+\ldots+\sigma_m,$$

то

$$\left[\frac{m+1}{1}\right]+\left[\frac{m+1}{2}\right]+\ldots+\left[\frac{m+1}{m+1}\right]=\sigma_1+\sigma_2+\ldots+\sigma_m+\sigma_{m+1}.$$

б) $$\left[\frac{m+1}{1}\right]+2\left[\frac{m+1}{2}\right]+\ldots+(m+1)\left[\frac{m+1}{m+1}\right]=$$

$$=\left[\frac{m}{1}\right]+2\left[\frac{m}{2}\right]+\ldots+m\left[\frac{m}{m}\right]+s_{m+1},$$

т. е. ако

$$\left[\frac{m}{1}\right]+2\left[\frac{m}{2}\right]+\ldots+m\left[\frac{m}{m}\right]=s_1+s_2+\ldots+s_m,$$

то

$$\left[\frac{m+1}{1}\right]+2\left[\frac{m+1}{2}\right]+\ldots+(m+1)\left[\frac{m+1}{m+1}\right]=s_1+s_2+\ldots+s_m+s_{m+1}.$$

85. Като използувате равенствата от предната задача, пресметнете броя на делителите на всички естествени числа от 1 до 28 и сумата от тези делители.

Отг. 101 и 660.

86. Докажете, че ако a, b и n са произволни естествени числа, то

$$\left[\frac{\left[\frac{n}{a}\right]}{b}\right]=\left[\frac{n}{ab}\right].$$

Решение. Да положим $\left[\frac{n}{a}\right]=q$, $\left[\frac{q}{b}\right]=q_1$.

Тогава ще имаме

$$n=aq+r,\ q=bq_1+r_1,$$

където $0\leqq r<a$, $0\leqq r_1<b$. Оттук получаваме

$$n=abq_1+(r+ar_1),$$

където $0\leqq r+ar_1\leqq a-1+a(b-1)=ab-1<ab$. Следователно

$$\left[\frac{n}{ab}\right]=q_1=\left[\frac{q}{b}\right]=\left[\frac{\left[\frac{n}{a}\right]}{b}\right],$$

което трябваше да докажем.

87. Намерете показателя на най-високата степен на простото число p, която дели $n!$

Отг. $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$

88. Намерете степенния показател на числото 11 в каноничното разлагане на числото 1000!.

Отг. 98.

89. С колко нули окончава числото 293!?

Отг. 71.

90. Намерете броя на естествените числа, ненадминаващи 1000 и взаимно прости с 363.

Отг. 393.

91. Ако n е цяло положително число и $\alpha, \beta, \gamma, \ldots, \lambda$ са естествени числа, за които $\alpha+\beta+\gamma+\ldots+\lambda=n$, докажете, че

$$\frac{n!}{\alpha!\,\beta!\,\gamma!\ldots\lambda!} \tag{1}$$

е цяло число.

Решение. Нека p е произволно просто число. Показателят k на степента на p, която дели знаменателя на (1), е равен на

$$k=\sum_m\left[\frac{\alpha}{p^m}\right]+\sum_m\left[\frac{\beta}{p^m}\right]+\ldots+\sum_m\left[\frac{\lambda}{p^m}\right],$$

а показателят k_1 на p в числителя е $k_1=\sum\limits_m\left[\frac{n}{p^m}\right]$.

Понеже $n=\alpha+\beta+\gamma+\ldots+\lambda$, то

$$\left[\frac{n}{p^m}\right]\geq\left[\frac{\alpha}{p^m}\right]+\left[\frac{\beta}{p^m}\right]+\ldots+\left[\frac{\lambda}{p^m}\right],$$

т. е. $k_1\geq k$. Следователно всяка степен на просто число, която дели знаменателя на (1), ще дели и числителя.

92. Да се определи най-високата степен на едно просто число p, която дели $\binom{n}{m}$.

Отг. $\sum\limits_i\left[\frac{n}{p^i}\right]-\sum\limits_i\left[\frac{m}{p^i}\right]-\sum\limits_i\left[\frac{n-m}{p^i}\right]$.

93. Да се определи показателят на най-високата степен на едно просто число p, която дели $(m+1)(m+2)\ldots(n-1)n$.

Отг. $\sum\limits_i\left[\frac{n}{p^i}\right]-\sum\limits_i\left[\frac{m}{p^i}\right]$.

94. Да се определи показателят на най-високата степен на простото число p, която дели произведението

$$1.\ 3.\ 5.\ 7\ldots(2n+1).$$

Отг. $\sum\limits_i\left[\frac{2n+1}{p^i}\right]-\sum\limits_i\left[\frac{n}{p^i}\right]$

95. Като използувате резултата от зад. 92, намерете показателя на най-високата степен на числото 7, която дели биномния коефициент $\binom{117}{32}$.

Отг. 1.

96. Като използувате резултата от зад. 94, намерете показателя на най-високата степен на числото 5, която дели числото 3. 5. 7...301.

Отг. 37.

§ 2. СРАВНЕНИЯ

Определение. Ако естественото число m дели разликата $a-b$ на целите числа a, b пишем

$$a \equiv b \pmod m \tag{1}$$

и казваме, че a е *сравнимо* с b по модул m.

Сравнението (1) е равносилно с равенство от вида

$$a = b + km \quad (k\text{—цяло}).$$

Очевидно $a \equiv b \pmod m$ тогава и само тогава, когато числата a и b имат един и същ остатък при деление с m.

Свойства:

а) $a \equiv a \pmod m$;

б) $a \equiv b \pmod m$ е равносилно с $b \equiv a \pmod m$;

в) от $a \equiv b \pmod m$ и $b \equiv c \pmod m$ следва $a \equiv c \pmod m$;

г) релацията сравнение по модул m е съгласувана с алгебричните операции събиране и умножение, т. е. сравненията по даден модул m могат да се събират и умножават почленно: от $a \equiv a_1 \pmod m$ и $b \equiv b_1 \pmod m$ следва $a+b \equiv a_1+b_1 \pmod m$ и $ab \equiv a_1b_1 \pmod m$;

д) от $ka \equiv kb \pmod m$ и $(k, m) = \delta$ следва $a \equiv b \left(\bmod \frac{m}{\delta}\right)$ — в частност можем да съкращаваме двете страни на сравнението на общ множител k, без да променяме модула m само когато този общ множител е взаимно прост с модула m.

Свойствата а), б), в) означават, че сравнението по даден модул m е релация на еквивалентност в множеството Z на целите числа. Следователно посредством тази релация множеството Z се разбива на непресичащи се класове от сравними помежду си числа. Броят на тези класове е равен на броя m от всевъзможните остатъци, които се получават при деление с модула m. Ако $a \in Z$ дава остатък r при деление с m, класът $\bar{a}$, към който принадлежи числото a, ще се състои от всички цели числа $r+km$, k— произволно цяло число.

Множеството от всичките класове

$$\bar{0},\ \bar{1},\ \bar{2},\ldots,\ \overline{m-1},$$

съдържащи съответно числата

$$0,\ 1, 2,\ldots,\ m-1,$$

ще означаваме с Z_m. Елементите на Z_m ще наричаме още класове от остатъци по модул m.

Определение. Всяка система от m на брой несравними помежду си по модул m числа ще наричаме *пълна система от остатъци* по модул m.

Най-прост пример за пълна система остатъци по модул m е системата от числата $0, 1, 2,\ldots, m-1$. Ако $x_0, x_1,\ldots, x_{m-1}$ е пълна система остатъци по модул m, класовете

$$\bar{x}_0,\ \bar{x}_1,\ldots,\ \bar{x}_{m-1}$$

са различни и изчерпват цялото множество Z_m.

Теорема. Ако $x_0, x_1,\ldots, x_{m-1}$ е пълна система остатъци по модул m и числото a е взаимно просто с m, числата

$$ax_0+b,\ ax_1+b,\ldots, ax_{m-1}+b,$$

където b е произволно цяло число, също образуват пълна система остатъци по модул m.

Определение. Казваме, че числото x_0 е *решение* на сравнението

(2) $$ax+b\equiv 0 \pmod{m},$$

когато $ax_0+b\equiv 0 \pmod{m}$, и при това всеки две решения x_1 и x_2 на сравнението (2), за които $x_1\equiv x_2 \pmod{m}$, ще считаме за неразлични.

Теорема. При $(a, m)=1$ сравнението (2) има точно едно решение.

Пример. Сравнението $5x+4\equiv 0 \pmod{12}$ има точно едно решение $x\equiv 4 \pmod{12}$.

По-общо в сила е следната теорема: при $(a, m)=\delta$ сравнението (2) има точно δ на брой решения по модул m или няма решения в зависимост от това, дали δ дели свободния член b, или не го дели.

За да решим сравнението (2), достатъчно е да решим неопределеното уравнение $ax+b=my$ в цели числа x, y. Решението на последното уравнение може да се извърши по метода на Ойлер, който ще изясним чрез следния пример. Да решим сравнението

$$15x+7\equiv 0 \pmod{23}.$$

С други думи, трябва да решим неопределеното уравнение

$$15x+7=23y.$$

Решаваме това уравнение спрямо неизвестното с по-малък коефициент и получаваме

$$x=\frac{23y-7}{15}=y+\frac{8y-7}{15}.$$

Понеже x и y са цели числа, числото $\frac{8y-7}{15}=z$ трябва също да е цяло. Записваме последното уравнение във вида $8y-7=15z$ и го решаваме спрямо неизвестното y, което се явява с по-малък коефициент. Получаваме

$$y=\frac{15z+7}{8}=2z-\frac{z-7}{8}.$$

Числото $\frac{z-7}{8}=u$ трябва да бъде цяло, откъдето намираме $z=7+8u$. Тогава за неизвестното x ще имаме $x=21+23u$. И така решенията на неопределеното уравнение $15x+7=23y$ са $x=21+23u$, $y=14+15u$, където u е произволно цяло число. Оттук получаваме, че решението на даденото сравнение

$$15x+7\equiv 0 \pmod{23}$$

е

$$x\equiv 21 \pmod{23}.$$

Когато коефициентът a не е взаимно прост с модула m, т. е. $(a, m)=\delta>1$, и когато δ/b, за да решим сравнението (2), разделяме почленно двете страни и модула с δ и разглеждаме сравнението

$$a_1x+b_1\equiv 0 \pmod{m_1}, \tag{3}$$

където $a_1=\frac{a}{\delta}$, $b_1=\frac{b}{\delta}$, $m_1=\frac{m}{\delta}$.

Имаме $(a_1, m_1)=1$ и следователно можем да намерим решение x_0 на сравнението (3). Тогава числата

$$x_k=x_0+k\frac{m}{\delta},\ k=0,\ 1,\ 2, \ldots,\ \delta-1$$

ще представляват всичките δ на брой различни решения на даденото сравнение (2).

Определение. Всяка система от $\varphi(m)$ на брой числа, които са несравними по модул m и са взаимно прости с модула, се нарича *приведена система остатъци* по модул m.

Теорема. Ако $(a, m)=1$ и $x_1, x_2, \ldots, x_k$, $k=\varphi(m)$ е приведена система остатъци по модул m, числата

$$ax_1, \ ax_2, \ldots, ax_k$$

също образуват приведена система остатъци по модул m.

Теорема на Ферма—Ойлер. При $(a, m)=1$ е в сила сравнението

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

В частност при $m=p$ просто се получава следната

Теорема на Ферма. За всяко цяло число a, което не се дели на простото число p, е в сила сравнението

$$a^{p-1} \equiv 1 \pmod{p}.$$

Теорема на Уилсън. За всяко просто p е в сила сравнението

$$(p-1)!+1 \equiv 0 \pmod{p}.$$

Алгебрични действия в Z_m. Свойството г) наред с изброените по-горе свойства на сравненията ни дава възможност да дефинираме по естествен начин операциите събиране и умножение в множеството Z_m, като приемем по дефиниция следните равенства:

$$\bar{a}+\bar{b}=\overline{a+b} \text{ и } \bar{a}\,\bar{b}=\overline{ab}.$$

Относно така дефинираните операции в Z_m са в сила обичайните закони, както при действията събиране и умножение с числа. Когато модулът $m=p$ е просто число, в Z_p можем да извършваме и деление, стига делителят да е $\neq \bar{0}$, т. е. уравнението

$$\bar{a}\,\bar{x}=\bar{b} \quad (\bar{a}, \bar{b} \in Z_p, \ \bar{a} \neq \bar{0})$$

има точно едно решение $\bar{x} \in Z_p$.

Пример. В Z_5 уравнението $\bar{3}\,\bar{x}+\bar{4}=\bar{0}$ има единствено решение $\bar{x}=\bar{2}$, което може да се получи, като решим сравнението $3x+4 \equiv 0 \pmod{5}$.

Ще илюстрираме действията в Z_m, като разгледаме за конкретност случая $m=4$ и посочим съответните таблици за събиране и умножение в Z_4:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

1. Докажете, че цялото число N се дели на 9 тогава и само тогава, когато сумата от цифрите му се дели на 9.

2. Докажете, че цялото число N се дели на 11 тогава и само тогава, когато сумата от цифрите му, стоящи на нечетно място, е сравнима със сумата от цифрите, стоящи на четно място по модул 11.

3. Докажете, че числото $2^{32}+1$ се дели на 641.

Решение. Имаме

$$641=5^4+2^4\equiv 0 \pmod{641}.$$

От друга страна,

$$641=640+1=5\,.\,128+1=5\,.\,2^7+1\equiv 0 \pmod{641},$$

т. е. $5\,.\,2^7\equiv -1 \pmod{641}$, откъдето получаваме $5^4\,.\,2^{28}\equiv 1 \pmod{641}$. Тогава $-2^4\,.\,2^{28}\equiv 1 \pmod{641}$, или все едно $2^{32}+1\equiv 0 \pmod{641}$.

4. Намерете остатъка от делението на числото 341^{17} с числото 72.

Отг. 53.

5. Намерете последните две цифри на числото 783^{15}.

Упътване. Намерете остатъка от делението на даденото число със 100.

Отг. 0 и 7.

6. Докажете, че

$$2^{11\,.\,31}\equiv 2 \pmod{11\,.\,13}.$$

Решение. С непосредствена проверка се убеждаваме, че

$$11\,.\,31-1=340=5\,.\,68 \text{ и } 2^5\equiv -1 \pmod{11}.$$

Като повдигнем последното сравнение в 68-ма степен, получаваме

$$(1)\qquad (2^5)^{68}=2^{340}=2^{11\,.\,31-1}\equiv 1 \pmod{11}.$$

Тъй като $2^5\equiv 1 \pmod{31}$, то

$$(2)\qquad (2^5)^{68}=2^{11\,.\,31-1}\equiv 1 \pmod{31}.$$

Понеже числата 11 и 31 са взаимно прости, то

$$2^{11\,.\,31-1}\equiv 1 \pmod{11\,.\,31},$$

откъдето получаваме исканото сравнение.

7. Покажете, че ако $100a+10b+c\equiv 0 \pmod{21}$, то

$$a-2b+4c\equiv 0 \pmod{21}.$$

Решение. Като съберем очевидните сравнения

$$400\,a\equiv a \pmod{21},$$
$$40\,b\equiv -2b \pmod{21},$$
$$4c\equiv 4c \pmod{21},$$

получаваме

$$400a+40b+4c\equiv a-2b+4c \pmod{21}.$$

8. Нека p е просто число, а a и b са произволни цели числа. Докажете, че

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Решение. Тъй като

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \ldots + \binom{p}{p-1} ab^{p-1} + b^p,$$

то за да решим задачата, е достатъчно да покажем, че всеки от биномните коефициенти $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ се дели на p. Наистина числото $\binom{p}{k}$ $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1\ 2\ldots k}$ е цяло и тъй като p е просто и $p>k$, то p не се съкращава с никой от множителите на знаменателя. Следователно $\binom{p}{k} = pm$.

9. Като използувате резултата от предната задача, докажете теоремата на Ферма—Ойлер:

Ако a е произволно число и числото p е просто, то

$$a^p \equiv a \pmod{p}.$$

Упътване. В сравнението

$$(h_1+h_2+\ldots+h_a)^p \equiv h_1^p + h_2^p + \ldots + h_a^p$$

положете $h_1 = h_2 = \ldots = h_a = 1$.

10. Нека p е просто число, а a и b са произволни цели числа. Докажете, че ако $a \equiv b \pmod{p^n}$, то $a^p \equiv b^p \pmod{p^{n+1}}$.

11. Докажете, че ако p е просто число, то

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Решение. Като умножим очевидните сравнения

$$\left.\begin{array}{r} p-1\equiv -1 \\ p-2\equiv -2 \\ p-3\equiv -3 \\ \cdots\cdots \\ p-k\equiv -k \end{array}\right\} \pmod{p},$$

получаваме

$$(p-1)(p-2)\ldots(p-k) \equiv (-1)^k\, 1 . 2 \ldots k \pmod{p}.$$

Тъй като $(1 . 2 \ldots k, p) = 1$, то като разделим двете страни на последното сравнение с $1 . 2 \ldots k$, ще имаме $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$.

12. Покажете, че ако m е произволно нечетно естествено число, то $(m-1)! \equiv (-1)^{\frac{m-1}{2}} \left[\left(\frac{m-1}{2}\right)!\right]^2 \pmod{m}$.

13. Докажете, че уравнението

$$x^3+y^3+z^3=5$$

няма решение в цели числа.

Упътване. Използувайте, че ако a е произволно цяло число, то остатъкът от делението на a^3 с 9 е 0 или ± 1.

14. Докажете, че уравнението

$$5x^2-7y^2=1$$

няма решения в цели числа.

15. Докажете, че ако p е нечетно просто число и

$$x^p+y^p\equiv 0 \pmod{p}, \text{ то } x^p+y^p\equiv 0 \pmod{p^2}.$$

Упътване. Използувайте, че $x^p+y^p\equiv x+y \pmod{p}$ (вж. зад. 9).

16. Докажете, че ако нечетното просто число p не дели цялото число a, уравнението

$$x^p+y^p=p\,.\,a$$

няма решение в цели числа.

17. Покажете, че числата 24, 18, —19, 37, 28, —23, —32, 5, 41, —35, —33 образуват пълна система остатъци по модул 11.

18. Покажете, че числата 11, —1, 17, —19 образуват приведена (редуцирана) система остатъци по модул 8.

19. Като използувате теоремата на Ферма—Ойлер, намерете остатъка при делението на числото a с числото b, където:

а) $a=387^{175}$, $b=45$; б) $a=439^{291}$, $b=60$;

в) $a=(12\,371^{76}+34)^{150}$, $b=111$; г) $a=3.5^{75}+4,7^{100}$, $b=132$.

Отг. а) 32; б) 19; в) 84; г) 7

20. Докажете, че

$$2^{1092}\equiv 1 \pmod{1093^2}.$$

Решение. Ще използуваме сравнението $3^{11}\equiv 4p+1 \pmod{p^2}$, $p=1093$, което следва от равенствата:

$$3^7=2187=2\,.\,1093+1=2p+1,$$

$$3^{11}=4p^2+4p+1$$

и факта, че в сравнения от вида $c\equiv ap+b \pmod{p^2}$ можем да заменим коефициента a с кое да е число, сравнимо с a по модул p. Получаваме последователно

$$2^{14}=16\,384=15\,p-11,$$

$$2^{28}\equiv -330p+121 \pmod{p^2},$$

$$3^2\,.\,2^{28}\equiv -2970p+1089\equiv -2969p-4\equiv 310p-4 \pmod{p^2},$$

$$3^2\,.\,2^{28}\,.\,7\equiv 2170p-28\equiv -16p-28 \pmod{p^2},$$

$$3^2\,.\,2^{26}\,.\,7\equiv -4p-7 \pmod{p^2},$$

$$3^{14}\cdot 2^{182}\cdot 7^7\equiv-(4p+7)^7\equiv-7\cdot 4p\cdot 7^6-7^7 \pmod{p^2},$$

или

$$3^{14}\cdot 2^{182}\equiv-4p-1 \pmod{p^2}.$$

Тъй като $3^{14}\equiv 4p+1 \pmod{p^2}$, последното сравнение може да се запише във вида

$$3^{14}\cdot 2^{182}\equiv-3^{14} \pmod{1093^2},$$

или

$$2^{182}\equiv-1 \pmod{1093^2},$$

откъдето получаваме исканото сравнение.

21. Докажете, че

$$10^{486}\equiv 1 \pmod{487^2}.$$

22. Докажете, че произведение на три последователни цели числа, от които средното е куб на цяло число, се дели на 504.

23. Докажете, че ако простото число p не дели числото a и $a^p\equiv\pm 1 \pmod p$, то $a^p\equiv\pm 1 \pmod{p^2}$.

Решение. Нека например $a^p\equiv 1 \pmod p$.

$$a^p-1=(a-1)(a^{p-1}+a^{p-2}+\dots+a+1)\equiv 0 \pmod p.$$

Съгласно теоремата на Ферма ще имаме

$$a^p-1\equiv a-1 \pmod p,$$

т. е. $a-1\equiv 0 \pmod p$. От последното сравнение получаваме

$$\left.\begin{aligned} a^{p-1}&\equiv 1\\ a^{p-2}&\equiv 1\\ &\dots\\ a&\equiv 1\\ 1&\equiv 1\end{aligned}\right\} \pmod p.$$

Като съберем тези сравнения, ще имаме

$$a^{p-1}+a^{p-2}+\dots+a+1\equiv p\equiv 0 \pmod p$$

и следователно $a^p-1\equiv 0 \pmod{p^2}$.

Аналогично се разглежда случаят $a^p\equiv-1 \pmod p$.

24. Нека p и q са различни прости числа. Докажете, че

$$p^{q-1}+q^{p-1}\equiv 1 \pmod{pq}.$$

25. Нека m е нечетно число, по-голямо от 1. Докажете, че остатъкът от делението на $2^{\varphi(m)-1}$ с m е равен на $m-\left[\frac{m}{2}\right]$.

26. Нека m е нечетно число, по-голямо от 1. Намерете остатъка от делението на числото $4^{\varphi(m)-1}$ с m.

Отг. $m-\left[\frac{m}{4}\right]$.

27. Нека $a_1, a_2, \ldots, a_n$ се естествени числа. Докажете, че ако числото $N=a_1+a_2+\ldots+a_n$ се дели на 30, то числото

$$M=a_1^5+a_2^5+\ldots+a_n^5$$

също се дели на 30.

28. Докажете, че ако $x^2+y^2\equiv 0 \pmod{21}$, то

$$x^2+y^2\equiv 0 \pmod{441}.$$

Упътване. Покажете, че всяко от числата x и y се дели както на 3, така и на 7.

29. Нека $p>2$ е просто число, а m е произволно естествено число. Докажете, че

$$1^m+2^m+3^m+\ldots+(p-1)^m\equiv\begin{cases}-1 \pmod{p}, & \text{ако } m \text{ се дели от } p-1,\\ 0 & \text{ако } m \text{ не се дели от } p-1.\end{cases}$$

30. Докажете, че ако a е цяло число, взаимно просто с 10, то за всяко естествено число n е в сила сравнението

$$a^{100n+1}\equiv a \pmod{1000}.$$

Упътване. Използувайте, че $(a, 2)=1$, $(a, 5)=1$ и $1000=2^3 . 5^3$.

31. Нека a е нечетно число, което не се дели на 5, и n е произволно естествено число. Покажете, че

$$a^{20n+1}\equiv a \pmod{100}.$$

32. Покажете, че ако a е число, взаимно просто с 546, то $a^{12}\equiv 1 \pmod{4368}$.

33. Нека a е цяло число, такова, че

$$a^7\not\equiv a \pmod{13}.$$

Докажете, че

$$a^{78}+1\equiv 0 \pmod{169}.$$

34. Нека числото $p=4\lambda+1$ е просто. Покажете, че $\lambda^{2\lambda}\equiv 1 \pmod{p}$.

35. Нека a е четно число, което не се дели на 10, и n е произволно естествено число. Докажете, че числото a^{20n} окончава на 76.

Решение. Съгласно условието на задачата имаме $a=2^\lambda q$, където $\lambda\geq 1$, $(q,10)=1$. С r да означим остатъка от делението на a^{20n} със 100. Ще покажем, че $r=76$. И наистина

$$a^{20n}\equiv r \pmod{100}$$

или още

(1) $$2^{20\lambda n}q^{20n}\equiv r \pmod{100}.$$

Но $(q, 100)=1$ и следователно

$$q^{\varphi(4)}=q^2\equiv 1 \pmod 4 \text{ и } q^{\varphi(25)}=q^{20}\equiv 1 \pmod{25}, \text{ т. е. } q^{20}\equiv 1 \pmod{100}.$$

Като вземем пред вид последното сравнение, (1) приема вида

$$2^{20\lambda n}\equiv r \pmod{100},$$

откъдето следва

$$2^{20in} \equiv r \pmod{25}.$$

От друга страна, $2^{\varphi(25)}=2^{20}\equiv 1 \pmod{25}$. Следователно $r\equiv 1 \pmod{25}$, т. е. $r=1+25k$.

Тъй като r е число, по-малко от 100, и съгласно (1) се дели на 4, то $r=76$.

36. Нека a е цяло число, взаимно просто с 35. Покажете, че

$$(a^4-1)(a^4+15a^2+1)\equiv 0 \pmod{35}.$$

37. Нека n е естествено число, което не се дели на 3. Докажете, че

$$1+2^n+2^{2n}\equiv 0 \pmod{7}.$$

38. Нека n е цяло неотрицателно число. Докажете, че

$$5^{2^n}\equiv 1 \pmod{2^{n+2}}.$$

39. Нека $a\neq 0$ е цяло число, което не се дели на 5. Докажете, че

$$a^{8n}+3a^{4n}\equiv 4 \pmod{100}.$$

Упътване. Използувайте тъждеството

$$a^{8n}+3a^{4n}-4=(a^{4n}-1)(a^{4n}+4).$$

40. Нека n е естествено число, което не се дели на 3. Докажете, че

$$n^{13}-n\equiv 0 \pmod{(2^{13}-2)}.$$

41. Проверете сравненията:

а) $2^{19.73}\equiv 2 \pmod{19.73}$;

б) $2^{37.73}\equiv 2 \pmod{37.73}$.

42. Нека p е просто число. Покажете, че числото $\dfrac{2^{p-1}-1}{p}$ е точен квадрат на цяло число само при $p=3$ и $p=7$.

Решение. Очевидно простото число 2 не удовлетворява условието на задачата. Нека $p>2$. Да положим

$$p=2q+1,\ 2^{p-1}-1=p\,.\,x^2.$$

Оттук следва, че

(1) $$(2^q-1)(2^q+1)=px^2.$$

Тъй като

$$(2^q-1)+2^q+1=2^{q+1},$$

то числата 2^q-1, 2^q+1 са взаимно прости. Следователно единият от множителите в (1) е точен квадрат, а другият е произведение на точен квадрат с числото p, т. е. $2^q=y^2\pm 1$.

Да разгледаме случая $2^q=y^2+1$. Ако $q=1$, то получаваме $y=1$, $p=3$. При $q>1$ равенството $2^q=y^2+1$ е невъзможно, тъй като лявата му страна се дели на 4, а дясната е сравнима с 2 по модул 4.

Нека сега $2^q=y^2-1$. Тъй като числата $y-1$ и $y+1$ имат общ множител само числото 2, то от равенството

$$2^q=(y-1)(y+1)$$

получаваме

$$y-1=2,\quad y+1=2^{q-1},$$

т. е. $y=3$, $q=3$, $p=7$.

43. Намерете всички прости числа p, за които е в сила сравнението

$$5^{p^2}+1\equiv 0 \pmod{p^2}.$$

Решение. Очевидно $p\neq 5$. Тогава

(1) $$5^{\varphi(p^2)}=5^{p^2-p}\equiv 1 \pmod{p^2}.$$

Като вземем пред вид това сравнение, за лявата страна на (1) имаме

$$5^{p^2}+1=5^{p^2-p}\,.\,5^p+1\equiv 5^p+1 \pmod{p^2}.$$

По такъв начин задачата се свежда до намиране на всички прости числа p, за които

(2) $$5^p+1\equiv 0 \pmod{p^2}.$$

Но ако за някое просто p е в сила сравнението (2), то

$$5^p+1\equiv 0 \pmod{p}$$

или още $5+1\equiv 0 \pmod{p}$, откъдето получаваме $p=2$ или $p=3$. С непосредствена проверка се убеждаваме, че при $p=2$ сравнението (2) не е в сила, а при $p=3$ това сравнение е изпълнено.

44. Нека числото $p=4\lambda-1$ е просто и k е цяло число, за което $2k-1$ не се дели на p. Докажете, че

$$[\lambda+k(k-1)]^{2\lambda-1}\equiv 1 \pmod{p}.$$

Решение. По модул p имаме

$$4\lambda\equiv 1 \text{ и } 4k^2-4k\equiv(2k-1)^2-1,$$

откъдето получаваме сравнението

$$4[\lambda+k(k-1)]\equiv(2k-1)^2.$$

Оттук, като повдигнем двете страни на това сравнение в степен $2\lambda-1=\frac{p-1}{2}$, ще имаме

$$2^{p-1}[\lambda+k(k-1)]^{2\lambda-1}\equiv(2k-1)^{p-1},$$

т. е.

$$[\lambda+k(k-1)]^{2\lambda-1}\equiv 1 \pmod{p},$$

което трябваше да докажем.

45. Нека числото $p=4n+1$ е просто. Докажете, че

$$(2n!)^2+1\equiv 0 \pmod{p}.$$

Упътване. Използувайте зад. 12 и теоремата на Уилсън.

46. Докажете, че числата p и $p+2$ са едновременно прост- (т. е. прости числа „близнаци") тогава и само тогава, когато

$$4[(p-1)!+1]+p \equiv 0 \pmod{p(p+2)}.$$

Решение. Съгласно теоремата на Уилсън

$$(p-1)!+1 \equiv 0 \pmod{p}.$$

Като умножим двете страни на това сравнение с 4 и прибавим към лявата му страна p, получаваме

(1) $$4[(p-1)!+1]+p \equiv 0 \pmod{p}.$$

Като умножим двете части на сравнението $p \equiv -2 \pmod{p+2}$ с $p+1$, ще имаме

$$p(p+1) \equiv -2(p+1) = -2[(p+2)-1] \equiv -2(p+2)+2 \equiv 2 \pmod{p+2},$$

т. е.

$$p(p+1) \equiv 2 \pmod{p+2}.$$

От последното сравнение получаваме

$$(p-1)!\,p(p+1).2 \equiv 4\,[(p-1)!] \pmod{p+2}$$

или

$$(p+1)!.2 \equiv 4\,[(p-1)!] \pmod{p+2}.$$

Като прибавим към двете части на последното сравнение $4+p$, ще имаме

$$(p+1)!\,2+2+(p+2) \equiv 4\,[(p-1)!]+4+p \pmod{p+2},$$

т. е.

(2) $$2[(p+1)!+1]+(p+2) \equiv 4[(p-1)!]+4+p \pmod{p+2}.$$

Ако $p+2$ е просто, то използувайки теоремата на Уилсън, за лявата част на (2) ще имаме

(3) $$2[(p+1)!+1]+(p+2) \equiv 2 \pmod{p+2}.$$

От (2) и (3) получаваме

(4) $$4[(p-1)!+1]+p \equiv 0 \pmod{p+2}$$

и като вземем пред вид (1), ще имаме

(5) $$4[(p-1)!+1]+p \equiv 0 \pmod{p\,(p+2)}.$$

Обратно, от (5) и (1) следва (4), откъдето, като вземем пред вид (2), получаваме

$$(p+1)!+1 \equiv 0 \pmod{p+2}.$$

Съгласно теоремата на Уилсън това означава, че числото $p+2$ е просто.

47. Докажете, че ако простото число p е по-голямо от 5, то равенството

$$(p-1)!+1=p^m$$

не е възможно за никое естествено число m.

Решение. За всяко просто число $p>5$ ще имаме

$$2<\frac{p-1}{2}<p-1,$$

откъдето получаваме, че числото $(p-1)^2=2\frac{p-1}{2}(p-1)$ дели $(p-1)!$. Да допуснем, че за някое просто число $p>5$ е в сила равенството

(1) $$(p-1)!+1=p^m.$$

Тогава числото $(p-1)^2$ дели p^m-1. Оттук следва, че числото $p-1$ дели $p^{m-1}+$ $+p^{m-2}+\ldots+p+1$. Тъй като $p^k\equiv 1 \pmod{p-1}$ за $k=0, 1, 2, \ldots$, то

$$p^{m-1}+p^{m-2}+\ldots+p+1\equiv m \pmod{p-1}.$$

Следователно $p-1$ дели m, т. е. $m\geq p-1$. Тогава

$$p^m\geq p^{p-1}>(p-1)^{p-1}>(p-1)!;\ p^m>(p-1)!+1,$$

което противоречи на допускането, че е в сила равенството (1).

48. Нека p и q са прости числа и x е такова цяло число, за което p дели $\sum\limits_{k=0}^{q^r-1} x^k$ за някое естествено число r. Докажете, че $p=q$ или q дели $p-1$.

Решение. Нека $p\neq q$. Тогава $x\not\equiv 1 \pmod p$. Тъй като p дели $\sum\limits_{k=0}^{q^r-1} x^k=\frac{x^q-1}{x-1}$, то $x^{q^r}\equiv 1 \pmod p$. От друга страна, съгласно теоремата на Ферма имаме $x^{p-1}\equiv 1 \pmod p$. Да означим с d най-малкото естествено число, за което $x^d\equiv 1 \pmod p$. (Съгласно теоремата на Ферма такова число d съществува.) Лесно се вижда, че d дели q^r и $p-1$. Следователно $d=q^s$, q^s дели $p-1$, т. е. q дели $p-1$.

49. Решете сравненията от първа степен:

а) $4x\equiv -3 \pmod{17}$;
б) $29x+3\equiv 0 \pmod{12}$;
в) $3x-8\equiv 0 \pmod{13}$;
г) $7x\equiv 4 \pmod{19}$;
д) $37x\equiv 25 \pmod{117}$;
е) $13x\equiv 178 \pmod{153}$;
ж) $18x\equiv 5 \pmod{51}$;
з) $10x\equiv 25 \pmod{35}$;
и) $39x\equiv 84 \pmod{93}$;
к) $117x\equiv 42 \pmod{87}$.

Отг. а) $x\equiv 12 \pmod{17}$;
б) $x\equiv 9 \pmod{12}$;
в) $x\equiv 7 \pmod{13}$;
г) $x\equiv 6 \pmod{19}$;
д) $x\equiv 7 \pmod{117}$;
е) $x\equiv 49 \pmod{153}$;
ж) няма решение;
з) $x\equiv 6, 13, 20, 27, 34 \pmod{35}$;
и) $x\equiv 26, 57, 88 \pmod{31}$;
к) $x\equiv 13, 52, 81 \pmod{87}$.

50. Към числото 423 припишете вдясно три цифри така, че новополученото шестзначно число да се дели на 7, 8, и 9.

Решение. Нека $\overline{423abc}$ е полученото шестзначно число и да означим с x числото $x=\overline{abc}$. Ще имаме

$$423.10^3+x\equiv 0 \pmod{7\,.\,8\,.\,9},$$

или още

$$423\,000+x\equiv 0 \pmod{504}.$$

От последното сравнение получаваме

$$x\equiv 360 \pmod{504},$$

откъдето $x=360+504k$. Ясно е, че числото x е трицифрено само при $k=0$ и $k=1$. Следователно $x=360$ и $x=864$.

51. Към числото 32 припишете вляво две цифри така, че полученото четиризначно число да се дели на 3 и 7.

Отг. 19, 40, 61, 82.

52. Нека $(a, m)=1$. Покажете, че числото $ba^{\varphi(m)-1}$ е решение на сравнението

$$ax \equiv b \pmod{m}.$$

53. Решете системата уравнения

$$\begin{cases} 3x \equiv 1 \pmod{7} \\ 4x \equiv 5 \pmod{11}. \\ 2x \equiv 3 \pmod{5} \end{cases}$$

Решение. Дадената система може да се запише във вида

$$(1) \qquad \begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 4 \pmod{11}. \\ x \equiv 4 \pmod{5} \end{cases}$$

От първото сравнение на (1) имаме $x=5+7y$. Така намереното x заместваме във второто сравнение на (1). Получаваме

$$5+7y \equiv 4 \pmod{11},$$

откъдето намираме $y \equiv 3 \pmod{11}$, т. е. $y=3+11z$. За x ще имаме

$$x=5+7y=5+7(3+11z)=26+77z.$$

Последната стойност на x заместваме в третото сравнение на системата (1). Получаваме

$$26+77z \equiv 4 \pmod{5},$$

откъдето намираме $z \equiv 4 \pmod{5}$, т. е. $z=4+5t$. Тогава за x ще имаме

$$x=26+77z=26+77(4+5t)=334+385t,$$

или още $x \equiv 334 \pmod{385}$. Очевидно най-малкото положително решение на дадената система е $x=334$.

54. Решете системата

$$\begin{cases} 3x \equiv 7 \pmod{10} \\ 2x \equiv 5 \pmod{15}. \\ 7x \equiv 5 \pmod{12} \end{cases}$$

Решение. Дадената система може да се запише във вида

$$(1) \qquad \begin{cases} x \equiv 9 \pmod{10} \\ x \equiv 10 \pmod{15}. \\ x \equiv 11 \pmod{12} \end{cases}$$

От първото сравнение на (1) имаме $x=9+10y$. Така намереното x заместваме във второто сравнение на (1). Получаваме

$$(2) \qquad 9+10y \equiv 10 \pmod{15}.$$

Тъй като $(10, 15)=5$ и числото 1 не се дели на 5, то сравнението (2) няма решение. Оттук следва, че дадената система също няма решение.

55. Решете системата:

а) $\begin{cases}5x+1\equiv 0 \pmod{24}\\ 4x\equiv 19 \pmod{21};\end{cases}$ б) $\begin{cases}3x+1\equiv 0 \pmod{35}\\ 7x\equiv 11 \pmod{20};\end{cases}$

в) $\begin{cases}4x\equiv 1 \pmod{9}\\ 5x\equiv 3 \pmod{7}\\ 4x\equiv 5 \pmod{12};\end{cases}$ г) $\begin{cases}5x\equiv 1 \pmod{12}\\ 5x\equiv 2 \pmod{8};\\ 7x\equiv 3 \pmod{11}\end{cases}$

д) $\begin{cases}3x\equiv 1 \pmod{10}\\ 4x\equiv 3 \pmod{5};\\ 2x\equiv 7 \pmod{9}\end{cases}$ е) $\begin{cases}2x+3\equiv 0 \pmod{15}\\ 4x-9\equiv 0 \pmod{21};\\ 5x-3\equiv 0 \pmod{12}\end{cases}$

ж) $\begin{cases}2x\equiv 7 \pmod{13}\\ 5x\equiv 8 \pmod{17}\\ 3x\equiv 7 \pmod{31};\\ 14x\equiv 35 \pmod{19}\end{cases}$ з) $\begin{cases}4x\equiv 7 \pmod{13}\\ x\equiv 2 \pmod{17}\\ 5x\equiv 3 \pmod{9};\\ 8x\equiv 4 \pmod{14}\end{cases}$

Отг. а) $x\equiv 115 \pmod{168}$, б) $x\equiv 90 \pmod{140}$;
в) няма решение; г) няма решение;
д) $x\equiv 17 \pmod{90}$; е) $x\equiv 291 \pmod{420}$;
ж) $x\equiv 85\,056 \pmod{130\,169}$; з) $x\equiv 9573 \pmod{13\,923}$

56. Намерете най-малкото естествено число, което при деление на 7, 5, 3, 11 дава остатъци съответно равни на 3, 2, 1, 9.

Отг. 262

57. Намерете стойностите на париметъра a, при които системите сравнения са съвместими:

а) $\begin{cases}x\equiv 5 \pmod{18}\\ x\equiv 8 \pmod{21};\\ x\equiv a \pmod{35}\end{cases}$ б) $\begin{cases}x\equiv 3 \pmod{11}\\ x\equiv 11 \pmod{20}.\\ x\equiv 1 \pmod{15}\\ x\equiv a \pmod{18}\end{cases}$

Отг: а) $a\equiv 1 \pmod{7}$; б) $a\equiv 1 \pmod{6}$

58. Решете системата сравнения

$$\begin{cases}x\equiv 3 \pmod{7}\\ x^2\equiv 44 \pmod{7^2}.\\ x^3\equiv 111 \pmod{7^3}\end{cases}$$

Отг. $x\equiv 17 \pmod{7^3}$.

59. Намерете цифрите x и y така, че шестзначното число $4x87y6$ да се дели на 56.

Отг. $x=2$, $y=3$; $x=9$, $y=3$; $x=6$, $y=7$.

60. Намерете цифрите x, y и z в шестзначното число $xyz\,138$ така, че то да се дели на 7, а числото $138\,xyz$ при деление с 13 да дава остатък 6 и числото $x1y3z8$ при деление с 11 да дава остатък 5.

Отг. $x=3$, $y=1$, $z=3$; $x=4$, $y=9$, $z=5$.

61. Намерете цифрите x, y и z в седемзначното число $13xy45z$ така, че то да се дели на 792.

Отг. $x=8$, $y=0$, $z=6$.

ГЛАВА VII

ПРЪСТЕНИ И ПОЛЕТА

§ 1. ОСНОВНИ ОПРЕДЕЛЕНИЯ И ПРИМЕРИ

Определение. Нека R е множество, в което са дефинирани две операции, наречени събиране и умножение. Ще казваме, че множеството R *е пръстен* (по отношение на горните две операции), когато са в сила следните аксиоми:

1. $a+b=b+a$ (комутативен закон за събирането);
2. $a+(b+c)=(a+b)+c$ (асоциативен закон за събирането);
3. съществува елемент $o\in R$ (нулев елемент), такъв, че $a+o=a$ за всяко $a\in R$;
4. за всеки елемент a съществува елемент $-a\in R$ (противоположен на a), такъв, че $a+(-a)=0$;
5. $a(bc)=(ab)c$ (асоциативен закон за умножението);
6. $a(b+c)=ab+ac$

(дистрибутивни закони).

$(b+c)a=ba+ca$

Непосредствени следствия от определението за престен:

а) нулевият елемент 0 е единствен;

б) противоположният елемент $-a$ на елемента a е еднозначно определен чрез a;

в) $a(b-c)=ab-ac$, $(b-c)\,a=ba-ca$,

където под разлика $b-c$ се разбира елементът $b+(-c)$;

г) $a.0=0.a=0$ за всяко $a\in R$;

д) $(-a)b=a(-b)=-ab$;

е) $(-a)(-b)=ab$.

Приети са следните означения: ако n е произволно естествено число, то

$$na=\underbrace{a+a+\ldots+a}_{n \text{ пъти}},\quad (-n)a=n(-a)=-na.$$

В сила са равенствата

$$na+ma=(n+m)a,\quad na.ma=nma$$

за произволен елемент $a\in R$ и произволни цели числа m и n.

Определение. Ако е в сила комутативният закон за умножението, т. е. $ab=ba$ за всеки два елемента a, b от R, пръстенът се нарича *комутативен*.

Примери.

а) Множеството Z на целите числа е комутативен пръстен относно обичайните действия събиране и умножение.

б) Множеството $2Z$ от всички четни числа е комутативен пръстен относно обичайните действия събиране и умножение.

в) Множеството на числата от вида $a+b\sqrt{2}$, където $a, b \in Z$, е комутативен пръстен относно обичайните действия събиране и умножение.

Изобщо всяко множество от числа, затворено относно действията събиране, изваждане и умножение, представлява комутативен пръстен. Такива пръстени се наричат числови.

г) Множеството на квадратните матрици от n-ти ред е некомутативен пръстен относно обичайните действия събиране и умножение на матрици.

д) Множеството Z_n на класовете остатъци по модул n е краен пръстен с n елемента относно въведените в предишната глава операции събиране и умножение на класове.

Определение. Пръстенът R се нарича *пръстен с делители на нулата*, когато съществуват два ненулеви елемента a, b от R, така че $ab=0$. Елементите a и b с това свойство се наричат делители на нулата. Ако от равенството $ab=0$ следва $a=0$ или $b=0$, пръстенът се нарича *пръстен без делители на нулата*.

Например всеки числов пръстен е пръстен без делители на нулата.

Напротив, от равенството

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

се вижда, че пръстенът на квадратните матрици от втори ред е пръстен с делители на нулата.

Определение. Елементът e от пръстена R се нарича *единичен елемент* (*единица*) на R, когато за всеки елемент $a \in R$ имаме $ae=ea=a$.

Лесно се вижда, че ако R има единица, тя е единствена.

Например пръстенът Z на целите числа е пръстен с единица, докато пръстенът $2Z$ на четните числа няма единица.

Определение. Комутативен пръстен без делители на нулата се нарича *област на цялостност.*

Например всеки числов пръстен е област на цялостност.

Определение. Пръстен, в който операцията умножение е обратима, т. е. уравненията

$$ax=b, \quad ya=b$$

имат единствени решения при всяко $a \neq 0$ и всяко b, се нарича *тяло.*

Определение. Тяло, в което е в сила комутативният закон за умножението, се нарича *поле.*

Например пръстените Q, D и C съответно на рационалните, реалните и комплексните числа са полета. Също така пръстените Z_p, където p е просто число, са полета. Примери за некомутативни тела се построяват по-трудно и ще бъдат изложени в някои от следващите задачи.

Всяко поле притежава еднозначно определен единичен елемент e и за всеки ненулев елемент a от полето съществува еднозначно определен обратен елемент a^{-1} със свойството $aa^{-1}=e$. За краткост единичния елемент e ще означаваме с 1.

Лесно се вижда, че всяко поле е област на цялостност.

Определение. Казваме, че полето P е с *характеристика* 0, когато $p.1 \neq 0$ при всяко естествено число p. Ако съществува естествено число p, такова че $p.1=0$, ще казваме, че полето е с характеристика $\neq 0$. В този случай най-малкото естествено число p, за което $p.1=0$, се нарича *характеристика* на полето. Характеристиката p е просто число.

Характеристиката на всяко числово поле е равна на нула. Всяко крайно поле има характеристика различна от нула. За всяко просто число p съществуват както крайни, така и безкрайни полета с характеристика p.

Ако P е поле с характеристика $p \neq 0$, то за всеки елемент $a \in P$ е в сила равенството $pa=0$.

Ако P е поле с характеристика $p \neq 0$ и n е цяло число, за което $n.1=0$, то p дели n.

Определение. Пръстените R и R' се наричат *изоморфни*, когато между елементите им може да се установи взаимно еднозначно съответствие, такова че

$$(a+b)'=a'+b',$$
$$(ab)'=a'b',$$

където $x' \in R'$ означава образа на елемента $x \in R$ при това съответствие.

Например множеството на линейните оператори, действуващи в n-мерно линейно пространство, е пръстен относно обичайните действия събиране и умножение на оператори, който е изоморфен с пръстена на квадратните матрици от n-ти ред.

Определение. Всеки изоморфизъм на пръстена R върху себе си се нарича *автоморфизъм* на пръстена R.

Например съответствието, при което на всяко комплексно число съпоставяме спрегнатото му, е автоморфизъм на полето на комплексните числа.

1. Проверете кои от следните числови множества са пръстени и кои полета:

а) множеството от всички цели числа, кратни на дадено естествено число n;

б) множеството на числата от вида $a+b\sqrt{3}$, където a, b са цели числа;

в) множеството на числата от вида $a+b\sqrt{5}$, където a, b са рационални числа;

г) множеството на комплексните числа от вида $a+bi$, където a, b са цели числа;

д) множеството на числата от вида $a+b\sqrt{d}$, където d е фиксирано цяло число, а a, b са цели (съответно рационални) числа. Кога това множество съвпада с пръстена на целите числа (съответно с полето на рационалните числа)?

е) множеството на числата от вида $\frac{a}{2}+\frac{b}{2}\sqrt{d}$, където d е фиксирано цяло число, такова че $d\equiv 1 \pmod 4$, а a, b са произволни цели числа, удовлетворяващи сравнението $a\equiv b \pmod 2$;

ж) множеството на числата от вида $a+b\sqrt[3]{2}$, където a, b са произволни рационални числа.

2. Покажете, че числата от вида $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, където a, b, c са рационални числа, образуват поле. Намерете обратния елемент на числото $1-\sqrt[3]{2}+2\sqrt[3]{4}$.

Отг. $\frac{1}{43}\left(5+9\sqrt[3]{2}-\sqrt[3]{4}\right)$.

3. Покажете, че числата от вида $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, където a, b, c и d са рационални числа, образуват поле. Покажете също, че всяко число от указания вид може да се запише във вида $x+y\theta+z\theta^2+t\theta^3$, където x, y, z, t са рационални, а $\theta=\sqrt{2}+\sqrt{3}$.

4. Покажете, че всички квадратни матрици от вида $\begin{pmatrix} a & b \\ db & a \end{pmatrix}$, където a, b са рационални числа, а d е цяло число, което не е точен квадрат, образуват поле относно обичайните действия събиране и умножение на матрици. Покажете също, че това поле е изоморфно с полето от зад. 1, д).

5. Покажете, че матриците от вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, където a, b са реални числа, образуват поле, изоморфно на полето на комплексните числа.

6. Покажете, че матриците от вида $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$, където a, b, c, d са реални числа, образуват некомутативно тяло.

7. Покажете, че множеството на квадратните матрици от вида:

$$\text{а)}\ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ 0 & 0 & \dots & a_{nn} \end{pmatrix};\ \text{б)}\ \begin{pmatrix} 0 & a_{12} & \dots & a_{1,\,n-1} & a_{1n} \\ 0 & 0 & \dots & a_{2,\,n-1} & a_{2n} \\ . & . & . & . & . \\ 0 & 0 & \dots & 0 & a_{n-1,\,n} \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

образуват подпръстен на пръстена от всички квадратни матрици от ред n.

8. Докажете, че една матрица A е делител на нулата в пръстена на квадратните матрици от n-ти ред тогава и само тогава, когато е особена, т. е. когато детерминантата на A е равна на нула.

9. Нека M е множеството от всички наредени двойки (c, b), където a, b са елементи на пръстена R. В M дефинираме операции събиране и умножение чрез равенствата

$$(a, b)+(c, d)=(a+c, b+d),$$
$$(a, b)(c, d)=(ac, bd).$$

Покажете, че относно тези операции M е пръстен с делители на нулата. Намерете всички делители на нулата в M, в случай че R е пръстенът на целите числа.

10. Покажете, че множеството на всички непрекъснати в интервала $[a, b]$ функции е пръстен относно обичайните операции събиране и умножение на функции. Има ли делители на нулата в този пръстен?

11. Покажете, че множеството от тригонометрични полиноми от вида $a_0+\sum_{k=1}^{n}(a_k\cos kx+b_k\sin kx)$ с реални коефициенти е пръстен. Образуват ли пръстен полиномите от вида $a_0+\sum_{k=1}^{n} a_k\cos kx$ или от вида $\sum_{k=1}^{n} b_k \sin kx$?

12. Проверете, че множеството $\{a, b, c, d\}$ със събиране и умножение, дефинирани чрез таблиците

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

е пръстен. Пресметнете $a^2+b^2+c^2+d^2$. [illegible] $= c$

13. Попълнете таблицата за умножение на пръстена $R=\{a, b, c, d\}$, където:

а)

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

.	a	б	c	d
a	a	a	a	a
b	a	b	.	.
c	a	.	.	a
d	a	b	c	.

;

б)

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

.	a	b	c	d
a	a	a	a	a
b	a	b	.	.
c	a	.	.	c
d	a	b	c	.

.

14. Проверете, че множеството $S=\{a, b, c, d, e, f, g, h\}$ е поле по отношение на операциите събиране и умножение, зададени с таблиците

+	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	d	c	f	e	h	g
c	c	d	a	b	g	h	e	f
d	d	c	b	a	h	g	f	e
e	e	f	g	h	a	b	c	d
f	f	e	h	g	b	a	d	c
g	g	h	e	f	c	d	a	b
h	h	g	f	e	d	c	b	a

;

.	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	b	c	d	e	f	g	h
c	a	c	h	f	g	e	b	d
d	a	d	f	g	c	b	h	e
e	a	e	g	c	d	h	f	b
f	a	f	e	b	h	c	d	g
g	a	g	b	h	f	d	e	c
h	a	h	d	e	b	g	c	f

.

15. Покажете, че всичките наредени двойки реални числа образуват поле по отношение на покомпонентното събиране

$$(a, b)+(c, d)=(a+c, b+d)$$

и умножение, дефинирано с равенството

$$(a, b)(c, d)=(ac-bd, ad+bc-bd),$$

Покажете още, че това поле е изоморфно с полето на комплексните числа.

Упътване. Постройте изоморфизъм, при който на имагинерната единица i съответствува елементът $\frac{1}{\sqrt{3}}(\omega-\omega^2)$, където $\omega=(0, 1)$.

16. Покажете, че пръстенът Z_n от остатъци по модул n е поле тогава и само тогава, когато n е просто число.

17. Нека p е просто число. Покажете, че полето Z_p има характеристика p.

18. Покажете, че всяко поле с характеристика 0 съдържа еднозначно определено подполе, изоморфно на полето Q на рационалните числа.

19. Покажете, че всяко поле с характеристика $p \neq 0$ съдържа еднозначно определено подполе, изоморфно с полето Z_p.

20. Решете системата уравнения

$$\begin{cases} x+2y=1 \\ y+2z=2 \\ 2x+z=1 \end{cases}$$

във всяко едно от полетата Z_3, Z_5, Z_7.

21. Решете системата уравнения

$$\begin{cases} x+3y+5z=1 \\ 3x+4y+2z=0 \\ 4x+y+z=3 \\ x+2y+2z=6 \end{cases}$$

във всяко едно от полетата Z_5, Z_7, Z_{11}.

22. Намерете стойностите на параметъра λ, при които системата

$$\begin{cases} \lambda x+y+z=1 \\ x+\lambda y+z=2 \\ x+y+\lambda z=3 \end{cases}$$

е съвместима в полето Z_7, и решете системата при тези λ.

23. Докажете, че всеки краен пръстен без делители на нулата е тяло.

Упътване. Използувайте обстоятелството, че ако $x \neq 0$ и $x_1, x_2, \ldots, x_n$ са всички елементи на пръстена, елементите $xx_1, xx_2, \ldots, xx_n$ $(x_1x, x_2x, \ldots, x_nx)$ са различни и следователно изчерпват всички елементи на пръстена.

24. Покажете, че ако P е поле с характеристика $p \neq 0$, за всяко $a \in P$ е в сила равенството $pa=0$. Ако за някое $a \in P$ и някое естествено число n е изпълнено равенството $na=0$, то p дели n.

25. Докажете, че ако P е поле с характеристика $p \neq 0$, за всеки два елемента $x, y \in P$ е в сила равенството

$$(x+y)^p=x^p+y^p.$$

По-общо, ако k е естествено число, то

$$(x+y)^{p^k}=x^{p^k}+y^{p^k}.$$

26. При предположенията от предната задача покажете, че от $x^p=y^p$ следва $x=y$.

27. Покажете, че ако P е крайно поле с характеристика $p \neq 0$, за всяко $a \in P$ уравнението $x^p=a$ има единствено решение в P.

Упътване. Нека $x_1, x_2, \ldots, x_n$ са всички елементи на P; тогава елементите x_1^p, $x_2^p, \ldots, x_n^p$ ще бъдат различни помежду си.

28. Нека P е крайно поле с n елемента. Покажете, че за всяко $x \in P$ е в сила равенството

$$x^n = x.$$

В частност, ако p е просто число и a е произволно цяло число, то

$$a^p \equiv a \pmod p \qquad \text{(теорема на Ферма).}$$

Решение. Нека $x \neq 0$ и $x_1, x_2, \ldots, x_{n-1}$ да означават всички ненулеви елементи на P; тогава елементите $xx_1, xx_2, \ldots, xx_{n-1}$ ще бъдат все различни и ще изчерпват всички ненулеви елементи на P. Оттук следва равенството $xx_1 \; xx_2 \ldots xx_{n-1} = x_1x_2 \ldots x_{n-1}$ или $x^{n-1} = 1$. Следователно $x^n = x$. Последното равенство очевидно е в сила и при $x = 0$. В частност за всяко $x \in Z_p$ имаме $x^p = x$.

29. Нека P е крайно поле с n елемента и $x_1, x_2, \ldots, x_{n-1}$ да означават всички ненулеви елементи на P. Докажете равенството

$$x_1x_2 \ldots x_{n-1} + 1 = 0.$$

В частност, ако p е просто число, в сила е сравнението

$$(p-1)! + 1 \equiv 0 \pmod p \; \text{(теорема на Уилсън).}$$

Упътване. Използувайте обстоятелството, че при всяко $x \neq 0$ и $x \neq \pm 1$ имаме $x \neq x^{-1}$. Следователно в произведението $x_1x_2 \ldots x_{n-1}$ от всички ненулеви елементи на полето P множителите, различни от ± 1, се съкращават два по два. Уточнете горното разсъждение за случая на поле с характеристика 2.

30. Нека R е краен комутативен пръстен с единица и k е броят на обратимите елементи на R. Докажете, че за всеки обратим елемент $x \in R$ е в сила равенството

$$x^k = 1.$$

В частност, ако цялото число a е взаимно просто с дадено естествено число n, то

$$a^{\varphi(n)} \equiv 1 \pmod n \; \text{(теорема на Ферма — Ойлер).}$$

Упътване. За доказателство на първото твърдение използувайте начина на разсъждение към решението на зад. 28. За второто твърдение използувайте факта, че класът $\bar{a}$ е обратим в пръстена Z_n тогава и само тогава, когато $(a, n) = 1$.

31. Докажете, че броят на елементите на всяко крайно поле е степен на характеристиката на полето.

Решение. Съгласно зад. 19 можем да считаме, че Z_p се съдържа в даденото поле P, където p е характеристиката на P. Ако $Z_p = P$, твърдението е доказано. Нека $x_1 \notin Z_p$. Разглеждаме множеството от всички елементи от вида $\alpha_0 + \alpha_1x_1$, α_0, $\alpha_1 \in Z_p$. Лесно се вижда, че броят на тези елементи е p^2. Ако те изчерпват цялото множество P, твърдението е доказано. В противен случай нека $x_2 \in P$ няма разглеждания вид. По-нататък да разгледаме множеството на всички елементи от вида $\alpha_0 + \alpha_1x_1 + \alpha_2x_2$, $\alpha_0, \alpha_1, \alpha_2 \in Z_p$, което се състои от p^3 на брой елемента. Ако това множество съвпада с P, твърдението е доказано. В противен случай, следвайки същия път на разсъждение, се убеждаваме, че винаги броят на елементите на крайното поле P има вида $n = p^k$.

Забележка. Както читателят може да се убеди от някои задачи в следващите параграфи, за всяко число от вида p^{λ}, p-просто, съществува поле с p^{λ} на брой елемента и всеки две такива полета с равен брой елементи са изоморфни. Следващите три задачи илюстрират горното твърдение в по-прости частни случаи.

32. Постройте поле с 4 елемента и покажете, че всеки две такива полета са изоморфни.

Упътване. С помощта на конструкцията от зад. 15, като разглеждате двойки от елементи на Z_2, дефинирайте събиране и умножение в множеството от всички наредени двойки (a, b), $a, b \in Z_2$. При доказателството на втората част от твърдението използвайте обстоятелството, че всяко поле с 4 елемента съдържа поле, изоморфно с Z_2. Пример за поле с 4 елемента се дава от следните таблици

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

33. Постройте поле с 25 елемента.

Упътване. Използвайте конструкцията за дефиниране на комплексни числа, като си служите с наредени двойки от елементи на Z_5.

34. За всяко просто число p постройте поле с p^2 елемента.

Упътване. Покажете, че съществува елемент $\alpha \in Z_p$, за който уравнението $x^2=\alpha$ няма решение в Z_p. Разгледайте множеството от всички наредени двойки (a, b) от елементи на Z_p и в това множество въведете събиране и умножение по формулите

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

35. Нека R е пръстен с единица. В R дефинираме операции $\oplus$ и $\odot$ по формулите

$$a\oplus b=a+b-1,$$
$$a\odot b=a+b-ab.$$

Покажете, че R е пръстен и по отношение на така дефинираните операции, изоморфен на първоначално зададения пръстен.

36. Нека a и b са два различни елемента от дадено поле P. В P дефинираме нови операции:

$$x\oplus y=x+y-a, \qquad x\odot y=a+\frac{(x-a)(y-a)}{b-a}.$$

Покажете, че относно тези операции множеството P е поле. Определете нулевия и единичния елемент в това поле.

37. Нека R е пръстен с единица. Докажете, че R е тяло тогава и само тогава, когато за всяко $a \in R$ с изключение на един елемент от R, уравнението $a+x=ax$ има решение.

38. Нека R е пръстен с единица и нека $x^2 \neq 0$ за всеки ненулев елемент $x \in R$. Докажете, че ако за всеки ненулев елемент $x \in R$ съществуват елементи $a, b \in R$, така че $axb=1$, то R е тяло.

39. Нека R е пръстен, такъв че за всяко $x \in R$ е в сила равенството $x^2 = x$. Докажете, че пръстенът R е комутативен и че за всяко $x \in R$ е в сила равенството $x + x = 0$.

40. Нека R е тяло, в което за всеки два елемента x, y е в сила равенството $x^2 y = y x^2$. Докажете, че R е поле.

41. Нека R е пръстен, в който за всеки два елемента x, y е в сила равенството $(x^2 - x)y = y(x^2 - x)$. Докажете, че пръстенът R е комутативен.

42. Нека R е краен пръстен, в който съществуват елементи a и b, такива че за всяко $x \in R$, $x \neq 0$ е в сила

$$xa \neq 0, \quad bx \neq 0.$$

Докажете, че пръстенът R притежава единичен елемент.

Решение. Съответствията $x \to xa$ и $x \to bx$ изобразяват R върху целия пръстен R. Оттук следва, че съществуват елементи e и f, така че

$$a = ea \text{ и } b = bf.$$

Тогава за всеки елемент $x \in R$ имаме

$$xa = xea \text{ и } bx = bfx,$$

откъдето $x = xe$ и $x = fx$. Следователно $e = fe$, $f = fe$, т. е. $e = f$.

43. Нека K е четиримерно линейно пространство над полето на реалните числа и e, i, j, k да означават произволен базис K. В K дефинираме умножение по такъв начин, че да са изпълнени равенствата $i^2 = j^2 = k^2 = -e$, $ij + ji = 0$, $ij = k$, а също така и дистрибутивните и асоциативните закони. Покажете, че K е тяло, изоморфно с тялото от зад. 6. Това тяло се нарича тяло на кватернионите.

§ 2. ИДЕАЛИ. ФАКТОР ПРЪСТЕНИ. ХОМОМОРФИЗМИ

Нека R е пръстен и I е непразно подмножество на R. Ще казваме, че I е *ляв идеал* на R, когато са в сила следните свойства:

1. Ако $x, y \in I$, то $x - y \in I$;
2. Ако $x \in I$ и a е произволен елемент от R, то $ax \in I$.

Непразното подмножество I наричаме *десен идеал*, когато е в сила първото от посочените свойства и за всеки елемент $x \in I$ имаме $xa \in I$, където a е произволен елемент от R. Ако I е едновременно и ляв, и десен идеал в пръстена R, то I се нарича *двустранен идеал* на R.

Ако пръстенът R е комутативен, очевидно горните три понятия съвпадат и тогава говорим просто за идеал.

Примери.

а) Множеството, състоящо се от нулевия елемент на произволен пръстен R, е двустранен идеал на R. Очевидно целият пръстен R е също двустранен идеал на R. Тези два идеала се наричат несобствени.

б) Множеството от всички цели числа, кратни на дадено естествено число, е идеал на пръстена Z на целите числа.

в) Нека a е фиксиран елемент от пръстена R. Множеството от всички елементи на R, които имат вида ax, където x е произволен елемент от R, е десен идеал на R. Този идеал обикновено се означава с aR. В случая, когато пръстенът R е комутативен, aR се нарича *главен идеал, породен от елемента a*, и се означава още с (a).

г) Множеството от квадратните матрици, които могат да имат ненулеви елементи само в първия си ред, образува десен идеал в пръстена на квадратните матрици от ред n. Лесно се вижда, че това множество не е ляв идеал.

От определението за идеал следва, че ако I е идеал в пръстена R то $0 \in I$ и ако $x \in I$, то $-x \in I$. Също така, ако $x, y \in I$, то $x+y \in I$.

Нека I е двустранен идеал в пръстена R. Два елемента x, y от R наричаме *сравними по модул I*, когато $x-y \in I$. Ако x и y са сравними по модул I, пишем $x \equiv y \pmod{I}$. Тази релация притежава следните свойства:

1. $x \equiv x \pmod{I}$ за всяко $x \in R$.
2. Ако $x \equiv y \pmod{I}$, то $y \equiv x \pmod{I}$.
3. Ако $x \equiv y \pmod{I}$ и $y \equiv z \pmod{I}$, то $x \equiv z \pmod{I}$.
4. Ако $x \equiv y \pmod{I}$ и $z \equiv t \pmod{I}$, то $x+z \equiv y+t \pmod{I}$ и $xz \equiv yt \pmod{I}$.

Нека R е пръстен и I е двустранен идеал в R. С помощта на I елементите на R се разбиват на класи на еквивалентност по следния начин: *два елемента x, y принадлежат на един и същ клас тогава и само тогава, когато $x \equiv y$* $\pmod{I}$. Ясно е, че всеки елемент x от R принадлежи на точно един клас, който се означава с $\bar{x}$. Лесно се вижда, че $\bar{x}$ се състои от всички елементи на R, които могат да се представят във вида $x+a$, където $a \in I$. Множеството на всички такива класове означаваме с R/I. В R/I дефинираме събиране и умножение по следните формули:

$$\bar{x}+\bar{y}=\overline{x+y},$$
$$\bar{x}\bar{y}=\overline{xy}.$$

От изложените по-горе свойства на сравненията следва, че сумата и произведението на два класа не зависят от изборите на техните представители. Относно така дефинираните операции R/I е пръстен, който се нарича *факторопръстен на пръстена R, по идеала I*. За нулев елемент в пръстена R/I служи класът $\bar{0}=I$. Ако R има единица 1, то $\bar{1}$ е единица на факторпръстена R/I.

Пример. Пръстенът Z_n е факторпръстен на пръстена на целите числа по идеала (n).

Определение. Нека R и R' са два пръстена. Едно изображение φ на R в R' се нарича *хомоморфизъм*, когато са в сила равенствата:

$$\varphi(a+b)=\varphi(a)+\varphi(b),\quad \varphi(ab)=\varphi(a)\varphi(b),$$

за произволни $a, b\in R$ (тук $\varphi(x)$ означава образа на елемента x от R в R').

Ако φ е хомоморфизъм на R в R', множеството от елементи x на R, за които $\varphi(x)=0'$, се нарича *ядро* на φ и се означава с $\operatorname{Ker}\varphi$. Доказва се, че $\operatorname{Ker}\varphi$ е двустранен идеал в R.

Пример. Нека I е двустранен идеал на пръстена R. На всеки елемент $x\in R$ да съпоставим $\bar{x}$ от R/I. Лесно се вижда, че така полученото изображение на R в R/I е хомоморфизъм. Този хомоморфизъм се нарича *каноничен хомоморфизъм* на R върху R/I.

Теорема за хомоморфизмите. Нека φ е хомоморфизъм на пръстена R върху пръстена R'. Тогава R' е изоморфен на факторпръстена $R/\operatorname{Ker}\varphi$. По-точно съществува единствен изоморфизъм θ на $R/\operatorname{Ker}\varphi$ върху R', така че $\varphi=\theta\circ\eta$, където η е каноничният хомоморфизъм на R върху $R/\operatorname{Ker}\varphi$.

Определение. Един идеал M на комутативния пръстен R се нарича *максимален*, когато $M\neq R$ и не съществува идеал $I\neq R$, така че $M\subset I$, $M\neq I$.

Определение. Един идеал P в комутативния пръстен R се нарича *прост*, когато от $xy\in P$, следва $x\in P$ или $y\in P$.

Теорема. Ако R е комутативен пръстен с единица, то всеки собствен идеал на R се съдържа в максимален и всеки максимален идеал е прост.

Теорема. Нека R е комутативен пръстен с единица. Идеалът I на R е максимален тогава и само тогава, когато факторпръстенът R/I е поле. Идеалът I е прост тогава и само тогава, когато R/I е област на цялост.

1. Покажете, че ако $a_1, a_2,\ldots, a_n$ са елементи от пръстена R с единица, то множеството от всички елементи $x\in R$, които могат да се представят във вида

$$x=x_1a_1+x_2a_2+\ldots+x_na_n,$$

където $x_1, x_2,\ldots, x_n$ са произволни елементи от R, е идеал на R. Този идеал се нарича *идеал, породен от елементите* $a_1, a_2,\ldots, a_n$, и се означава с $(a_1, a_2,\ldots, a_n)$.

2. Покажете, че идеалът от предишната задача е минималният идеал, съдържащ елементите $a_1, a_2,\ldots, a_n$.

3. Покажете, че сечението на произволен брой идеали на пръстена R е идеал в R.

4. Нека X е подмножество на комутативния пръстен R. Покажете, че сечението (X) на всички идеали в R, съдържащи X,

е идеал, който се състои от всички елементи на R, представими като крайни суми на елементи от nx и ry, $n \in Z$, $r \in R$ и $x, y \in X$. (X) се нарича идеал, породен от множеството X.

5. Нека R е комутативен пръстен и X е подмножество на R. Покажете, че множеството I, състоящо се от елементи на R, които могат да се представят във вид на крайни суми $\sum_{i=1}^{n} r_i x_i$, където $r_i \in R$ и $x_i \in X$ е идеал в R. В случай че R е пръстен с единица, идеалът I съвпада с идеала (X), породен от множеството X.

6. Посочете пример на комутативен пръстен R и подмножество X, така че идеалът от предната задача да не съвпада с (X).

7. Формулирайте и докажете твърдения, подобни на тези от зад. 4, 5, в случай че пръстенът е некомутативен.

Определение. Под *сума на два идеала* I, J разбираме множеството $I+J=\{x+y : x \in I, y \in J\}$. Под *произведение* на идеала I с идеала J се разбира множеството от всички крайни суми $\sum x_i y_i$, $x_i \in I, y_i \in J$. Това произведение ще означаваме с IJ.

8. Докажете, че сумата и произведението на идеали са също идеали.

9. Покажете, че $I+J=(I \cap J)$.

10. Докажете, че за произволни идеали I, J, K имаме:

а) $I(JK)=(IJ)K$;

б) $I(J+K)=IJ+IK$;

в) $IJ \subset I \cap J$;

г) $I \cap (J+K)=J+(I \cap K)$ при $J \subset I$ (модулярен закон).

11. Посочете пример, когато включването $IJ \subset I \cap J$ е строго.

12. Нека (a) и (b) са два главни идеала в даден комутативен пръстен с единица и без делители на нулата. Докажете, че $(a)=(b)$ тогава и само тогава, когато $a=ub$ при някой обратим елемент u от пръстена.

13. Нека R е комутативен пръстен с единица. Докажете, че един елемент $x \in R$ е обратим тогава и само тогава, когато главният идеал, породен от (x), съвпада с R.

14. Нека R е пръстен с единица. Докажете, че R е тяло тогава и само тогава, когато всеки ненулев идеал (изобщо едностранен — ляв или десен) в R съвпада с R.

15. Докажете, че всеки идеал в пръстена Z на целите числа е главен. Представете всеки един от идеалите

$$(m)+(n),\ (m)(n),\ (m)\cap(n)$$

като главен идеал.

16. Докажете, че в пръстена $Z[\sqrt{-1}]$ от целите гаусови числа $a+bi$, a, $b \in Z$ всеки идеал е главен.

17. Да се намерят всички идеали в пръстена от 4 елемента, зададен с таблиците

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

,

.	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

и да се покаже, че те са главни идеали.

18. Да се докаже, че в пръстена S от 8 елемента, зададен с таблиците

+	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	d	c	f	e	h	g
c	c	d	a	b	g	h	e	f
d	d	c	b	a	h	g	f	e
e	e	f	g	h	a	b	c	d
f	f	e	h	g	b	a	d	c
g	g	h	e	f	c	d	a	b
h	h	g	f	e	d	c	b	a

,

.	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	b	a	b	a	b	a	b
c	a	c	a	c	a	c	a	c
d	a	d	a	d	a	d	a	d
e	a	e	a	e	a	e	a	e
f	a	f	a	f	a	f	a	f
g	a	g	a	g	a	g	a	g
h	a	h	a	h	a	h	a	h

множеството $\{a, b, c, d\}$ е десен идеал в S, но не е ляв идеал Да се покаже, че следните множества:

$$\{a, c\}, \{a, e\}, \{a, g\}, \{a, c, e, g\}$$

са двустранни идеали в S.

Определение. Нека I и J са идеали в комутативен пръстен R. С $(I:J)$ означаваме множеството на всички елементи x от R, за които $xJ \subset I$. Множеството $(I:J)$ се нарича *ньотерово частно* на идеалите I и J.

19. Докажете, че ньотеровото частно на идеалите I и J е също идеал.

20. Нека I, J, K да означават идеали в комутативен пръстен R. Докажете, че:

а) $(I:R) \supset I$, като в случая на пръстен с единица имаме $(I:R)=I$;

б) $(I:J)=R$ при $J \subset I$. В случай на пръстен с единица, обратно, от $(I:J)=R$ следва $I \supset J$;

в) $(I \cap J:K)=(I:K) \cap (J:K)$;

г) $(I:(J+K))=(I:J) \cap (I:K)$;

д) $(I:JK)=((I:J):K)$.

21. Намерете частното $((m):(n))$ на идеалите (m) и (n) в пръстена Z на целите числа.

22. Докажете, че идеалът P в комутативен пръстен с единица е прост тогава и само тогава, когато за всеки два идеала I и J от дадения пръстен R, удовлетворяващи условието $IJ \subset P$, имаме $I \subset P$ или $J \subset P$.

23. Един елемент от пръстен с единица е обратим тогава и само тогава, когато не принадлежи на никой максимален идеал.

24. Опишете всичките прости и всичките максимални идеали в пръстена Z на целите числа.

25. Нека R е комутативен пръстен. Докажете, че множеството от нилпотентните елементи на R е идеал в R. Този идеал се нарича *нилрадикал* на R. (Един елемент $x \in R$ се нарича *нилпотентен*, когато $x^k=0$ при някое естествено число k.)

26. Нека R е комутативен пръстен и I е идеал в R. Покажете, че множеството от елементите $x \in R$, някоя степен на всеки един от които принадлежи на I, е идеал, съдържащ I. Този идеал се нарича *радикал* на идеала I и се бележи с $r(I)$.

Забележка. Очевидно нилрадикалът на пръстена R (вж. зад. 25) съвпада с радикала $r(0)$ на нулевия идеал.

27. Нека R е комутативен пръстен и I, J са идеали в R. Докажете, че:

а) ако $I^k \subset J$ за някое естествено число k, то $r(I) \subset r(J)$;

б) $r(IJ)=r(I \cap J)=r(I) \cap r(J)$;

в) $r(I+J)=r(r(I)+r(J))$;

г) $r(r(I))=r(I)$.

28. Нека R е комутативен пръстен с единица. Докажете теоремата, че всеки собствен идеал на R се съдържа в максимален.

Доказателство. Нека Σ е множеството на всички собствени идеали в R, наредено по включване. Достатъчно е да покажем, че Σ удовлетворява предположенията на лемата на Цорн. Действително нека L е линейно наредено подмножество на Σ и $I=\bigcup \{J : J \in L\}$. Лесно се вижда, че I е идеал. Този идеал е собствен, защото в противен случай $1 \in I$, следователно $1 \in J$ за някой $J \in L$, откъдето $J=R$, което е невъзможно. По такъв начин показахме, че L е ограничено в Σ (идеалът I е горна граница на L). С това доказателството е завършено

29. Нека R е комутативен пръстен с единица. Докажете, че ако I е произволен идеал в R, то $r(I)$ съвпада със сечението на всички прости идеали, съдържащи I. В частност нилрадикалът на R съвпада със сечението на всички прости идеали в R.

Решение. Ако P е прост идеал, съдържащ I, то $r(I) \subset P$. Действително $r(I) \subset r(P)$, но, както лесно се вижда, $r(P)=P$. Остава да покажем, че ако $a \notin r(I)$, съществува прост идеал P, така че $I \subset P$ и $a \notin P$. За целта разглеждаме множеството Σ на всички идеали J в R, такива че $I \subset J$ и $a \notin r(J)$, наредено по включване. Непосредствено се проверява, че множеството Σ е непразно и удовлетворява условията на лемата на Цорн. Следователно в него има максимален елемент P. Доказателството ще бъде завършено, ако покажем, че идеалът P е прост. Да предположим, че $xy \in P$, но $x \notin P$ и $y \notin P$. Тогава идеалите $P+Rx$ и $P+Ry$ ще съдържат строго P и поради максималността на P няма да принадлежат на Σ, т. е. $a \in r(P+Rx)$ и $a \in r(P+Ry)$. Това означава, че съществува естествено число n, така че $a^n \in P+Rx$ и $a^n \in P+Ry$. В такъв случай $a^{2n} \in (P+Rx)(P+Ry) = P+PRx+PRy+Rxy \subset P$, понеже $Rxy \subset P$, откъдето $a \in r(P)$, което противоречи на избора на P.

30. При предположенията от предната задача докажете по-силното твърдение, че $r(I)$ съвпада със сечението на всички минимални прости идеали, съдържащи I.

Решение. Достатъчно е да покажем, че всеки прост идеал, съдържащ I, съдържа минимален прост идеал, съдържащ I. За целта означаваме със Σ множеството от прости идеали, които съдържат I. Ще установим, че всяко линейно наредено подмножество L на Σ е ограничено отдолу. Нека $P=\bigcap\{Q: Q\in L\}$. Очевидно $I\subseteq P$ и остава да се покаже, че P е прост. Да предположим, че $xy\in P$, но $x\notin P$ и $y\notin P$. Тогава $x\notin Q_1$ и $y\notin Q_2$ за някои $Q_1, Q_2\in L$. Нека $Q_1\subset Q_2$ (множеството L е линейно наредено). В такъв случай $x\notin Q_1$ и $y\notin Q_1$, откъдето $xy\notin Q_1$, понеже идеалът Q_1 е прост. Но тогава $xy\notin P$, което противоречи на предположението $xy\in P$.

31. Нека R е комутативен пръстен с единица. Покажете, че един идеал съвпада с радикала си тогава и само тогава, когато може да се представи като сечение на прости идеали.

Определение. Нека R е комутативен пръстен. Идеалът Q в R, $Q\neq R$, се нарича *примарен*, когато от $xy\in Q$ и $x\notin Q$ следва $y^k\in Q$ за някое естествено число K.

32. Покажете, че всеки прост идеал е примарен. Ако един идеал е примарен, радикалът му е прост.

33. Покажете, че ако $I_1, I_2, \ldots, I_n$ са примарни идеали с един и същ радикал, сечението им е примарен идеал със същия радикал.

34. Докажете, че радикалът на идеала (n) в пръстена Z на целите числа, където $n=p_1^{\lambda_1}p_2^{\lambda_2}\ldots p_s^{\lambda_s}$ е кононичното разлагане на n, е идеалът, породен от произведението $p_1p_2\ldots p_s$ на различните прости делители на n. С други думи, в сила е равенството

$$r((p_1^{\lambda_1}p_2^{\lambda_2}\ldots p_s))=(p_1p_2\ldots p_s).$$

35. Опишете всички примарни идеали в пръстена Z на целите числа.

Отг. (p^λ), p—просто, λ—естествено.

Определение. Нека R е комутативен пръстен с единица 1. С G означаваме множеството от всички елементи $x\in R$, такива че за всяко $y\in R$ елементът $1-xy$ е обратим. Множеството G се нарича *радикал на Джекобсън* на пръстена R.

36. Докажете, че радикалът на Джекобсън на пръстена R е идеал в пръстена R, който съдържа нилрадикала на R.

37. Докажете, че радикалът на Джекобсън на пръстена R съвпада със сечението на всички максимални идеали на R.

Решение. Нека x принадлежи на всички максимални идеали на R. Ще покажем, че $x\in G$. В противен случай съществува $y\in R$, така че елементът $1-xy$ е необратим. Тогава идеалът $R(1-xy)$ е собствен, следователно се съдържа в някакъв максимален идеал M. Но $x\in M$, откъдето следва $1\in M$, което е невъзможно. Следователно $x\in G$. Обратно, нека $x\in G$ и M е максимален идеал. Ако предположим, че $x\notin M$, от максималността на M следва $M+Rx=R$, т. е. съществува $y\in R$ и $m\in M$, така че $m+xy=1$ или $m=1-xy$. Следователно елементът m е обратим, което е невъзможно, тъй като един собствен идеал не може да съдържа обратими елементи.

38. Нека R е пръстен и I, J, K са идеали на R, такива че $I\subset J\cup K$. Покажете, че $I\subset J$ или $I\subset K$.

Решение. Да предположим, че съществуват x, $y\in I$, така че $x\notin J$ и $y\notin K$. Тогава $x\in K$ и $y\in J$. Но $x+y\in I$, откъдето $x+y\in J$ или $x+y\in K$. Ако $x+y\in J$, получаваме $x\in J$, което е невъзможно.

39. Нека R е комутативен пръстен и I, $P_1, P_2, \ldots, P_n$ са идеали в R, такива че $I\subset P_1\bigcup P_2\bigcup\ldots\bigcup P_n$ и $P_1, P_2, \ldots, P_n$ са прости. Покажете, че $I\subset P_k$ за някое k.

Решение. Доказателството ще извършим индуктивно по n. При $n=1$ твърдението е очевидно. В общия случай да допуснем, че съществува i, така че $P_i\cap I\subset\bigcup\{P_j : j\neq i\}$. Тогава лесно се вижда, че $I\subset\bigcup\{P_j : j\neq i\}$ и съгласно индуктивното предположение $I\subset P_k$ за някое k. Нека сега за всяко i $P_i\cap I\not\subset\bigcup\{P_j : j\neq i\}$. В такъв случай съществуват елементи x_i, така че $x_i\in P_i\cap I$, но $x_i\notin P_j$, при $j\neq i$. Да разгледаме елемента $y=x_1+x_2x_3\ldots x_n$. Очевидно $y\in I$ и следователно $y\in P_i$ за някое i. Понеже $x_2x_3\ldots x_n\in P_j$, $j=2,\ldots,n$, а $x_1\notin P_j$, то $y\notin P_j$ $j=2,\ldots,n$. Остава $y\in P_1$. Но $x_1\in P_1$, а $x_2x_3\ldots x_n\notin P_1$, понеже P_1 е прост, откъдето $y\notin P_1$, което е противоречие.

Забележка. От доказателството е ясно, че твърдението остава в сила при по-слабото предположение, че поне $n-2$ от идеалите $P_1, P_2, \ldots, P_n$ са прости. Ще отбележим обаче, че ако последното предположение се отслаби, твърдението престава да бъде вярно.

40. Покажете, че факторпръстенът $Z_n=Z/(n)$ на пръстена на целите числа Z по главния идеал (n) се състои от n елемента. Покажете също, че Z_n е поле тогава и само тогава, когато естественото число n е просто.

41. Съставете таблиците за събиране и умножение във факторпръстена R/I, където:

а) $R=Z$, $I=(6)$;

б) $R=Z$, $I=(7)$;

в) $R=2Z$ е пръстенът на всички четни числа, $I=2R$;

г) R е пръстенът от зад. 18, $I=\{a, c\}$;

д) $R=Z[i]$, $I=2R$;

е) $R=Z[\sqrt{-1}]$, $I=(1+i)$.

42. Нека R е пръстен и I е двустранен идеал в R, $S=R/I$ и η е каноничният хомоморфизъм на R върху S. Докажете, че ако S' е произволен подпръстен на S, то $R'=\eta^{-1}(S')$ е подпръстен на R, съдържащ идеала I, като при това $R'/I=S'$. Освен това, ако S' е ляв (десен, двустранен) идеал в S, то R' е ляв (десен, двустранен) идеал в R.

43. При означенията от предната задача покажете, че посредством изображението $S'\to\eta^{-1}(S')$ се установява взаимно еднозначно обратимо съответствие между подпръстените (левите идеали, десните идеали, двустранните идеали) на S и подпръстените (левите идеали, десните идеали, двустранните идеали) на R, съдържащи I. Покажете, че ако I' и J' са идеали в S', то

$$\eta^{-1}(I'+J')=\eta^{-1}(I')+\eta^{-1}(J') \text{ и } \eta^{-1}(I'J')=\eta^{-1}(I')\cap\eta^{-1}(J').$$

44. При означенията от задача 42, ако R_1 е подпръстен на R, то R_1+I също е подпръстен на R, $\eta(R_1)$ е подпръстен на S и са в сила следните канонични изоморфизми:

$$\eta(R_1)\cong R_1/(R_1\cap I)\cong(R_1+I)/I.$$

45. Нека I и J са два двустранни идеала в пръстена R и $I\subset J$. Покажете, че J/I е идеал в R/I и съществува каноничен изоморфизъм

$$(R/I)/(J/I)\cong R/J.$$

46. Нека A и B са пръстени и φ е хомоморфизъм на A в B. Покажете, че ако J е идеал в B, то множеството

$$\varphi^{-1}(J)=\{x\in A:\varphi(x)\in J\}$$

е идеал в A. В частност при $J=0$ получаваме $\operatorname{Ker}\varphi$.

47. При означенията от предишната задача покажете, че ако идеалът P на B е прост, то и $\varphi^{-1}(P)$ е прост. Вярно ли е това твърдение, ако вместо прости разглеждаме максимални идеали?

48. Нека A и B са пръстени и φ е хомоморфизъм на A върху B. Покажете, че ако I е идеал в A, то множеството

$$\varphi(I)=\{\varphi(x)\in B:x\in I\}$$

е идеал в B. Вярно ли е твърдението, ако хомоморфизмът φ не е върху?

49. Нека $R_1, R_2,\dots,R_n$ са пръстени и $R=\prod_{i=1}^{n} R_i$ е декартовото произведение на множествата R_i. В R въвеждаме операции събиране и умножение по следните формули:

$$(x_1, x_2,\dots,x_n)+(y_1, y_2,\dots,y_n)=(x_1+y_1, x_2+y_2,\dots,x_n+y_n),$$

$$(x_1, x_2,\dots,x_n)(y_1,y_2,\dots,y_n)=(x_1y_1, x_2y_2,\dots,x_ny_n).$$

Да се покаже, че R е пръстен относно така дефинираните операции.

Определение. Пръстенът R, построен в предната задача, се нарича *декартово произведение* на пръстените $R_1, R_2,\dots,R_n$.

50. Нека $R_1, R_2,\dots,R_n$ са пръстени и R е тяхното декартово произведение. Означаваме с R_i' множеството от елементи на R, имащи вида $(0, 0,\dots,a_i,\dots,0)$. Покажете, че R_i' е двустранен идеал в R, който е изоморфен (като пръстен) на пръстена R_i. Покажете също така, че $R_i'R_j'=0$ при $i\neq j$ и че всеки елемент на R еднозначно може да се представи във вида $x_1+x_2+\dots+x_n$, където $x_i\in R_i'$.

51. Нека R е пръстен и $R_1, R_2, \ldots, R_n$ са двустранни идеали в R, удовлетворяващи условията:

а) $R=R_1+R_2+\ldots+R_n$;
б) $R_i\bigcap(R_1+R_2+\ldots+R_{i-1}+R_{i+1}+\ldots+R_n)=0$ за $i=1,2,\ldots,n$;
в) $R_i R_j=0$ при $i\neq j$.

Покажете, че R е изоморфен на декартовото произведение $\prod_{i=1}^{n} R_i$.

Упътване. Покажете, че всеки елемент $x\in R$ еднозначно може да се представи във вида $x=x_1+x_2+\ldots+x_n$, където $x_i\in R_i$ и съпоставете на x елемента $(x_1, x_2, \ldots x_n)$ от $\prod_{i=1}^{n} R_i$.

52. Нека $R_1, R_2, \ldots, R_n$ са пръстени и R е тяхното декартово произведение. Нека $i_1<i_2<\ldots<i_k$ са k индекса от 1 до n и $j_1<j_2<\ldots<j_{n-k}$ са останалите $n-k$. Означаваме с S множеството от елементи $(x_1, x_2, \ldots, x_n)$ на R, за които $x_i=0$ при $i\neq i_1, i_2, \ldots, i_k$. Покажете, че S е двустранен идеал в R, изоморфен (като пръстен) със $\prod_{\alpha=1}^{k} R_{i_\alpha}$ и че факторпръстенът R/S е изоморфен на $\prod_{\beta=1}^{n-k} R_{j_\beta}$.

53. Покажете, че декартовото произведение на пръстени има единица тогава и само тогава, когато всеки множител има единица.

54—55. Покажете, че декартовото произведение на пръстени е комутативен пръстен тогава и само тогава, когато всеки множител е комутативен.

Определение. Два идеала I и J на пръстена R се наричат ***взаимно прости,*** когато $I+J=R$. По-общо, ако за идеалите $I_1, I_2, \ldots, I_n$ имаме $I_1+I_2+\ldots+I_n=R$, ще казваме, че тези идеали са взаимно прости. (Предполагаме, че разглежданите идеали са ненулеви, а R е комутативен пръстен с единица.)

56. Покажете, че главните идеали $(n_1), (n_2), \ldots, (n_k)$ в пръстена Z на целите числа са взаимно прости тогава и само тогава, когато числата $n_1, n_2, \ldots, n_k$ са взаимно прости, т. е. $(n_1, n_2, \ldots, n_k)=1$.

57. Покажете, че ако идеалите I и J са взаимно прости и m, n са естествени числа, идеалите I^m и J^n също са взаимно прости. Обобщете твърдението за произволен краен брой взаимно прости идеали.

58. Нека I и J са взаимно прости идеали. Покажете, че

$$I\bigcap J=IJ.$$

59. Нека $I_1, I_2, \ldots, I_n$ са идеали в пръстена R така, че $I_1 \cap I_2 \cap \ldots \cap I_n = 0$. Покажете, че изображението $f: R \to \prod_{j=1}^{n} R/I_j$, определено чрез равенството

$$f(a) = (a \pmod{I_1},\ a \pmod{I_2}, \ldots, a \pmod{I_n}),$$

е хомоморфизъм с нулево ядро и следователно от $a_1 \neq a_2$ следва $f(a_1) \neq f(a_2)$. (Тук под $a \pmod{I}$ разбираме класа в R/I, съдържащ елемента $a \in R$.)

60. Нека $I_1, I_2, \ldots, I_n$ и I са идеали в пръстена R, като $I_1 \cap I_2 \cap \ldots \cap I_n = I$. Покажете, че изображението

$$f: R/I \to \prod_{j=1}^{n} R/I_j,$$

дефинирано чрез равенството

$$f(a \pmod{I}) = (a \pmod{I_1},\ a \pmod{I_2}, \ldots, a \pmod{I_n}),$$

е хомоморфизъм, който на всеки два различни елемента от R/I съпоставя различни елементи на $\prod_{j=1}^{n} R/I_j$.

61. Нека I, J са идеали в пръстена R, за които $I+J=R$ (т. е които са взаимно прости). Докажете, че пръстените R/IJ и $R/I \times R/J$ са изоморфни. (Тук $R/I \times R/J$ означава декартовото произведение на пръстените R/I и R/J.)

Упътване. Използувайте зад. 58 и зад. 60.

62. Нека $I_1, I_2, \ldots, I_n$ са два по два взаимно прости идеала в пръстена R, т. е. $I_j + I_k = R$ за всички стойности на индексите j, k. Докажете, че пръстените $R/I_1 I_2 \ldots I_n$ и $\prod_{s=1}^{n} R/I_s$ са изоморфни (*китайска теорема за остатъците*).

Упътване. Докажете и използувайте следното обобщение на твърдението от зад. 58: $I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \ldots \cap I_n$ при $I_j + I_k = R$, $j \neq k$. Използувайте и зад. 60.

63. Нека $n_1, n_2, \ldots, n_k$ са две по две взаимно прости естествени числа. Докажете, че пръстените $Z_{n_1 n_2 \ldots n_k}$ и $\prod_{i=1}^{k} Z_{n_i}$ са изоморфни.

64. Нека a и b са две взаимно прости естествени числа. Докажете, че $\varphi(ab)=\varphi(a)\varphi(b)$, където φ означава функцията на Ойлер.

Упътване. Използувайте предната задача.

Определение. Естественото число n се нарича *характеристика* на пръстена R, когато $nx=0$ за всяко $x \in R$ и n е най-малкото естествено число с това свойство, т. е. от $mx=0$ за всяко $x \in R$ следва $n \leq m$. Ако такова естествено число не съществува, казваме, че пръстенът R има характеристика 0.

65. Докажете, че характеристиката на всеки пръстен без делители на нулата е или нула, или просто число.

66. Нека R е пръстен с характеристика $n \neq 0$ и m е естествено число. Означаваме с I_m множеството

$$I_m=\{x : x \in R \text{ и } mx0\}.$$

а) Докажете, че I_m е двустранен идеал в R и $I_m=I_d$, където $d=(m, n)$.

б) Нека $n=kl$, където $(k,l)=1$. Докажете че $R \cong I_k \times I_l$.

в) Ако $n=p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k}$ е каноничното разлагане на n на прости множители, покажете, че $R \cong \prod_{i=1}^{k} I_{p_i^{\lambda_i}}$.

Докажете също, че всеки пръстен $I_{p_i^{\lambda_i}}$ има характеристика $p_i^{\lambda_i}$.

67. Нека R е краен пръстен с характеристика p — просто число. Докажете, че броят на елементите на R е степен на p.

Упътване. Пръстенът R може да се разглежда като линейно пространство над полето Z_p.

68. Нека R е краен пръстен и $n=p_1 p_2 \ldots p_k$ е броят на елементите на R ($p_1, p_2, \ldots, p_k$ са различни прости числа). Докажете, че пръстенът R е комутативен.

Упътване. С помощта на зад. 66 сведете към случая, когато $n=p$ е просто число. Покажете, че тогава или $R \cong Z_p$ или $xy=0$ за произволни $x, y \in R$.

69. Нека R е пръстенът на всички непрекъснати в интервала $[0, 1]$ функции и a е точка от този интервал. Покажете, че множеството M от функции, които се анулират в точката a, е ма-

ксимален идеал в R и факторпръстенът R/M е изоморфен на полето на реалните числа.

Определение. Пръстенът R се нарича *булев,* когато $x^2=x$ за всяко $x \in R$, т. е. когато всеки елемент на R е идемпотентен.

Съгласно зад. 39, § 1 всеки булев пръстен е комутативен и има характеристика 2.

70. Покажете, че всеки булев пръстен без делители на нулата е изоморфен с полето Z_2.

71. Нека R е булев пръстен и $x \in R$. Покажете, че $x \in Rx$ и x е единица на пръстена Rx.

72. Нека R е булев пръстен и $x_1, x_2, \ldots, x_n \in R$. Покажете, че идеалът, породен от елементите $x_1, x_2, \ldots, x_n$, е главен, в частност той е пръстен с единица. Оттук следва, че всеки краен булев пръстен има единица.

Упътване. Покажете равенството $Rx_1+Rx_2=Ry$, където $y=x_1+x_2+x_1x_2$

73. Покажете, че в булев пръстен с единица всеки прост идеал е максимален.

74. Покажете, че в булев пръстен с единица радикалът на Джекобсън е нула.

Упътване. Покажете, че в R няма нилпотентни елементи и използувайте предната задача.

75. Нека E е множество и P_E е множеството от всички подмножества на E. За произволни $A, B \in P_E$ полагаме

$$A+B=(A \sim B)\cup(B \sim A) \text{ и } AB=A \cap B.$$

Покажете, че относно така дефинираните операции P_E е булев пръстен с единица E и нула $\emptyset$. Пресметнете $A+A+AB$.

76. Нека E е крайно множество с n елемента. Покажете, че пръстенът P_E е изоморфен с пръстена Z_2^n. (Тук Z_2^n означава произведение на n пръстена, съвпадащи със Z_2.)

77. Нека E е множество и F_E означава множеството на всички изображения на E в Z_2. Покажете, че F_E е булев пръстен относно обичайните действия над функции, изоморфен с пръстен P_E от зад. 75.

Упътване. На всеки $A \in P_E$ съпоставяме характеристичната функция χ_A на A, дефинирана с условията $\chi_A(x)=1$ при $x \in A$ и $\chi_A(x)=0$ при $x \notin A$.

78. Докажете, че всеки краен булев пръстен е изоморфен с пръстен от вида P_E.

Решение. Нека R е краен булев пръстен и $M_1, M_2, \ldots, M_n$ са всички максимални идеали в R. Очевидно те са два по два взаимно прости, а от зад. 74 следва $M_1 M_2 \ldots M_n=0$. Тогава съгласно зад. 62 $R \cong \prod_{i=1}^{n} R/M_i$, а всеки R/M_i е изоморфен със Z_2.

79. Нека R е булев пръстен с единица и E е множеството от максимални идеали на R. За произволно $x \in R$ означаваме с $U(x)$ множеството от всички $M \in E$, за които $x \notin M$. Покажете, че изображението $x \to U(x)$ е изоморфизъм на пръстена R върху подпръстен на P_E.

Решение. Равенството $U(xy) = U(x)U(y)$ се проверява непосредствено. Ще покажем, че $U(x+y) = U(x) + U(y)$. Нека $M \in U(x+y)$, т. е. $x+y \notin M$. Тогава $x \notin M$ или $y \notin M$. Нека например $x \notin M$. В такъв случай ще имаме $y \in M$. Действително, ако $y \notin M$, класовете $\bar{x}$ и $\bar{y}$ ще бъдат ненулеви елементи във факторпръстена R/M. Но $R/M \cong Z_2$, така че $\bar{x} = \bar{y} = \bar{1}$, откъдето $\bar{x} + \bar{y} = \bar{0}$, което означава $x+y \in M$. И така, ако $x \notin M$, то $y \in M$ или $M \in U(x) \sim U(y)$. По такъв начин е доказано включването $U(x+y) \subset U(x) + U(y)$. Обратното включване се установява непосредствено. Остава да покажем, че от $x \neq y$ следва $U(x) \neq U(y)$ или все едно от $x \neq 0$ следва $U(x) \neq \emptyset$. Но това следва непосредствено от зад. 74. Накрая ще отбележим, че $U(1) = E$, т. е. че изоморфизмът U преобразува единица в единица.

80. Нека E е компактно топологично пространство и C_E означава множеството от всички едновременно отворени и затворени подмножества на E. Покажете, че C_E е подпръстен на пръстена P_E от зад. 75, съдържащ единицата E.

81. Теорема на Стоун за представяне на булеви пръстени. Нека R е булев пръстен с единица. Съществува компактно хаусдорфово напълно несвързано топологично пространство E, така че R е изоморфен с пръстена C_E, дефиниран в предната задача.

Упътване. Съгласно зад. 79 пръстенът R е изоморфен с подпръстена S на P_E, образуван от всички множества от вида $U(x)$, $x \in R$. Теоремата ще бъде доказана, ако върху E се дефинира такава компактна хаусдорфова напълно несвързана топология, че $C_E = S$. С непосредствена проверка се вижда, че топологията, породена от множеството S (най-малката топология, за която елементите на S са отворени множества), притежава исканите свойства.

Забележка. Едно топологично пространство се нарича напълно несвързано, ако едновременно отворените и затворените негови подмножества образуват база на топологията му.

82. Нека R е булев пръстен. За произволни елементи x, y от R нека $x \leq y$ тогава и само тогава, когато $xy = x$. Покажете, че релацията $\leq$ е частична наредба в R и че R е решетка относно тази наредба. Покажете също, че нулата е най-малък елемент на R, а в случай че R има единица, тя е най-голям елемент на R.

Упътване. За да покажете, че R е решетка, покажете, че елементите $x + y + xy$ и xy са съответно точна горна и точна долна граница на двойката елементи x, y.

83. Нека E е множество и R е пръстенът P_E от подмножества на E. Покажете, че за $A, B \in P_E$, $A \leq B$ в смисъл на предната задача тогава и само тогава, когато $A \subset B$.

ГЛАВА VIII

ПОЛИНОМИ

§ 1. ПРЪСТЕН ОТ ПОЛИНОМИ НА ЕДНА ПРОМЕНЛИВА

Нека P е произволно поле. Да разгледаме множеството R от всички редици от вида

$$f=(a_0, a_1, a_2, \dots, a_k, \dots),$$

гдето $a_i \in P$, $i=0, 1, 2, \dots, n, \dots$ и от известно място нататък членовете на редицата са равни на нула. В R дефинираме две алгебрични операции ***събиране и умножение*** по следния начин:
ако

$$f=(a_0, a_1, \dots, a_n, \dots)$$

и

$$g=(b_0, b_1, \dots, b_n, \dots),$$

то

$$f+g=(c_0, c_1, c_2, \dots),$$
$$fg=(d_0, d_1, d_2, \dots),$$

където

$$c_i=a_i+b_i, \qquad i=0, 1, 2, \dots$$
$$d_i=\sum_{\mu+\nu=i} a_\mu b_\nu .$$

Ясно е, че от $f, g \in R$ следва $f+g \in R$ и $fg \in R$. Непосредствено се проверява, че относно така дефинираните две операции множеството R е комутативен пръстен с нулев елемент

$$0=(0, 0, 0, \dots)$$

и единичен елемент

$$(1, 0, 0, \dots).$$

Множеството $P' \subset R$, състоящо се от елементи от вида

$$(c, 0, 0, \dots), \ c \in P,$$

е подпръстен на R, който е изоморфен с полето P. За краткост редиците от горния вид се отъждествяват със съответните елементи $c \in P$. Пишем

$$c=(c, 0, 0, \dots).$$

Имайки пред вид споменатия изоморфизъм, считаме, че полето P се съдържа в R. Имаме

$$cf=(ca_0,\ ca_1,\ ca_2,\ldots).$$

С x ще означаваме редицата

$$x=(0,\ 1,\ 0,\ 0,\ldots).$$

Имаме

$$x^2=(0,\ 0,\ 1,\ 0,\ldots),\qquad x^3=(0,\ 0,\ 0,\ 1,\ 0,\ldots),\ldots$$

Съгласно възприетите по-горе дефиниции можем да пишем

$$(1)\qquad f=a_0+a_1x+a_2x^2+\ldots+a_nx^n$$

при някое цяло $n\geq 0$.

Елементите $f\in R$, принадлежащи на R, се наричат *полиноми на x*; $a_0,\ a_1,\ a_2,\ldots,a_n$ се наричат коефициенти на полинома f. Пръстенът R, състоящ се от всички полиноми на x с коефициенти на полето P, ще означаваме с $P[x]$. Когато $a_n\neq 0$, казваме, че полиномът (1) е от *степен n*. Единствено нулевият полином, т. е. полиномът, на който всички коефициенти са равни на нула, не притежава определена степен. Полиномите от нулева степен това са отличните от нула елементи на P. Записването на полином f във вида (1) е традиционно и особено удобно при извършване на алгебричните действия с полиноми. Ако

$$f=a_0+a_1x+\ldots+a_nx^n$$

и

$$g=b_0+b_1x+\ldots+b_mx^m$$

са два полинома от $P[x]$, записани във вида (1) и например $n\geq m$, за сбора $f+g$ имаме

$$f+g=a_0+b_0+(a_1+b_1)x+\ldots+(a_n+b_n)x^n,$$

гдето считаме $b_k=0$ при $k>m$. Анологично за произведението fg имаме

$$fg=a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+(a_0b_k+a_1b_{k-1}+\\+\ldots+a_kb_0)x^k+\ldots+a_nb_mx^{n+m}.$$

Ясно е, че от $a_n\neq 0$ и $b_m\neq 0$ следва $a_nb_m\neq 0$ (тъй като в полето P няма делители на нулата). Следователно, ако полиномът f е от степен n и g е от степен m, произведението fg е полином от степен $n+m$. Оттук следва, че пръстенът $P[x]$ на полиномите на една променлива с коефициенти от полето P е без делители на нулата. Пръстенът $P[x]$ е област на цялостност. Следователно пръстенът $P[x]$ може да се допълни до поле от частни, което се означава с $P(x)$ и се нарича *поле от рационални функции* на x.

Ако R' е някакъв комутативен пръстен, който съдържа полето P и $t \in R'$, под $f(t)$ (където f означава полинома от (1)) ще разбираме следния елемент на R':

$$f(t)=a_0+a_1t+\ldots+a_nt^n.$$

Казваме, че $f(t)$ е *стойност* на полинома f за $t \in R'$. В този смисъл можем да пишем

$$f(x)=a_0+a_1x+\ldots+a_nx^n,$$

където $x \in P[x]$ означава дефинирания посредством

$$x=(0,\ 1,\ 0,\ldots)$$

полином от първа степен.

Изображението $f \to f(t)$ е хомоморфизъм на $P[x]$ в R', т. е от $h(x)=f(x)+g(x)$ и $q(x)=f(x)g(x)$ следва

$$h(t)=f(t)+g(t) \text{ и } q(t)=f(t).g(t)$$

при всички стойности на $t \in R'$.

Деление на полиноми. Нека $f(x)$ и $g(x)$ са полиноми на x от степени n и m. Съществуват полиноми $q(x)$ и $r(x)$, такива, че

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

като при това полиномът $r(x)$ или е равен на 0, или е от степен $<m$. Двата полинома $q(x)$ и $r(x)$ са определени еднозначно чрез $f(x)$ и $g(x)$ и се наричат съответно *частно и остатък* при делението на $f(x)$ с $g(x)$. Ако частното $q(x)\neq 0$, степента на $q(x)$ е равна на разликата $n-m$ от степените на $f(x)$ и $g(x)$. Когато $r(x)=0$, казваме, че полиномът $f(x)$ се дели на полинома $g(x)$. В такъв случай пишем

$$g(x)/f(x).$$

Намирането на частното и остатъка на практика се извършва по познатия алгоритъм, наподобяващ начина за деление на многоцифрени числа. Нека например

$$f(x)=2x^5+3x^4-x^2+8x-5 \text{ и } g(x)=x^3+2x+1,$$

Разглеждаме тези полиноми над полето на рационалните числа. Делението извършваме по следната схема:

$$\begin{array}{rl|l}
 & 2x^5+3x^4-x^2+8x-5 & x^3+2x+1 \\ \cline{3-3}
- & 2x^5+4x^3+2x^2 & 2x^2+3x-4 \\ \cline{2-2}
 & 3x^4-4x^3-3x^2+8x-5 & \\
- & 3x^4+6x^2+3x & \\ \cline{2-2}
 & -4x^3-9x^2+5x-5 & \\
- & -4x^3-8x-4 & \\ \cline{2-2}
 & -9x^2+13x-5. &
\end{array}$$

Получаваме

$$q(x)=2x^2+3x-4$$

и

$$r(x)=-9x^2+13x-5.$$

С други думи, в сила е равенството

$$2x^5+3x^4-x^2+8x-5=(x^3+2x+1)(2x^2+3x-4)-9x^2+13x-5.$$

Определение. Нека $f(x)$, $g(x)\in P[x]$. Под *най-голям общ делител* на $f(x)$ и $g(x)$ разбираме полинома $h(x)\in P[x]$, удовлетворяващ следните условия:

1. $h(x)/f(x)$ и $h(x)/g(x)$;

2. ако $h_1(x)/f(x)$ и $h_1(x)/g(x)$, то $h_1(x)/h(x)$.

С точност до ненулев множител от полето P съществува единствен най-голям общ делител. Всеки два полинома притежават най-голям общ делител и ако $h(x)$ е най-големият общ делител на полиномите $f(x)$ и $g(x)$, ще пишем

$$h(x)=(f(x),\ g(x)).$$

Най-големият общ делител на $f(x)$ и $g(x)$ може да се представи във вида

$$h(x)=u(x)f(x)+v(x)g(x),$$

където $u(x)$ и $v(x)$ са полиноми на x.

Намирането на най-големия общ делител се извършва удобно чрез познатия от елементарната аритметика алгоритъм на Евклид.

Определение. Казваме, че два полинома $f(x)$ и $g(x)$ са *взаимно прости,* когато нямат нито един общ делител от положителна степен.

Пример. Да се намери най-големият общ делител на полиномите

$$f(x)=x^4+2x^2+x+2 \text{ и } g(x)=x^3+2x^2+2x+1.$$

Разделяме най-напред $f(x)$ на $g(x)$:

$$\begin{array}{l|l} x^4+2x^2+x+2 & x^3+2x^2+2x+1 \\ \underline{x^4+2x^3+2x^2+x} & \overline{x-2} \\ \quad -2x^3+2 & \\ \quad \underline{-2x^3-4x^2-4x-2} & \\ \qquad 4x^2+4x+4 & \end{array}$$

Получаваме остатък $4(x^2+x+1)$. Делим след това полинома $g(x)$ на получения остатък x^2+x+1:

$$\begin{array}{l|l} x^3+2x^2+2x+1 & x^2+x+1 \\ \underline{x^3+x^2+x} & \overline{x+1} \\ \quad x^2+x+1 & \\ \quad \underline{x^2+x+1} & \\ \qquad 0 & \end{array}$$

Получаваме остатък 0. Следователно най-големият общ делител на дадените два полинома е x^2+x+1.

Неразложими полиноми. Разлагане на полиноми на неразложими множители

Определение. Един полином $p(x) \in P[x]$ се нарича *неразложим над полето P*, когато е от степен ≥ 1 и не може да се представи като произведение на два полинома от $P[x]$, имащи положителни степени.

Теорема. Всеки полином $f(x)$ от степен ≥ 1 може да се представи като произведение на неразложими полиноми. С точност до ненулеви множители от полето P това представяне е еднозначно.

Ако $p_1(x), \ldots, p_k(x)$ са различните делители на $f(x)$, ще имаме

$$f(x)=p_1^{\alpha_1}(x)\,p_2^{\alpha_2}(x)\ldots p_k^{\alpha_k}(x),$$

където числата $\alpha_1, \alpha_2, \ldots, \alpha_k$ са цели положителни и се наричат кратности съответно на неразложимите множители $p_1(x), p_2(x), \ldots, p_k(x)$. Изобщо казваме, че неразложимият полином $p(x)$ е *α-кратен множител* на $f(x)$, когато $f(x)=p^{\alpha}(x)f_1(x)$ и полиномът $f_1(x)$ не се дели на $p(x)$.

Определение. Нека

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

е полином от $P[x]$. Полиномът

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

се нарича *производна* на $f(x)$.

В сила са обичайните правила за диференциране:

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

В частност при всяко $c\in P$ имаме

$$[cf(x)]'=cf'(x).$$

Пример. Да намерим производната на полинома

$$f(x)=x(x^p-1),\quad f(x)\in Z_p[x].$$

Имаме

$$f'(x)=(x)'(x^p-1)+x(x^p-1)'=x^p-1+xpx^{p-1}=x^p-1.$$

Производната от n-ти ред на полинома $f(x)$ се дефинира чрез равенството

$$f^{(n)}(x)=(f^{(n-1)}(x))'.$$

Теорема за кратните множители. Ако $p(x)$ е α-кратен неразложим множител на полинома $f(x)\in P[x]$, то $p(x)$ е поне $(\alpha-1)$-кратен множител на производната $f'(x)$. В случай че характеристиката на полето P е равна на нула, кратността на $p(x)$ като множител на $f'(x)$ е точно $\alpha-1$.

С други думи, при диференциране кратностите на неразложимите множители намаляват с единица. Условието характеристиката на полето да е равна на нула е съществено. Например, ако $f(x)=x^p(x+1)\in Z_p[x]$, то $f'(x)=x^p$ и следователно неразложимият множител x се явява от една и съща кратност p в $f(x)$ и $f'(x)$.

Корени на алгебрични уравнения

Определение. Нека

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

е полином над дадено поле P. Ако $c\in P$ и $f(c)=0$, казваме, че c е *корен* на алгебричното уравнение $f(x)=0$. Казваме още, че c е нула на полинома $f(x)$ (корен на $f(x)$).

Теорема. Елементът $c\in P$ е тогава и само тогава корен на полинома $f(x)\in P[x]$, когато $x-c$ дели $f(x)$.

Казваме, че $c \in P$ е k-кратен корен на $f(x)$ или k-кратен корен на алгебричното уравнение $f(x)=0$, когато $x-c$ е k-кратен множител на $f(x)$, т. е.

$$f(x)=(x-c)^k f_1(x)$$

и за полинома $f_1(x)$ имаме $f_1(c)\neq 0$.

От теоремата за кратните множители непосредствено следва, че в случая на поле с характеристика нула, ако c е k-кратен корен на $f(x)$, то c е $(k-1)$-кратен корен на $f'(x)$. Следователно c е k-кратен корен на $f(x)$ тогава и само тогава, когато

$$f(c)=f'(c)=\dots=f^{(k-1)}(c)=0,\ f^{(k)}(c)\neq 0.$$

1. Пресметнете сбора и произведението на елементите $f(x)$ и $g(x)$ от $P[x]$, където:

а) $f(x)=x^2-3x+4$,
$g(x)=3x^2-1$, $P=Q$;

б) $f(x)=x^3-x+7$,
$g(x)=2x^4+5x^2-1$, $P=Q$;

в) $f(x)=x^4-\sqrt{2}x^3+4\sqrt{2}x+5$,
$g(x)=x^4+\sqrt{2}x^3-3\sqrt{2}x+7$, $P=D$;

г) $f(x)=2x^3-(3+i)x^2+4ix-1+i$,
$g(x)=-2x^3+(3-i)x^2+3ix+2-i$, $P=C$;

д) $f(x)=2x^3+3x^2+x+4$,
$g(x)=3x^2+3x+2$, $P=Z_5$;

е) $f(x)=x^4-x^2+6x+5$,
$g(x)=2x^3+5x^2-2x+3$, $P=Z_7$;

ж) $f(x)=2x^3+x^2-3x-1$,
$g(x)=3x^5-x^2+2x+3$

и P е полето с четири елемента, зададено с таблиците

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

2. Докажете тъждеството

$$\sum_{s=0}^{k}(-1)^s\binom{n}{k}\binom{n}{k-s}=\begin{cases}0, & \text{ако } k=2m+1,\\ (-1)^m\binom{n}{m}, & \text{ако } k=2m.\end{cases}$$

Упътване. Използувайте тъждеството

$$(x+1)^n(x-1)^n=(x^2-1)^n$$

и сравнете коефициентите.

3. Докажете, че над всяко поле с характеристика $p \neq 0$ са в сила тъждествата:

а) $(x+a)^p = x^p + a^p$

за всеки елемент a от полето;

б) $(x-1)^{p-1} = x^{p-1} + x^{p-2} + \dots + x + 1$.

Решение.

а) Тъждеството се получава непосредствено чрез развитие на бинома $(x+a)^p$ по формулата на Нютон, като се вземе пред вид, че при p просто биномните коефициенти $\binom{p}{k}$, $1 \leq k < p$ се делят на p.

б) Имаме

$$(x-1)^p = x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1),$$

откъдето чрез съкращаване на ненулевия полином $x-1$ получаваме

$$(x-1)^{p-1} = x^{p-1} + x^{p-2} + \dots + x + 1.$$

4. Докажете, че за всяко просто число p е в сила сравнението

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Упътване. Използувайте тъждеството б) от предната задача.

5. Намерете сумата на коефициентите на полинома

$$(2-4x+x^3)^{33}(3-5x+8x^2-6x^3)^{121}.$$

Отг. 0.

6. Докажете тъждествата:

а) $1 + \frac{1}{2}\binom{n}{1} + \frac{1}{3}\binom{n}{2} + \dots + \frac{1}{n+1}\binom{n}{n} = \frac{1}{n+1}(2^{n+1}-1)$;

б) $\binom{n}{0}\binom{n}{k} + \binom{n}{1}\binom{n}{k-1} + \dots + \binom{n}{k}\binom{n}{0} = \binom{2n}{k}$;

в) $\binom{n}{0}^2 + \binom{n}{1}^2 + \dots + \binom{n}{n}^2 = \binom{2n}{n}$;

г) $\binom{n}{1} + \binom{n}{3} + \dots + \binom{n}{2k+1} = \binom{n}{0} + \binom{n}{2} + \dots + \binom{n}{2s} = 2^{n-1}$,

където k и s са цели числа, такива, че $k \leq \frac{1}{2}(n-1) < k+1$,

$$s \leq \frac{n}{2} < s+1.$$

Решение.

а) От тъждеството

$$(1+x)^{n+1} = \binom{n+1}{0} + \binom{n+1}{1}x + \binom{n+1}{2}x^2 + \dots + \binom{n+1}{n+1}x^{n+1}$$

получаваме

$$\frac{(1+x)^{n+1}-1}{n+1} = \binom{n}{0}x + \frac{1}{2}\binom{n}{1}x^2 + \dots + \frac{1}{n+1}\binom{n}{n}x^{n+1}.$$

Интересуващото ни тъждество следва от последното равенство, като положим $x=1$.

б) От тъждеството $(1+x)^n=\sum_{s=0}^{n}\binom{n}{s}x^s$ имаме

$$\sum_{s=0}^{n}\binom{n}{s}x^s\sum_{t=0}^{n}\binom{n}{t}x^t=\sum_{k=0}^{2n}\binom{n}{k}\binom{n}{n-k}x^k=(1+x)^{2n}=\sum_{k=0}^{2n}\binom{2n}{k}x^k.$$

Като сравним коефициентите пред x^k, получаваме желаното тъждество.

в) Тъждеството следва от б) при $k=n$.

г) Тъждествата се доказват по подобен начин, като се разглеждат полиномите

$$\frac{1}{2}\left[(1+x)^n-(1-x)^n\right] \text{ и } \frac{1}{2}\left[(1+x)^n+(1-x)^n\right].$$

7. Намерете частното $q(x)$ и остатъка $r(x)$ от делението на полинома $f(x)$ с полинома $g(x)$, $f(x)$, $g(x)\in P[x]$, където:

а) $f(x)=x^5+3x^4+4x^2+2x-1$,
$g(x)=x^3+x+1$; $P=Q$;

б) $f(x)=3x^5+2x^4-x^3+x^2-4x+2$,
$g(x)=x^3-2x+3$, $P=Q$;

в) $f(x)=x^4-2x^3+4x^2-6x+8$,
$g(x)=x^3+3x-4$, $P=Z_{11}$;

г) $f(x)=2x^6-5x^4+3x^2+4x-1$,
$g(x)=3x^5-2x^4+7x^3-3x+5$, $P=Z_{11}$;

д) $f(x)=3x^7+2x^5+4x^3-3x+2$,
$g(x)=4x^5+3x^2-x+3$, $P=Z_5$;

е) $f(x)=2x^4-3x^3+x^2+3$,
$g(x)=2x+3$

и P е полето с четири елемента от зад. 1, ж);

ж) $f(x)=cx^5+gx^4+gx^3+bx^2+ax+e$,
$g(x)=cx^2+hx+d$

и $P=S$ е полето от § 1, зад. 14.

Отг. а) $q(x)=x^2+3x-1$, $r(x)=0$;
б) $q(x)=3x^2+2x+5$, $r(x)=-4x^2-13$;
в) $q(x)=x-2$, $r(x)=x^2+4x$;
г) $q(x)=8x-2$, $r(x)=x^4+3x^3+6x^2+2x-2$;
д) $q(x)=2x^2+3$, $r(x)=-x^4+x^3+3x^2$;
е) $q(x)=x^3+3x+1$, $r(x)=0$;
ж) $q(x)=hx^3+gx^2+cx+d$, $r(x)=bx+c$.

8. Намерете най-големия общ делител $d(x)$ на полиномите $f(x)$ и $g(x)$ от $P[x]$, където:

а) $f(x)=x^4+x^3-3x^2-4x-1$,
$g(x)=x^3+x^2-x-1$, $P=Q$;

б) $f(x)= x^5+x^4-x^3-2x-1$,
$g(x)=3x^4+2x^3+x^2+2x-2, \quad P=Q$;

в) $f(x)= x^6-7x^4+8x^3-7x+7$,
$g(x)=3x^5-7x^3+3x^2-7, \quad P=Q$;

г) $f(x)= x^4+7x^3+19x^2+23x+10$,
$g(x)= x^4+7x^3+18x^2+22x+12, \ P=Q$;

д) $f(x)= x^4+x^3-4x^2+x+1$,
$g(x)= x^4-x^3+x+4, \ P=Z_7$;

е) $f(x)= x^4+x^3-x^2+6x+4$,
$g(x)= x^3+5x^2+x+3, \ P=Z_{11}$;

ж) $f(x)= x^3+3x^2+3x+1$,
$g(x)= x^3+1$

и P е полето с четири елемента от зад. 1, ж).

Отг. а) $d(x)=x+1$;
б) $d(x)=x^2+1$;
в) $d(x)=x^3+1$;
г) $d(x)=1$;
д) $d(x)=x^2+3x+1$;
е) $d(x)=1$;
ж) $d(x)=x+1$.

9. Като използувате алгоритъма на Евклид, намерете полиноми $u(x)$ и $v(x)$, така че

$$u(x)f(x)+v(x)g(x)=d(x),$$

където $d(x)$ е най-големият общ делител на полиномите $f(x)$ и $g(x)$ от $P[x]$:

а) $f(x)=x^4+2x^3-x^2-4x-2$,
$g(x)=x^4+x^3-x^2-2x-2, \quad P=Q$;

б) $f(x)=x^5+3x^4+x^3+x^2+3x+1$,
$g(x)=x^4+2x^3+x+2, \quad P=Q$;

в) $f(x)=4x^4-2x^3-16x^2+5x+9$,
$g(x)=2x^3-x^2-5x+4, \quad P=Q$;

г) $f(x)=3x^7+6x^6-3x^5+4x^4+14x^3-6x^2-4x+4$,
$g(x)=3x^6-3x^4+7x^3-6x+2, \quad P=Q$;

д) $f(x)=3x^5+x^4+3x^3+4$,
$g(x)=2x^4+2x^3+2x+3, \quad P=Z_5$;

е) $f(x)=x^5+x^4+x^3-5x^2+2x-5$,
$g(x)=x^4+3x^3-x+4, \quad P=Z_{11}$;

ж) $f(x)=x^4+x^3+3x^2+2x+2$,
$g(x)=x^4+3x^2+2$

и P е полето от задача 1, ж),

з) $f(x)=cx^4+hx^3+ax^2+gx+e$;
$g(x)=gx^3+hx^2+dx+g$

и P е полето с 8 елемента от § 1, зад. 14.

Отг. а) $d(x)=x^2-2$, $u(x)=-x-1$, $v(x)=x+2$;
б) $d(x)=x^3+1$, $u(x)=-1$, $v(x)=x+1$;
в) $d(x)=x-1$, $u(x)=\frac{1}{3}(1-x)$, $v(x)=\frac{1}{3}(2x^2-2x-3)$;
г) $d(x)=x^3+2$, $u(x)=1-x^2$, $v(x)=x^3+2x^2-x-1$;
д) $d(x)=x^2+1$, $u(x)=3$, $v(x)=3x+3$;
е) $d(x)=x^2+x+1$, $u(x)=5$, $v(x)=2x+3$;
ж) $d(x)=x^2+2$, $u(x)=x$, $v(x)=x+1$;
з) $d(x)=u(x)\,f(x)+v(x)\,g(x)$, $u(x)=gx+h$, $v(x)=cx^2+hx+e$.

10. Нека $d(x)$ е най-големият общ делител на полиномите $f(x)$ и $g(x)$ и $u(x)$, $v(x)$ са полиноми, такива, че

$$u(x)\,f(x)+v(x)\,g(x)=d(x).$$

Намерете най-големия общ делител на $u(x)$ и $v(x)$.

Отг. $(u(x), v(x))=1$.

11. Нека $f(x)$ и $g(x)$ са взаимно прости полиноми от степени, съответно равни на n и m. Покажете, че полиномите $u(x)$ и $v(x)$ от равенството

$$u(x)\,f(x)+v(x)\,g(x)=1$$

могат да се подберат така, че степените им да не надминават съответно $m-1$ и $n-1$ и при тези условия полиномите $u(x)$ и $v(x)$ са определени еднозначно.

Упътване. Ако полиномите $u_1(x)$ и $v_1(x)$ удовлетворяват равенството $u_1(x)\,f(x)+v_1(x)\,g(x)=d(x)$, заместваме тези полиноми съответно с остатъците им при делението с $g(x)$ и $f(x)$.

12. Нека $f(x)$ и $g(x)$ са полиноми от степени съответно n и m и k да е степента на най-големия им общ делител $d(x)$. Покажете, че полиномите $u(x)$ и $v(x)$ в равенството

$$u(x)\,f(x)+v(x)\,g(x)=d(x)$$

могат да се подберат така, че степените им да не надминават съответно $m-k-1$ и $n-k-1$. При тези условия полиномите $u(x)$ и $v(x)$ са определени еднозначно.

Упътване. Използувайте предната задача.

13. Намерете по метода на неопределените коефициенти полиномите $u(x)$ и $v(x)$ от зад. 11 и 12 за полиномите:

а) $f(x)=x^3+x^2-x-2$, $g(x)=x^3-4x^2+5x-2$;
б) $f(x)=x^5$, $g(x)=(x-2)^3$;
в) $f(x)=x^5+2x^4+4x^3+10x^2+16x+12$, $g(x)=x^4+2x^3+3x^2+$
$+2x+2$;
г) $f(x)=x^4-4x^3+1$, $g(x)=x^3-3x^2+1$;
д) $f(x)=x^4$, $g(x)=(1-x)^4$;
е) $f(x)=x^m$, $g(x)=(1-x)^n$.

Отг. а) $u(x)=\frac{1}{8}(41x^2-114x+65)$, $v(x)=-\frac{1}{8}(41x^2+91x+69)$;

б) $u(x)=\frac{1}{128}(15x^2-70x+84)$, $v(x)=-\frac{1}{128}(15x^4+20x^3+24x^2+$
$+24x+16)$;

в) $u(x)=-\frac{1}{37}(x-6)$; $v(x)=\frac{1}{37}(x^2-6x+1)$;

г) $u(x)=\frac{1}{3}(-16x^2+37x+26)$, $v(x)=\frac{1}{3}(16x^3-53x^2-37x-23)$;

д) $u(x)=-20x^3+70x^2-84x+35$, $v(x)=20x^3+10x^2+4x+1$;

е) $u(x)=1+\frac{m}{1}(1-x)+\frac{m(m+1)}{1.2}(1-x)^2+\cdots$

$\cdots+\frac{m(m+1)\ldots(m+n-2)}{1.2\ldots(n-1)}(1-x)^{n-1}$,

$v(x)=1+\frac{n}{1}x+\frac{n(n+1)}{1.2}x^2+\ldots+\frac{n(n+1)\ldots(n+m-2)}{1.2\ldots(m-1)}x^{m-1}$.

14. Под *най-малко общо кратно* на полиномите $f(x)$ и $g(x)$ разбираме полином $m(x)$, който притежава свойствата:

(I) $m(x)$ се дели на $f(x)$ и на $g(x)$;

(II) всеки полином $M(x)$, който се дели на $f(x)$ и на $g(x)$, се дели и на $m(x)$. Докажете, че всеки два полинома притежават еднозначно определено, с точност до ненулев множител, най-малко общо кратно и е в сила равенството

$$m(x)=\frac{f(x)\,g(x)}{d(x)},\quad \text{където}\quad d(x)=(f(x),\,g(x)).$$

15. Намерете най-малкото общо кратно на полиномите $f(x)$ и $g(x)$, където:

а) $f(x)=x^4+x^3-x^2+x-2$, $g(x)=x^4-2x^3+2x^2-2x+1$;
б) $f(x)=2x^4-5x^3+x^2-10x-6$, $g(x)=x^4-7x^2-18$.

Отг. а) $m(x)=x^5-2x^3+2x^2-3x+2$;
б) $m(x)=2x^5+x^4-14x^3-7x^2-36x-18$.

16. Нека $f(x)$ е полином с коефициенти от дадено поле P и α, β са елементи от P. Намерете остатъка от делението на полинома $f(x)$ с полинома $(x-\alpha)(x-\beta)$.

Отг. $r(x)=\frac{f(\alpha)-f(\beta)}{\alpha-\beta}x+\frac{\alpha f(\beta)-\beta f(\alpha)}{\alpha-\beta}$,

при $\alpha\neq\beta$ и $r(x)=f'(\alpha)x-f(\alpha)-\alpha f'(\alpha)$ при $\beta=\alpha$.

17. Определете кратността на корена α за полинома $f(x)$, където:

а) $\alpha=2$, $f(x)=x^5-5x^4+7x^3-2x^2+4x-8$;

б) $\alpha=-2$, $f(x)=x^5+7x^4+16x^3+8x^2-16x-16$;

в) $\alpha=1$, $f(x)=x^{2n+1}-(2n+1)x^{n+1}+(2n+1)x-1$;

г) $\alpha=1$, $f(x)=x^{2n}-n^2x^{n+1}+2(n^2-1)x^n-n^2x^{n-1}+1$.

Отг. а) 3; б) 4; в) 3; г) 4.

18. Определете стойностите на a и b, при които $\alpha=1$ е двукратен корен на полинома $f(x)$, където:

а) $f(x)=ax^4+bx^3+1$;

б) $f(x)=ax^{n+1}+bx^n+1$.

Отг. а) $a=3$, $b=-4$;
б) $a=n$, $b=-n-1$.

19. Намерете условието, при което полиномът x^5+ax^3+b има двоен корен, различен от нула.

Отг. $3125b^2+108a^5=0$; $a\neq 0$

20. Намерете условието, при което полиномът $x^5+10ax^3+5bx+c$ има троен корен, различен от нула.

Отг. $b=9a^2$, $1728a^5+c^2=0$

21. Намерете остатъка от делението на $f(x)$ с $g(x)$ над полето P, където:

а) $f(x)=x^5+3x^4-2x^2-1$, $g(x)=(x-1)^2(x-3)(x-4)$, $P=Q$;

б) $f(x)=2x^6-x^3+7x^2+3x+4$, $g(x)=(x-1)^2(x+2)$, $P=Q$;

в) $f(x)=3x^5+2x^4-3x^3+x^2-1$, $g(x)=(x+2)^3$

и P е полето с 4 елемента от зад. 1, ж).

22. Покажете, че полиномът

$$f(x)=1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}$$

няма кратни корени.

Определение. Ще казваме, че полиномът $f(x)$ е *сравним* с полинома $g(x)$ по модул ненулевия полином $h(x)$, и ще пишем

$$f(x)\equiv g(x)\pmod{h(x)},$$

когато $f(x)-g(x)$ се дели на $h(x)$. (Даденото определение е съгласувано с определението за сравнимост по даден идеал, като тук се има пред вид главният идеал, породен от полинома $h(x)$.)

23. Докажете, че полиномът $x^{3m}+x^{3n+1}+x^{3p+2}$ се дели на x^2+x+1 каквито и да бъдат целите неотрицателни числа m, n и p.

Решение. По модул x^2+x+1 имаме

$$x^3\equiv 1,$$

откъдето

$$x^{3m}+x^{3n+1}+x^{3p+2}\equiv 1+x+x^2.$$

24. При какви стойности на показателя m полиномът $(x+1)^m+x^m+1$ се дели на x^2+x+1?

Отг. $m=6k\pm 2$.

25. При какви условия за m, n и p полиномът $x^{3m}-x^{3n+1}+x^{3p+2}$ се дели на x^2-x+1?

Решение. По модул x^2-x+1 имаме

$$x^3\equiv -1,$$

$$x^{3m}-x^{3n+1}+x^{3p+2}\equiv(-1)^m-(-1)^n x+(-1)^p x^2,$$

откъдето следва, че $(-1)^m=(-1)^n=(-1)^p$, т. е. числата m, n и p трябва да са от еднаква четност.

26. При какви стойности на показателя n полиномът

$$f(x)=(x+1)^n-x^n-1$$

се дели на полинома $g(x)=x^2+x+1$?

Решение. По модул x^2+x+1 имаме

$$x+1\equiv -x^2 \text{ и } x^3\equiv 1,$$

откъдето

$$(x+1)^n-x^n-1\equiv(-1)^n x^{2n}-x^n-1.$$

Нека $n=3k+i$, $i=0, 1, 2$. Тогава

$$(x+1)^n-x^n-1\equiv(-1)^n x^{2i}-x^i-1.$$

При $i=0$, $f(x)\equiv(-1)^n-1-1\neq 0$.

При $i=1$, $f(x)\equiv(-1)^n x^2-x-1$, откъдето $f(x)\equiv 0$, когато $(-1)^n=-1$, т. е. когато числото $n=3k+1$ е нечетно.

При $i=2$, $f(x)\equiv(-1)^n x^4-x^2-1\equiv(-1)^n x-x^2-1$, откъдето $f(x)\equiv 0$, когато числото $n=3k+2$ е нечетно.

Следователно полиномът $f(x)$ се дели на полинома $g(x)$ тогава и само тогава, когато $n=6s\pm 1$.

Полученият резултат е валиден за всяко поле с характеристика $p\neq 2, 3$. Лесно се вижда, че в случая, когато полиномите $f(x)$ и $g(x)$ се разглеждат над поле с характеристика 2 или 3, за n имаме $n\not\equiv 0 \pmod 3$, съответно $n=6s\pm 1$ или $n=6s+3$.

27. Намерете стойностите на показателя n, при които полиномът

$$f(x)=x^{4n}-x^{3n}+x^{2n}-x^n+1$$

се дели на полинома $g(x)=x^4-x^3+x^2-x+1$.

Решение. По модула $x^4-x^3+x^2-x+1$ имаме $x^5\equiv-1$. Нека $n=5k+i$, $i=0, 1, 2, 3, 4$. Тогава

$$f(x)\equiv x^{4i}-(-1)^{3k}x^{3i}+x^{2i}-(-1)^k x^i+1.$$

а) При $i=0$ имаме $f(x)\equiv 1-(-1)^{3k}+1-(-1)^k+1\not\equiv 0$.

б) При $i=1$ имаме $f(x)\equiv x^4-(-1)^{3k}x^3+x^2-(-1)^k x+1$.

Очевидно $f(x)\equiv 0$ тогава и само тогава, когато $(-1)^{3k}=(-1)^k=1$, т. е. $k=2s$ отkъдето $n=10s+1$.

в) При $i=2$ имаме $f(x)\equiv -x^3+(-1)^{3k}x+x^4-(-1)^k x^2+1$.

Очевидно $f(x)\equiv 0$ тогава и само тогава, когато $(-1)^{3k}=(-1)^k=-1$, т. е. $k=2s+1$, отkъдето $n=10s+7$.

г) При $i=3$ имаме $f(x)\equiv x^2+(-1)^{3k}x^4-x-(-1)^k x^3+1$.

Очевидно $f(x)\equiv 0$ тогава и само тогава, когато $(-1)^{3k}=(-1)^k=1$, т. е. $k=2s$, отkъдето $n=10s+3$.

д) При $i=4$ имаме $f(x)\equiv -x-(-1)^{3k}x^2-x^3-(-1)^k x^4+1$.

Очевидно $f(x)\equiv 0$ тогава и само тогава, когато $(-1)^{3k}=(-1)^k=-1$, т. е. когато $k=2s+1$, отkъдето получаваме $n=10s+9$.

И така $f(x)$ се дели на $g(x)$ тогава и само тогава, когато n е нечетно число, неделящо се на 5.

Полученият резултат е валиден за всяко поле с характеристика $p\neq 2, 3, 5$. Разгледайте отделно случаите на поле с характеристика 2, 3 и 5.

28. Намерете стойностите на показателя n, при които полиномът $f(x)=(x+1)^n-x^n-1$ се дели на полинома $g(x)=(x^2+x+1)^2$ при предположение, че основното поле има характеристика 0.

Решение. За да се дели $f(x)$ на $g(x)$, е необходимо и достатъчно да са изпълнени сравненията $f(x)\equiv 0\,(x^2+x+1)$ и $f'(x)\equiv 0\,(x^2+x+1)$. Съгласно зад. 26 първото сравнение е изпълнено тогава и само тогава, когато $n=6s+1$. При $n=6s+1$ имаме

$$f'(x)=n(x+1)^{n-1}-nx^{n-1}\equiv n(-1)^{n-1}x^{2n-2}-nx^{n-1}\equiv 0\,(x^2+x+1),$$

понеже $x^{n-1}\equiv x^{6s}=(x^3)^{2s}\equiv 1$. При $n=6s-1$ имаме

$$f'(x)\equiv(-1)^{6s-2}x^{2(6s-2)}-x^{6s-2}=x^{12s-4}-x^{6s-2}\equiv x^8-x^4\equiv x^2-x\not\equiv 0\,(x^2+x+1)$$

И така търсените стойности на n са от вида $n=6s+1$.

29. Намерете стойностите на показателя m, при които полиномът $f(x)$ се дели на полинома $g(x)$ при предположение, че основното поле има характеристика 0:

а) $f(x)=x^{2m}+x^m+1$, $g(x)=x^2+x+1$;

б) $f(x)=(x+1)^m-x^m-1$, $g(x)=x^2+x+1$;

в) $f(x)=(x+1)^m+x^m+1$, $g(x)=(x^2+x+1)^2$;

г) $f(x)=(x+1)^m-x^m-1$, $g(x)=(x^2+x+1)^3$.

Отг. а) $m\not\equiv 0 \pmod 3$;
б) $m=6s\pm 1$;
в) $m=6s+4$;
г) при никое m.

30. При какво условие за m, n и p полиномът $f(x)=x^{3m}+x^{3n+1}+x^{3p+2}$ се дели на полинома $g(x)=x^4+x^2+1$.

Отг. $m\equiv p\equiv n+1 \pmod 2$.

31. Нека p е цяло число. Докажете, че полиномът

$$f(x)=x^{n_1}+x^{n_2}+\dots+x^{n_p}$$

се дели на полинома $g(x)=1+x+x^2+\dots+x^{p-1}$ тогава и само тогава, когато $n_i \not\equiv n_j \pmod p$ при $i \neq j$.

Решение. Нека r_i е остатъкът на n_i по модул p. Тогава имаме

$$f(x)\equiv x^{r_1}+x^{r_2}+\dots+x^{r_p} \pmod{g(x)},$$

понеже $x^p \equiv 1 \pmod{g(x)}$. Тъй като степента на полинома $x^{r_1}+x^{r_2}+\dots+x^{r_p}$ е строго по-малка от p, сравнението $x^{r_1}+x^{r_2}+\dots x^{r_p}\equiv 0 \pmod{g(x)}$ е изпълнено тогава и само тогава, когато полиномът от лявата страна на сравнението съвпада с $g(x)$. Последното условие означава точно, че остатъците r_i са два по два различни т. е. $n_i \not\equiv n_j$ mod p) при $i \neq j$.

32. Докажете, че ако полиномът $f(x)=f_1(x^3)+xf_2(x^3)$ се дели на x^2+x+1, то $f_1(x)$ и $f_2(x)$ се делят на $x-1$.

33. Намерете най-големия общ делител на полиномите

$$f(x)=x^n-1 \text{ и } g(x)=x^m-1.$$

Решение. Нека $\delta=(n, m)$, $d(x)=(f(x), g(x))$ и $\varphi(x)=x^\delta-1$. Ще покажем, че $d(x)=\varphi(x)$. Очевидно $\varphi(x) \mid f(x)$ и $\varphi(x) \mid g(x)$, откъдето $\varphi(x) \mid d(x)$. Обратно, нека u и v са цели числа, така че $un+vm=\delta$, и нека за определеност да предположим, че $u>0$, $v<0$. Имаме сравненията $x^n\equiv 1 \pmod{d(x)}$ и $x^m\equiv 1 \pmod{d(x)}$, откъдето $x^{un}\equiv 1 \pmod{d(x)}$ и $x^{-vm}\equiv 1 \pmod{d(x)}$. От второто получаваме $x^{\delta}\cdot x^{-vm}\equiv x^\delta \pmod{d(x)}$. Но $\delta-vm=un$, следователно $x^\delta\equiv 1 \pmod{d(x)}$, т. е. $d(x) \mid \varphi(x)$, с което твърдението е доказано.

34. Намерете най-големия общ делител на полиномите x^n+a^n и x^m+a^m.

Отг. x^d+a^d, ако $\frac{n}{d}$ и $\frac{m}{d}$ са нечетни ($d=(n, m)$); 1 в противен случай.

35. Докажете, че ако полиномът $f(x^n)$ се дели на $x-1$, той се дели и на x^n-1.

36. Докажете, че ако полиномът $f(x^n)$ се дели на $(x-a)^k$, той се дели и на $(x^n-a^n)^k$ при $a \neq 0$.

37. Нека $f(x)$ и $g(x)$ са полиноми. Покажете, че ако $f(x)$ се дели на $(x-a)^k$ ($k \geq 1$) и $g'(a) \neq 0$, то $f(g(x))$ се дели и на $(g(x)-g(a))^k$.

38. Нека P е поле. Покажете, че съществуват безбройно много неразложими полиноми с коефициенти в P. В частност, ако полето P е крайно, съществуват полиноми с произволно високи степени.

Доказателство (Евклид). Нека $p_1(x)$, $p_2(x)$, ..., $p_n(x)$ са неразложими полиноми. Образуваме полинома

$$p_1(x)p_2(x)\dots p_n(x)+1.$$

Този полином има поне един неразложим делител $p(x)$ и очевидно $p(x) \neq p_i(x)$ за $i=1, 2, \dots, n$.

39. Покажете, че един полином от трета степен или е неразложим, или има корен в основното поле.

40. Намерете всички неразложими над Z_5 полиноми от вида $3x^2+cx+4$.

Отг. $3x^2+4$, $3x^2+x+4$, $3x^2+4x+4$.

41. Разложете на неразложими множители полиномите:

а) x^2+1 над Z_5;

б) $3x^3+4x^2+3$ над Z_5;

в) x^4-1 над Z_{11};

г) x^4-1 над Z_{13}.

Отг. а) $(x+2)(x+3)$;
б) $(x+2)^2(3x+2)$;
в) $(x+10)(x+1)(x^2+1)$;
г) $(x+1)(x+5)(x+8)(x+12)$.

42. Нека p е просто число. Покажете, че броят на неразложимите над Z_p полиноми от вида x^3+ax^2+bx+c $(a, b, c \in Z_p)$ е равен на $\frac{1}{3}p(p-1)(p+1)$.

43. Нека $f(x)=a_0+a_1x+\cdots+a_nx^n$ е полином над полето Z_p (p—просто). Да означим с $\bar{f}(x)$ полинома

$$\bar{f}(x)=a_0x+a_1x^p+\cdots+a_nx^{p^n}.$$

Покажете, че за два полинома $f(x)$ и $g(x)$ $g(x)$ дели $f(x)$ тогава и само тогава, когато $\bar{g}(x)$ дели $\bar{f}(x)$.

Упътване. Покажете, че $\overline{f(x)+g(x)}=\bar{f}(x)+\bar{g}(x)$ и $\overline{f(x)g(x)}=\bar{f}(x)\bar{g}(x)$.

44. Един полином $f(x)\in Z_p[x]$ се нарича *адитивен*, когато $f(\alpha+\beta)=f(\alpha)+f(\beta)$ за произволни $\alpha, \beta \in Z_p$. Покажете, че един полином $f(x)$ е адитивен тогава и само тогава, когато има вида

$$f(x)=a_0x+a_1x^p+\cdots+a_nx^{p^n}.$$

45. Покажете, че множеството R от всички адитивни полиноми над Z_p е куматативен пръстен относно обичайното събиране и умножението, дефинирано чрез равенството

$$f(x)\odot g(x)=f(g(x)).$$

Покажете също, че пръстенът R е изоморфен с пръстена $Z_p[x]$ от полиноми на променливата x с коефициенти в Z_p. Коя е единицата на R?

46. Нека P е крайно поле с q елемента и $f(x)$ е полином над P. С $\bar{f}(x)$ да означим остатъка, получен от делението на $f(x)$ с x^q-x. Докажете, че

$$f(a)=g(a)$$

за всяко $a\in P$ тогава и само тогава, когато $\bar{f}(x)=\bar{g}(x)$.

Упътване. Докажете и използувайте твърдението, че алгебрично уравнение не може да има повече корени, отколкото е степента на уравнението. Следователно, ако положим

$$f(x)=(x^q-x)f_1(x)+\bar{f}(x) \quad \text{и} \quad g(x)=(x^q-x)g_1(x)+\bar{g}(x)$$

и използуваме тъждеството $a^q=a$, ще имаме $\bar{f}(x)=\bar{g}(x)$ тогава и само тогава, когато $f(a)=g(a)$.

47. Нека P е поле. Докажете, че са в сила изоморфизмите:

$$P[x]/(x^2-1)\cong P[x]/(x^2-4),$$
$$P[x]/(x^2+1)\cong P[x]/(x^2+2x+2).$$

48. Покажете, че факторпръстенът $Z_2[x]/(x^2+x+1)$ е поле с 4 елемента и съставете таблиците за събиране и умножение в това поле.

49. Има ли неразложими полиноми от втора степен над полето от предната задача?

50. Покажете, че факторпръстенът $Z_3[x]/(x^2+1)$ е поле с 9 елемента, и съставете таблиците за събиране и умножение в това поле.

51. Покажете, че няма полиноми от втора степен, които да са неразложими над полето от предната задача. В частност разложете на множители полиномите:

а) x^2+1;
б) x^2+x+2;
в) $2x^2+x+1$.

Отг. а) $(x+i)(x+2i)$;
б) $(x+i+2)(x+2i+2)$;
в) $(x+i+1)(2x+i+2)$, където $i=\bar{x}\in Z_3[x]/(x^2+1)$.

52. Докажете, че в пръстена $P[x]$ от полиноми на една променлива над дадено поле P всеки идеал е главен.

Решение. Нека I е идеал в $P[x]$. Без ограничение на общността можем да предполагаме, че $I\neq(0)$. Нека $p(x)$ е ненулев елемент от I от възможно най-малка степен n. С $f(x)$ да означим произволен елемент от I. Да разделим полинома $f(x)$ на $p(x)$ и нека $q(x)$ и $r(x)$ са съответно частното и остатъкът. От равенството $f(x)=q(x)p(x)+r(x)$ следва, че $r(x)\in I$. Ако $r(x)\neq 0$, степента на $r(x)$ е $<n$, което обаче противоречи на избора на $p(x)$. Следователно $r(x)=0$, т. е. $f(x)=p(x)q(x)$ принадлежи на главния идеал $(p(x))$. По такъв начин показахме, че $I\subset(p(x))$. Обратното включване е очевидно. И така $I=(p(x))$.

53. Като използувате резултата от предната задача, докажете съществуването на най-голям общ делител $d(x)$ на произволна система от краен брой полиноми $f_1(x), f_2(x), \ldots, f_k(x)$, т. е. такъв полином $d(x)$, който е общ делител на дадените полиноми и се дели на всеки друг техен общ делител. Докажете, че полиномът $d(x)$ може да се представи във вида

$$d(x)=u_1(x)f_1(x)+u_2(x)f_2(x)+\cdots+u_k(x)f_k(x), \tag{1}$$

където $u_1(x), u_2(x), \ldots, u_k(x)$ са полиноми на x.

Решение. Разглеждаме идеала $I=(f_1(x))+(f_2(x))+\ldots+(f_k(x))$. Съгласно предната задача I е главен идеал. Нека $I=(d(x))$. Очевидно $(f_i(x))\subset I$, т. е. $d(x)$ дели $f_i(x)$ при всяко $i=1, 2, \ldots, k$. Понеже $d(x)\in I$, ще бъде в сила равенството (1). От последното равенство се вижда, че всеки общ делител на дадените полиноми е делител и на $d(x)$.

54. Докажете, че ако полиномите $f(x)$ и $g(x)$ са взаимно прости и $f(x)$ дели произведението $g(x)h(x)$, то $f(x)$ дели $h(x)$.

Решение. Понеже полиномите $f(x)$ и $g(x)$ са взаимно прости, т. е. техният най-голям общ делител е равен на 1, ще бъде в сила равенство от вида

$$u(x)f(x)+v(x)g(x)=1,$$

където $u(x)$ и $v(x)$ са полиноми на x. Като умножим двете страни на последното равенство с $h(x)$, получаваме

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

откъдето твърдението на задачата следва непосредствено.

55. Нека $p(x)$ е неразложим полином. Докажете, че полиномът е взаимно прост с даден полином $g(x)$ тогава и само тогава, когато $g(x)$ не се дели на $p(x)$.

56. Докажете, че ако неразложимият полином $p(x)$ дели произведението $g(x)h(x)$ на полиномите $g(x)$ и $h(x)$, то $p(x)$ дели поне един от множителите.

Решение. Твърдението следва непосредствено от предните две задачи. Ще приведем директно доказателство на това важно твърдение. Да допуснем, че твърдението не е вярно и нека $g(x)$ е полином от възможно най-малка степен и такъв, че за някой полином $h(x)$ да имаме: $p(x)$ дели $g(x)h(x)$, $p(x)$ не дели $g(x)$ и $p(x)$ не дели $h(x)$. Като разделим $p(x)$ на $g(x)$, ще получим $p(x)=g(x)q(x)+r(x)$, където $q(x)$ и $r(x)$ са съответно частното и остатъкът при това деление. Ако $r(x)=0$, ще имаме $p(x)=g(x)q(x)$ и понеже полиномът $p(x)$ е неразложим, полиномите $p(x)$ и $g(x)$ ще съвпадат с точност до константен множител. Последното обаче противоречи на предположението, че $p(x)$ не дели $g(x)$. И така остатъкът $r(x)$ е различен от нула. От очевидното равенство $p(x)h(x)=g(x)q(x)h(x)+r(x)h(x)$ следва, че $p(x)$ дели $r(x)h(x)$. Така достигнахме до противоречие с избора на полинома $g(x)$, понеже степента на остатъка $r(x)$ е по-малка от тази на $g(x)$ и $p(x)$ не дели $r(x)$.

57. Докажете, че ако полиномите $g(x)$ и $h(x)$ са взаимно прости и полиномът $f(x)$ се дели на $g(x)$ и на $h(x)$, то $f(x)$ се дели на произведението $g(x)h(x)$.

58. Като използувате предните задачи, докажете теоремата за еднозначно разлагане на полиноми на неразложими множители.

59. Нека f и g са полиноми с коефициенти в някакво поле P и

$$f=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}, \qquad g=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$$

са техните разлагания на неразложими множители. Покажете, че са в сила равенствата

$$(f, g)=p_1^{min(\alpha_1, \beta_1)}\dots p_n^{min(\alpha_n, \beta_n)}, \quad [f, g]=p_1^{max(\alpha_1, \beta_1)}\dots p_n^{max(\alpha_n, \beta_n)}.$$

(Тук някои от показателите α_i, β_i могат да са 0.)]

60. Покажете, че в пръстена от полиноми $P[x]$ са в сила следните равенства:

$$(f)+(g)=((f, g)), \qquad (f)\cap(g)=([f, g]).$$

61. Покажете, че в пръстена от полиноми $P[x]$ един идеал е максимален тогава и само тогава, когато има вида (p), където p е неразложим полином.

62. Опишете всички прости идеали в пръстена от полиноми $P[x]$.

Отг. Нулевият идеал е прост. Освен него други прости са само максималните.

63. Нека $f\in P[x]$ и $f=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$ е разлагането на p на неразложими множители. Покажете, че радикалът (зад. 29, § 2 гл. VII) $r((f))$ на идеала (f) съвпада с $(p_1 p_2 \dots p_n)$. Кои са минималните прости идеали, които съдържат (f)?

64. Нека $f\in P[x]$ и $f=p_1^{\alpha_1}\dots p_n^{\alpha_n}$ е разлагането на неразложими множители. Докажете, че е в сила изоморфизъм

$$P[x]/(f)\cong\prod_{i=1}^{n} p[x]/(p_i^{\alpha_i}).$$

Упътване. Вж. зад. 62, § 2, гл. VII.

65. Нека $p\in P[x]$ е неразложим полином. Опишете нилпотентните елементи в $P[x]/(p^n)$.

Отг. Нилрадикалът (зад. 25, § 2, гл. VII) на $p[x]/(p^n)$ съвпада с $(p)/(p^n)$.

В следващите няколко задачи се разглеждат полиноми с коефициенти в произволен комутативен пръстен с единица R. Пръстенът $R[x]$, от полиноми с коефициенти в R, се дефинира по същия начин, както и в случая, когато R е поле (вж. уводните бележки към този параграф). Както и в случая на поле, елементите на R се отъждествяват с полиномите от нулева степен и можем да считаме, че $R\subset R[x]$. При това единицата на R се оказва и единица на $R[x]$. По-нататък, ако S е подпръстен на R, имаме $S[x]\subset R[x]$.

66. Нека R е комутативен пръстен с единица и I е идеал в R. Покажете, че $I[x]$ е идеал в $R[x]$ и

$$R[x]/I[x]\cong(R/I)[x].$$

67. Нека r е комутативен пръстен с единица. Покажете, че $R[x]$ е пръстен без делители на нулата тогава и само тогава, когато R е без делители на нулата.

68. Усилете твърдението от предишната задача, като покажете, че един елемент $f\in R[x]$ е делител на нулата в $R[x]$ тогава и само тогава, когато съществува $c\in R$, $c\neq 0$, така че $cf=0$.

Решение. Нека $g\in R[x]$, $g\neq 0$ е такъв, че $gf=0$. Да положим $f(x)=\sum_{\nu=0}^{m}a_\nu x^\nu$ и $g(x)=\sum_{\nu=0}^{n}b_\nu x^\nu$. Сега, ако степента n на g е нула, твърдението е доказано. В случай че $n>0$, ще покажем, че съществува такъв $h\in R[x]$, $h\neq 0$, че $hg=0$ и степента на h не надминава $n-1$. Действително първо, ако $b_0=0$, g може да се представи във вид $g=xh$, където h е от степен $n-1$ и очевидно $xhf=0$. Но понеже x не е делител на нулата, получаваме $hf=0$. Нека сега $b_0\neq 0$. Да допуснем, че за всяко i, $a_ig=0$ е изпълнено. В такъв случай ще имаме $a_jb_i=0$ за всяко i, j и кой да е ненулев коефициент на g може да се вземе за h. Нека сега $a_ig\neq 0$ за някое i и нека p е най-малкият индекс с това свойство. В такъв случай $a_pb_0=0$. Действително нека $f(x)=\varphi(x)+x^p\psi(x)$, където $\varphi(x)=\sum_{\nu=0}^{p-1}a_\nu x^\nu$, $\psi(x)=\sum_{\nu=0}^{m-p}a_{p+\nu}x^\nu$. Имаме $\varphi g=0$ и следователно $x^p\psi g=0$. Но понеже x^p не е делител на нулата, $\psi g=0$; в частност и свободният член на ψg е нула, а той е точно a_pb_0. Сега да разгледаме полинома $a_p(g-b_0)$. Той е ненулев, защото $a_p(g-b_0)=a_pg-a_pb_0=a_pg$. Освен това той е без свободен член, т. е. има вида xh, където степента на h не надминава $n-1$. Накрая $hf=0$, защото

$$xhf=a_p(g-b_0)f=a_pgf-a_pb_0f=0.$$

Ясно е, че като продължаваме така няколко пъти, ще достигнем до равенство от вида $fc=0$, където $c\in R$, $c\neq 0$.

69. Нека R е комутативен пръстен с единица. Докажете, че един полином $f\in R[x]$ е нилпотентен тогава и само тогава, когато коефициентите му са нилпотентни, с други думи, нилрадикалът (зад. 25, § 2, гл. VII) на $R[x]$ съвпада с $N[x]$, където N е нилрадикалът на R. В частност пръстенът $R[x]$ няма нилпотенти (различни от 0) тогава и само тогава, когато R няма нилпотенти.

Решение. Ако $a\in R$ е нилпотентен, очевидно и всеки полином от вида ax^k е нилпотентен и понеже сума на нилпотенти е пак нилпотент, ясно е, че ако коефициентите на f са нилпотентни, то и f е нилпотентен. Обратно, нека f

е нилпотентен. Ще разсъждаваме индуктивно по степента n на f. При $n=0$ твърдението е ясно. Нека $n>0$ и нека $f^N=0$. Свободният член на полинома f^N е точно a^N, където a е свободният член на f. Следователно $a^N=0$, т. е. a е нилпотентен. Да разгледаме полинома $f-a=xh$. Като разлика на нилпотенти той е нилпотентен и понеже x не дели нулата, следва, че h е нилпотент. Но степента на h е $n-1$, следователно всички коефициенти на h са нилпотенти, с което твърдението е доказано.

70. Нека R е област на цялостност. Покажете, че единствените обратими елементи в пръстена $R[x]$ са обратимите елементи на R.

Упътване. В случая, когато пръстенът от коефициенти е област, степента на произведение на два полинома е сборът от степените им.

71. Нека R е област на цялостност. Покажете, че радикалът на Джекобсън (§ 2, гл. VII) на пръстена $R[x]$ е нулев.

Упътване. Използувайте предната задача.

72. Нека R е комутативен пръстен с единица и f, g са два полинома с коефициенти в R. Предполагаме, че старшият коефициент на полинома g е обратим елемент в пръстена R. Покажете, че съществуват еднозначно определени полиноми q, r, така че:

I. $f=q.g+r$.

II. $r=0$ или $r\neq 0$ и степента на r е по-малка от степента на g.

Решение. За простота ще предположим, че старшият коефициент на g е единица. Разглеждаме множеството от всички полиноми от вида $f-q.g$. Ако измежду тях е и нулевият полином, съществуването на q и r е доказано. В противен случай избираме в това множество полином r с най-малка възможна степен. По дефиниция имаме $f=q.g+r$ и остава да докажем, че степента m на r е по-малка от степента n на g. Ако това не е така, полиномът $r-ax^{m-n}g$, където a е старшият коефициент на r, ще има степен, по-малка от m. Освен това той има вида $f-q_1g$ с $q_1=q-axg$, което противоречи на избора на r. С това съществуването на q и r е доказано.

Остава да покажем единствеността на q и r. Наистина от равенствата $f=q_1g+r_1$ и $f=q_2g+r_2$ следва $(q_1-q_2)g=r_1-r_2$. Но това равенство е невъзможно при $q_1-q_2\neq 0$, защото в такъв случай отдясно стои полином, чиято степен не надминава $n-1$, а отляво такъв, чиято степен е поне n (тук използуваме предположението за старшия коефициент на g). Следователно $q_1-q_2=0$, откъдето и $r_1-r_2=0$.

73. Нека p е просто число. Покажете, че в пръстена $Z[x]$, където Z е пръстенът на целите числа, идеалът (x, p) не е главен. Покажете също, че този идеал е максимален. Покажете, че идеалът (p) е прост, но не е нито нулев, нито максимален. (Сравнете със зад. 52 и зад. 61.)

74. Нека P е поле. Покажете, че в пръстена от полиноми $P[x]$ един идеал е примарен тогава и само тогава, когато е степен на прост идеал, т. е. когато има вида (p^n) или (0), където p е неразложим полином. Напротив, покажете, че в пръстена $Z[x]$ идеалът (x^2, p) е примарен, но не е степен на прост идеал.

Решение. Ще докажем само второто твърдение. Нека $I=(x^2, p)$ и $P=(p, x)$. Съгласно предната задача идеалът p е прост. От $I\subset P$ следва $r(I)\subset r(P)=$

$=P$. От друга страна, $P^2 \subset I$, откъдето $P \subset r(I)$. Следователно $r(I)=P$. И така радикалът на I е простият идеал P, откъдето I е примарен. Но I не може да бъде степен на прост идеал, защото този прост идеал непременно трябва да е P, а както лесно се вижда, $I \neq P^k$ за $k=1, 2, \ldots, n, \ldots$

§ 2. ПОЛЕ НА РАЗЛАГАНЕ

Теорема. Нека

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

е произволен полином от степен $n \geq 1$ с коефициенти от дадено поле P. Съществува разширение $F \supset P$ на полето P, такова, че уравнението $f(x)=0$ има поне един корен в F.

Следствие. В подходящо разширение на полето P полиномът $f(x)$ се разлага на линейни множители:

$$f(x)=a_0(x-x_1)(x-x_2)\ldots(x-x_n).$$

Определение. Минималното поле, в което полиномът $f(x)$ се разлага на линейни множители, е еднозначно определено с точност на изоморфизъм и се нарича *поле на разлагане* на $f(x)$.

Обединявайки еднаквите линейни множители, съответствуващи на кратните корени, можем да пишем

$$f(x)=a_0(x-x_1)^{k_1}(x-x_2)^{k_2}\ldots(x-x_r)^{k_r},$$

където $x_1, x_2, \ldots, x_r$ са различните корени на уравнението $f(x)=0$ съответно от кратности $k_1, k_2, \ldots, k_r$ и $k_1+k_2+\ldots+k_r=n$. Горното представяне на полинома $f(x)$ е еднозначно определено.

Следствие. Уравнението от n-та степен $f(x)=0$ има най-много n корена.

Принцип за сравняване на коефициентите. Ако два полинома от степени $\leq n$ приемат съответно равни стойности за повече от n различни стойности на аргумента, то тези полиноми съвпадат.

Интерполационна формула на Лагранж. Нека $x_1, x_2, \ldots, x_n$ са n различни елемента от полето P и $y_1, y_2, \ldots, y_n$ са произволни елементи от P. Съществува еднозначно определен полином $f(x) \in P[x]$ от степен $\leq n-1$ (или нулевия полином), такъв, че

$$f(x_1)=y_1, f(x_2)=y_2, \ldots, f(x_n)=y_n$$

и този полином се определя от формулата

$$f(x)=\sum_{k=1}^{n}\frac{\omega(x)}{x-x_k}\cdot\frac{y_k}{\omega'(x_k)},$$

където $\omega(x)=(x-x_1)(x-x_2)\ldots(x-x_n)$.

Формули на Виет. Ако $x_1, x_2, \ldots, x_n$ са всичките корени на уравнението

$$a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n=0,$$

то

$$x_1+x_2+\ldots+x_n=-\frac{a_1}{a_0},$$

$$x_1x_2+x_1x_3+\ldots+x_{n-1}x_n=\frac{a_2}{a_0},$$

$$x_1x_2x_3+x_1x_2x_4+\ldots+x_{n-2}x_{n-1}x_n=-\frac{a_3}{a_0},$$

. . . .

$$x_1x_2\ldots x_n=(-1)^n\frac{a_n}{a_0}.$$

Горните формули, изразяващи връзките между корените и коефициентите на уравнението, се наричат **формули на Виет**. Лявата страна на k-тата формула на Виет съдържа $\binom{n}{k}$ на брой събираеми, представляващи всевъзможните произведения от корените, взети като комбинации на n елемента от k-ти клас.

Пример. От формулите на Виет при $x_1=x_2=\ldots=x_n=a$ получаваме известната формула за нютоновия бином

$$(x+a)^n=x^n+\binom{n}{1}x^{n-1}a+\binom{n}{2}x^{n-2}a^2+\ldots+\binom{n}{n-1}xa^{n-1}+a^n.$$

Когато полиномът $f(x)\in P[x]$ е неразложим над полето P, пръстенът $P[x]/(f(x))$ (факторпръстенът на $P[x]$ по модул $f(x)$) е поле, в което уравнението $f(x)=0$ има корен.

Едно поле се нарича *алгебрически затворено*, когато всяко алгебрично уравнение с коефициенти от това поле има корен в него.

Теорема. Всяко поле може да се вложи в алгебрически затворено поле.

1. Намерете условието, при което между корените x_1, x_2, x_3 на уравнението

$$x^3+px^2+qx+r=0$$

съществува зависимостта $x_1+x_2=x_3$.

Решение. Съгласно първата формула на Виет имаме

$$x_1+x_2+x_3=-p$$

и като вземем пред вид още равенството $x_1+x_2=x_3$, получаваме $x_3=-\frac{p}{2}$.

Заместваме x_3 в даденото уравнение и като приравним към нула, получаваме търсеното условие:

$$\left(-\frac{p}{2}\right)^3+p\left(-\frac{p}{2}\right)^2+q\left(-\frac{p}{2}\right)+r=0$$

или все едно

$$p^3-4pq+8r=0.$$

2. Намерете условието, при което корените на уравнението

$$x^3+px^2+qx+r=0$$

образуват аритметична прогресия.

Отг. $2p^3-9pq+27r=0.$

3. Намерете условието, при което корените на уравнението

$$x^3+px^2+qx+r=0$$

образуват геометрична прогресия.

Отг. $q^3-p^3r=0.$

4. Намерете условието, при което между корените x_1, x_2, x_3 на уравнението

$$x^3+px^2+qx+r=0$$

съществува зависимостта $x_1x_2=x_3$.

Отг. $(q-r)^2+(1-p)^2r=0.$

5. Намерете условието, при което сборът на два от корените на уравнението

$$x^4+px^3+qx^2+rx+s=0$$

е равен на дадена константа a.

Отг. $(p+2a)^2s=(a^3+a^2p+aq+r)(a^3+2a^2p+ap^2+aq+pq+r)$

6. Намерете стойностите на параметъра λ, при които между корените x_1, x_2, x_3 на уравнението

$$x^3+2x^2+x+\lambda=0$$

съществува зависимостта $x_1^2+x_2^2=x_3$.

Решение. Съгласно формулите на Виет имаме

$$x_1+x_2+x_3=-2,$$
$$x_1x_2+x_1x_3+x_2x_3=1,$$
$$x_1x_2x_3=-\lambda.$$

Като повдигнем първото равенство в квадрат, получаваме

$$x_1^2+x_2^2+x_3^2+2(x_1x_2+x_1x_3+x_2x_3)=4.$$

Оттук, като вземем пред вид второто равенство от формулите на Виет и дадената зависимост между корените, получаваме

$$x_3+x_3^2+2=4, \text{ т. е. } x_3^2+x_3-2=0.$$

За x_3 намираме две стойности 1 и -2 и като заместим тези стойности в даденото уравнение, за λ получаваме двете стойности $\lambda=-4$ и $\lambda=2$. По обратен път или директно се вижда, че при намерените стойности на параметъра λ между корените на уравнението $x^3+2x^2+x+\lambda=0$ наистина съществува указаната в задачата зависимост.

7. Намерете стойностите на параметъра λ, при които между корените на уравнението

$$x^3+2x^2+\lambda x-4=0$$

е в сила връзката $x_1^2+x_2^2=x_3^2$.

Отг. $\lambda=1$, $\lambda=-2$.

8. Намерете стойностите на параметъра λ, при които между два корена x_1 и x_2 на уравнението

$$x^3-5x^2+8x+\lambda=0$$

съществува зависимостта $x_1+x_2=x_1x_2$.

Отг. $\lambda=-6$, $\lambda=-4$

9. Намерете стойностите на параметъра λ, при които между два корена x_1 и x_2 на уравнението

$$x^4-x^3+\lambda x^2-x-6=0$$

съществува зависимостта $x_1+x_2=1$.

Отг. $\lambda-5$.

10. Намерете стойностите на параметъра λ, при които между корените на уравнението

$$x^4+3x^3+6x^2+\lambda x+4=0$$

съществува зависимостта $x_1=\frac{1}{x_2}+\frac{1}{x_3}+\frac{1}{x_4}$.

Отг. $\lambda=8$, $\lambda=10$.

11. Намерете стойностите на параметъра λ, при които между корените на уравнението

$$x^4+2x^3-6x^2+\lambda x+11=0$$

съществува зависимостта $x_1+x_2=x_3+x_4$, т. е. сборът на някои два от корените на уравнението да е равен на сбора на другите два.

12. Намерете стойностите на параметъра λ, при които произведението на някои два от корените на уравнението

$$x^4+4x^3+9x^2+12x+\lambda=0$$

е равно на произведението на другите два.

13. Намерете стойностите на параметъра λ, при които между два корена x_1 и x_2 на уравнението

$$2x^4-5x^3+4x^2+\lambda x-4=0$$

съществува зависимостта $x_1+x_2=x_1x_2$.

14. Намерете стойностите на параметъра λ, при които между два корена на уравнението

$$x^4+x^3-4x^2+\lambda x+1=0$$

съществува зависимостта $x_1+x_2=2x_1x_2$.

15. Намерете при какви стойности на λ уравнението

$$x^4+\lambda x^3+27=0$$

има двоен корен.

Отг. $\lambda=\pm 4$, $\lambda=\pm 4i$.

16. Намерете при кои стойности на λ и μ уравнението

$$x^4-3\lambda x^3+5ix^2+\mu=0$$

има двоен корен, който е равен на сбора на другите два корена.

17. Намерете при кои стойности на λ и μ уравнението

$$x^4+10x^3+\lambda x^2+36x+\mu=0$$

има един двоен корен, който е равен на сбора от реципрочните стойности на другите два корена.

Отг. $\lambda=-35$, $\mu=-12$; $\lambda=-31$, $\mu=12$; $\lambda=5$, $\mu=8$.

18. Намерете при кои стойности на λ и μ уравнението

$$x^4+\lambda x^3+8x^2-8x+\mu=0$$

има два двойни корена.

19. Намерете при кои стойности на λ и μ уравнението

$$x^5+10\lambda x^3+5\mu x+72=0$$

има троен корен.

20. Намерете при кои стойности на λ и μ между корените на уравнението

$$x^4+\lambda x+\mu=0$$

съществуват зависимостите $\begin{cases} x_1x_2+x_3+x_4=1 \\ x_1+x_2+x_3x_4=1 \end{cases}$.

21. Определете λ, μ, ν така, че ако x_1, x_2, x_3 са корените на уравнението

$$x^3+\lambda x^2+\mu x-\lambda-\mu=0,$$

то x_1+x_2, x_2+x_3, x_3+x_1 да са корените на уравнението

$$x^3+\nu x^2+(\mu-\nu)x-\nu=0.$$

Отг. $\lambda=\mu=\nu=0$; $\lambda=-2$, $\mu=-6$, $\nu=-4$.

22. Определете a, b и c така, че те да са корените на уравнението

a) $x^3-ax^2+bx-c=0$;
b) $x^3+ax^2+bx+c=0$.

Отг. а) $b=c=0$, a—произволно; $a=-1$, $b=-1$, $c=1$;

б) $a=b=c=0$; $a=1$, $b=-2$, $c=0$; $a=1$, $b=c=-1$; $b=\lambda$, $a=-\frac{1}{\lambda}$,

$c=\frac{2-\lambda^2}{\lambda}$, където $\lambda^3-2\lambda+2=0$.

23. Съставете уравнение от трета степен с корени x_1, x_2, x_3, така че да са в сила равенствата

$$\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}=-2,\quad \frac{1}{x_1^2}+\frac{1}{x_2^2}+\frac{1}{x_3^2}=1,\quad \frac{1}{x_1^4}+\frac{1}{x_2^4}+\frac{1}{x_3^4}=1.$$

Отг. $5x^3+24x^2+32x+16=0$.

24. Определете a, b, c така, че между корените на уравнението $f(x)=x^3+px+q=0$ да са в сила зависимостите

$$x_2=a+\frac{b}{c+x_1};\quad x_3=a+\frac{b}{c+x_2},\quad x_1=a+\frac{b}{c+x_3}.$$

Решение. Ако съберем почленно трите зависимости, ще имаме

(1) $$3a+b\left(\frac{1}{c+x_1}+\frac{1}{c+x_2}+\frac{1}{c+x_3}\right)=0.$$

Като използуваме тъждеството

$$\frac{f'(x)}{f(x)}=\frac{1}{x-x_1}+\frac{1}{x-x_2}+\frac{1}{x-x_3},$$

получаваме

$$\frac{1}{c+x_1}+\frac{1}{c+x_2}+\frac{1}{c+x_3}=-\frac{f'(-c)}{f(-c)}.$$

Ясно е тогава, че равенството (1) може да се запише във вида

(2) $$3a(c^3+pc-q)+b(3c^2+p)=0.$$

Като се освободим в дадените зависимости от знаменателите, ще имаме

$$\begin{aligned}x_1x_2+cx_2-ax_1&=ac+b,\\ x_2x_3+cx_3-ax_2&=ac+b,\\ x_3x_1+cx_1-ax_3&=ac+b.\end{aligned}$$

Събираме горните равенства почленно и получаваме $p=3(ac+b)$. Умножаваме същите равенства съответно с x_3, x_1, x_2 и отново събираме почленно. Ще имаме

$$-3q+(c-a)p=0,$$

откъдето намираме

$$a=c-\frac{3q}{p}\quad \text{и}\quad b=\frac{p}{3}-c\left(c-\frac{3q}{p}\right).$$

Равенството (2) може да се запише във вида

$$3(ac+b)c^2+3a(pc-q)+bp=0$$

и като заместим $3(ac+b)$ с p и a и b с намерените стойности, за c получаваме квадратното уравнение

$$c^2-\frac{3q}{p}c+\frac{3q^2}{p^2}+\frac{p}{9}=0.$$

И така търсените стойности a, b и c са

$$a=c-\frac{3q}{p},\quad b=\frac{p}{3}-c\left(c-\frac{3q}{p}\right),$$

където c е корен на квадратното уравнение

$$c^2-\frac{3q}{p}c+\frac{3q^2}{p^2}+\frac{p}{9}=0.$$

25. Решете уравнението

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n=0,$$

ако е известно, че корените му образуват аритметична прогресия

Отг. $x_i=-\frac{a_1}{n}+\frac{2i-n-1}{2}h,$

където $h=\frac{1}{n}\sqrt{\frac{12(n-1)a_1^2-24na_2}{n^2-1}}$.

26. Намерете полином от възможно най-ниска степен, който при $x=1, 2, 3, 4$ приема съответно стойности $f(x)=2, 1, 4, 3$.

Отг. $f(x)=-\frac{4}{3}x^3+10x^2-\frac{65}{3}x+15.$

27. Намерете полином от възможно най-ниска степен, който при $x=1, i, -1, -i$ приема съответно стойности $f(x)=1, 2, 3, 4$.

Отг. $f(x)=\frac{1}{2}[5-(1-i)x-x^2-(1+i)x^3].$

28. Намерете полином $f(x)$ от възможно най-ниска степен, за който $f(\omega_k)=k+1$ при $\omega_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$; $k=0, 1, 2, \ldots, n-1$.

Отг. $f(x)=\frac{n+1}{2}-\frac{1}{2}\sum_{k=1}^{n-1}\left[1-i\operatorname{ctg}\frac{k\pi}{n}\right]x^k.$

29. Намерете полином $f(x)$ от степен $\leq n-1$, за който $f(\omega_k)=y_k$, където $\omega_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$, $k=0, 1, 2, \ldots, n-1$.

Пресметнете $f(0)$.

Отг. $f(x)=\frac{1}{n}\sum_{k=0}^{n-1}\frac{y_k(1-x^n)}{1-x\omega_k^{-1}},\quad f(0)=\frac{1}{n}\sum_{k=0}^{n-1}y_k.$

30. Докажете, че ако нулите $x_1, x_2, \ldots, x_n$ на полинома $f(x)$ са различни, то

$$\sum_{i=1}^{n}\frac{x_i^s}{f'(x_i)}=0 \text{ при } 0\leq s\leq n-2.$$

Решение. Съгласно интерполационната формула на Лагранж имаме

$$x^s=\sum_{i=1}^{n}\frac{x_i^s\varphi(x)}{\varphi'(x_i)(x-x_i)}$$

и като сравним коефициентите пред x^{n-1}, получаваме исканото равенство.

31. При означенията от предишната задача пресметнете сбора

$$\sum_{i=1}^{n}\frac{x_i^{n-1}}{\varphi'(x_i)}.$$

Отг. 1.

32. Докажете следната интерполационна формула на Нютон: нека $f(x)$ е полином от степен $n-1$, който за n различни стойности $x_1, x_2, \ldots, x_n$ на променливата x приема n дадени стойности $y_1, y_2, \ldots, y_n$, тогава

$$f(x)=y_1+\alpha_1(x-x_1)+\alpha_2(x-x_1)(x-x_2)+\alpha_3(x-x_1)(x-x_2)(x-x_3)+$$
$$+\ldots+\alpha_{n-1}(x-x_1)(x-x_2)\ldots(x-x_{n-1}),$$

където

$$\alpha_k=\frac{y_1}{(x_1-x_2)\ldots(x_1-x_{k+1})}+\frac{y_2}{(x_2-x_1)\ldots(x_2-x_{k+1})}+\ldots+$$
$$+\frac{y_{k+1}}{(x_{k+1}-x_1)\ldots(x_{k+1}-x_k)}$$

(вж. напр. Н. Обрешков, „Висша алгебра“).

33. В означенията на предната задача покажете, че когато x приема стойностите

$$x_1, x_1+h,\ x_1+2h, \ldots, x_1+(n-1)h,$$

интерполационният полином $f(x)$ приема вида

$$f(x)=f(x_1)+\frac{z}{1}\Delta f(x_1)+\frac{z(z-1)}{2!}\Delta^2 f(x_1)+\ldots+$$
$$+\frac{z(z-1)\ldots(z-n+2)}{(n-1)!}\Delta^{n-1}f(x_1),\ldots,$$

където $x=x_1+zh$ и разликите $\Delta^k f(x)$ се определят от равенствата

$$\Delta f(x)=f(x+h)-f(x),\ \Delta^2 f(x)=\Delta(\Delta f(x)),\ldots,\Delta^k f(x)=\Delta(\Delta^{k-1}f(x)).$$

34. Постройте полином $f(x)$ от възможно най-ниска степен, който при указаните стойности на x приема съответно стойности $f(x)$, съгласно таблицата:

а)

x	0	1	2	$\ldots$	n
$f(x)$	1	2	4	$\ldots$	2^n;

б) $\begin{array}{c|c} x & 0\ 1\ 2 \ldots n \\ \hline f(x) & 1\ a\ a^2 \ldots a^n \end{array}$;

в) $\begin{array}{c|c} x & 1\ 2\ 3 \ldots n \\ \hline f(x) & 1\ \frac{1}{2}\ \frac{1}{3} \ldots \frac{1}{n} \end{array}$.

Отг.

а) $f(x)=1+\frac{x}{1!}+\frac{x(x-1)}{2!}+\ldots+\frac{x(x-1)\ldots(x-n+1)}{n!}$;

б) $f(x)=1+\frac{(a-1)x}{1!}+\frac{(a-1)^2x(x-1)}{2!}+\ldots+\frac{(a-1)^n x(x-1)\ldots(x-n+1)}{n!}$,

в) $f(x)=1-\frac{x-1}{2!}+\frac{(x-1)(x-2)}{3!}-\ldots+(-1)^n\frac{(x-1)(x-2)\ldots(x-n+1)}{n!}=$

$=\frac{n!-(1-x)(2-x)\ldots(n-x)}{n!x}$.

35. Намерете полином $f(x)$ от степен $2n$, който при деление с полинома $x(x-2)\ldots(x-2n)$ дава остатък 1, а при деление с полинома $(x-1)(x-3)\ldots[x-(2n-1)]$ дава остатък -1.

Отг. $f(x)=1-\frac{2x}{1}+\frac{2x(2x-2)}{2!}+\ldots+\frac{2x(2x-2)\ldots(2x-4n+2)}{(2n)!}$.

36. Намерете полином от степен $\leq n-1$, който приема в точките $x_1, x_2, \ldots, x_n$ стойности, съвпадащи съответно със стойностите на функцията $\frac{1}{x-a}$, $a \neq x_i$, $i=1, 2, \ldots, n$.

Отг. $f(x)=\frac{\varphi(a)-\varphi(x)}{\varphi(a)(x-a)}$, където $\varphi(x)=(x-x_1)(x-x_2)\ldots(x-x_n)$.

37. Докажете, че ако полиномът $f(x)$ от степен $k \leq n$ приема цели стойности при $n+1$ последователни цели значения на x, той приема цели стойности за всяко цяло x.

38. Докажете, че полиномът $f(x)$, който приема цели стойности при $x=0, 1, 4, 9, \ldots, n^2$ и е от степен n, приема цели стойности за всяко цяло x, което е точен квадрат.

39. Нека $x_0<x_1<x_2<\ldots<x_n$ са цели числа. Покажете, че всеки полином

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n$$

приема в точките $x_0, x_1, \ldots, x_n$ стойности, поне една от които е по модул $\geq \frac{n!}{2^n}$.

Решение. Нека $g(x)$ е разглежданият полином. Да положим

$$f(x)=(x-x_0)(x-x_1)(x-x_2)\ldots(x-x_n).$$

От тъждеството

$$g(x)=\sum_{\nu=0}^{n}\frac{g(x_\nu)}{f'(x_\nu)}\cdot\frac{f(x)}{x-x_\nu},$$

чрез сравняване на коефициентите пред x^n, получаваме

$$1=\sum_{\nu=0}^{n}\frac{g(x_\nu)}{f'(x_\nu)},$$

откъдето

$$1\leq M\sum_{\nu=0}^{n}\frac{1}{|f'(x_\nu)|},$$

където $M=\max|g(x_\nu)|$. По-нататък имаме

$$|f'(x_\nu)|=|(x_\nu-x_0)(x_\nu-x_1)\dots(x_\nu-x_{\nu-1})(x_\nu-x_{\nu+1})\dots(x_\nu-x_n)|\geq\nu!(n-\nu)!$$

$$\sum_{\nu=0}^{n}\frac{1}{|f'(x_\nu)|}\leq\sum_{\nu=0}^{n}\frac{1}{\nu!(n-\nu)!}=\frac{2^n}{n!}.$$

В следващите няколко задачи се установява съществуване и единственост на алгебрически затворено разширение на дадено поле и на поле на разлагане на даден полином. Във връзка с това ще направим някои предварителни бележки. Нека полето Q е разширение на полето P, т. е. P е подполе на Q. В такъв случай можем да разглеждаме Q като линейно пространство над полето P. Размерността на това пространство наричаме *степен на разширението* Q над P и означаваме с $(Q:P)$. Когато $(Q:P)=n<\infty$, полето Q се нарича крайно разширение на P. Нека $\alpha_1, \alpha_2, \dots, \alpha_n \in Q$; означаваме с $P[\alpha_1,\alpha_2,\dots,\alpha_n]$ (съответно с $P(\alpha_1,\alpha_2,\dots,\alpha_n)$) най-малкия (по отношение на включването) подпръстен (съответно подполе) на Q, който съдържа P и $\alpha_1,\alpha_2,\dots,\alpha_n$. Очевидно $P(\alpha_1,\alpha_2,\dots,\alpha_n)$ е разширение на P. Ако това разширение съвпада с Q, полето Q се нарича *крайно породено разширение* на P. В частност при $Q=P(\alpha)$, $\alpha\in Q$ полето Q се нарича *просто разширение* на P и елементът α — *примитивен* елемент на Q.

Нека $\alpha\in Q$. Елементът α се нарича *алгебричен* над P, когато съществува ненулев полином $g\in P[x]$, така че $g(\alpha)=0$. В противен случай α се нарича *трансцендентен* над P. Нека $\alpha\in Q$ е алгебричен елемент над P. Ясно е, че множеството I от всички полиноми $g\in P[x]$, за които $g(\alpha)=0$, е ненулев идеал в пръстена $P[x]$. Съгласно зад. 52 от § 1 този идеал е главен, т. е. има вида $I=(f)$, където полиномът $f\in P[x]$ е еднозначно определен с нормировката, старшият му коефициент да е равен на 1. Полиномът f ще наричаме *минимален полином на алгебричния елемент* α. От дефиницията е ясно, че ако $g \in P[x]$, равенството $g(\alpha)=0$ е равносилно с $f(x)/g(x)$.

40. Покажете, че минималният полином $f(x)$ на алгебричен елемент $\alpha \in Q$ е неразложим над полето P.

41. Нека $P \subset Q \subset R$ са полета; покажете, че

$$(R:P)=(R:Q)(Q:P).$$

В частност, ако R е крайно разширение на Q и Q е крайно разширение на P, то и R е крайно разширение на P.

Упътване. Покажете, че ако елементите ξ_i образуват базис на Q над P и η_j образуват базис на R над Q, то всевъзможните произведения $\xi_i\eta_j$ образуват базис на разширението R над P.

42. Покажете, че ако $(Q:P)=p$ — просто число, не съществуват разширения на P, които се съдържат в Q (междинни разширения). Покажете още, че Q е просто разширение на P.

43. Покажете, че ако $(Q:P)=2$, то $Q=P(\alpha)$, където $\alpha^2 \in P$.

44. Покажете (в означенията от предишната задача), че при предположение, че P е полето на рационалните числа, примитивният елемент α на квадратичното разширение $Q((Q:P)=2)$ може да се избере цяло число, което не се дели на точни квадрати.

45. Нека Q е разширение на P и $\alpha_i \in Q$. Покажете, че пръстенът $P[\alpha_1, \alpha_2, \ldots, \alpha_n]$ се състои от всички елементи на Q, които могат да се представят във вида $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$, където $f(x_1, x_2, \ldots, x_n)$ е произволен полином на $x_1, x_2, \ldots, x_n$ с коефициенти от P. В частност пръстенът $P[\alpha]$ се състои от всички елементи $f(\alpha)$, където $f \in P[x]$.

46. В означенията от предната задача покажете, че разширението $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ съвпада с полето от частни на пръстена $P[\alpha_1, \alpha_2, \ldots, \alpha_n]$ и се състои от всички елементи на Q, които могат да се представят във вида

$$\frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)}$$

$f(x_1, x_2, \ldots, x_n)$ и $g(x_1, x_2, \ldots, x_n)$ са полиноми на $x_1, x_2, \ldots, x_n$ с коефициенти от P и $g((\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0)$. В частност простото разширение $P(\alpha)$ се състои от всички елементи от вида $\frac{f(\alpha)}{g(\alpha)}(f, g \in P[x]$ и $g(\alpha) \neq 0))$.

47. Нека Q е разширение на полето P и $\alpha \in Q$. Покажете, че ако елементът α е трансцендентен над P, пръстенът $P[\alpha]$ е изоморфен с пръстена от полиноми $P[x]$, а полето $P(\alpha)$ — с полето от рационални функции $P(x)$.

Упътване. На всеки елемент $f \in P[x]$ съпоставете елемента $f(\alpha) \in Q$. Условието, че α е трансцендентен над P, означава, че ядрото на така дефинирания хомоморфизъм е нулево.

48. В означенията от предната задача покажете, че ако елементът α е алгебричен над P, пръстенът $P[\alpha]$ е изоморфен с фак-

торпръстена $P[x]/(f)$, където $f\in P[x]$ е минималният полином на α. При това имаме $I[\alpha]=P(\alpha)$. Обратно, ако $P[\alpha]=P(\alpha)$, елементът α е алгебричен над P.

Решение. Както и в предната задача, разглеждаме хомоморфизма $\varphi: P[x]\to Q$, дефиниран с $\varphi(g)=g(\alpha)$. Съгласно зад. 45 образът $\varphi(R[x])$ на пръстена $R[x]$ съвпада с $P[\alpha]$ и вследствие теоремата за хомоморфизмите (вж. уводните бележки към гл. I, §2) имаме

$$P[\alpha]\cong P[x]/I,$$

където I е ядрото на φ. По дефиниция $I=\{g: g(\alpha)=0\}=(f)$, където f е минималният полином на α. По-нататък полиномът f е неразложим, т. е. идеалът I е максимален, следователно $P[\alpha]$ е поле. Поради минималността на $P(\alpha)$ имаме $P(\alpha)\subset P[\alpha]$. Обратното включване е очевидно.

Нека, обратно, $P(\alpha)=P[\alpha]$. Ако α е трансцендентен елемент над P съгласно предната задача, пръстенът $P[\alpha]$ ще бъде изоморфен с пръстена от полиноми $P[x]$, който обаче не е поле; следователно елементът α е алгебричен над P.

49. Докажете, че всяко крайно разширение е алгебрично.

Решение. Нека Q е крайно разширение на P и $(Q:P)=n$. Ако $\alpha\in Q$, елементите $1, \alpha, \alpha^2, \ldots, \alpha^n$ са $n+1$ на брой и следователно са линейно зависими над P, т. е. съществуват такива $a_i\in P$, не всички равни на 0, че

$$a_0+a_1\alpha+\ldots+a_n\alpha^n=0,$$

което точно означава, че елементът α е алгебричен над P.

50. Нека Q е разширение на P и $\alpha\in Q$. Покажете, че елементът α е алгебричен над P тогава и само тогава, когато разширението $P(\alpha)$ над P е крайно. Покажете също, че степента $(P(\alpha):P)$ на разширението $P(\alpha)$ съвпада със степента n на минималния полином f на α и че елементите $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ образуват базис на полето $P(\alpha)$ над P, т. е. всеки елемент от $P(\alpha)$ се представя еднозначно във вида

$$a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1},\ a_i\in P.$$

Решение. Ако $(P(\alpha):P)<\infty$ съгласно предната задача, $P(\alpha)$ е алгебрично разширение на P и в частност елементът α е алгебричен. Обратно, нека α е алгебричен елемент и n да означава степента на минималния полином на α. Ще покажем, че елементите $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ образуват базис на $P(\alpha)$, откъдето ще следва, че $(P(\alpha):P)=n<\infty$. Съгласно зад. 48 имаме $P[\alpha]=P(\alpha)$, т. е. всеки елемент на $P(\alpha)$ има вида $g(\alpha)$, където $g\in P[x]$. Да разделим g на минималния полином f на елемента α. Имаме

$$g=qf+r,$$

където степента на r, ако r не е нулевият полином, е $<n$. От $f(\alpha)=0$ следва $g(\alpha)=r(\alpha)$. С други думи, всеки елемент на $P(\alpha)$ се изразява като линейна комбинация на $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Остава да покажем, че елементите $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ са линейно независими над P. Но ако те са линейно зависими, това ще означава, че съществува ненулев полином $\varphi\in P[x]$ от степен $<n$, така че $\varphi(\alpha)=0$. Последното обаче е невъзможно, тъй като минималният полином на α е от степен n и той трябва да дели φ.

51. Покажете, че разширението $Z_2(\alpha)$, където $\alpha^3+\alpha+1=0$, е поле с 8 елемента, и изразете чрез 1, α, α^2 следните елементи:

а) $(\alpha^2+\alpha+1)(\alpha^2+1)$; б) α^{-1}; в) $(\alpha^2+1)^{-1}$.

Отг. а) $\alpha^2+\alpha$; б) α^2+1; в) α

52. Изразете чрез 1, $\alpha, \alpha^2, \alpha^3$ следните елементи на $P(\alpha)$, където P е полето на рационалните числа и $\alpha^4+\alpha^3+\alpha^2+\alpha+1=0$:

а) $(1+\alpha+\alpha^3)(1+\alpha+\alpha^2)$; б) $(\alpha^2+\alpha+1)^{-1}$.

Отг. а) $\alpha^3+\alpha^2+\alpha+1$; б) α^3+1

53. Рационализирайте изразите, като ги представите като полиноми на α:

а) $\alpha(\alpha-1)^{-1}$, където $\alpha^3-2\alpha-2=0$;

б) $\alpha(\alpha^2+1)^{-1}$, където $\alpha^3+3\alpha^2-3\alpha+6=0$;

в) $\dfrac{1}{\alpha+2}$, където $\alpha^4-3\alpha+6=0$;

г) $\dfrac{\alpha}{\alpha^3+5}$, където $\alpha^3-8\alpha+2=0$;

д) $\dfrac{\alpha}{\alpha^4+1}$, където $\alpha^4+2\alpha+2=0$.

54. Рационализирайте знаменателите на следните изрази:

а) $\dfrac{2\sqrt[3]{5}-1}{\sqrt[3]{25}+4\sqrt[3]{5}+1}$; б) $\dfrac{\sqrt[3]{5}}{3\sqrt[3]{25}+3\sqrt[3]{5}+1}$;

в) $\dfrac{1}{\sqrt[3]{2}-1+\sqrt{2}}$; г) $\dfrac{\sqrt[3]{9}}{2\sqrt[3]{3}-\sqrt{2}+1}$;

д) $\dfrac{1}{\sqrt[3]{4}+\sqrt{3}+\sqrt{2}}$; е) $\dfrac{\sqrt[3]{2}}{\sqrt[3]{4}+2\sqrt{2}}$.

55. Покажете, че ако елементите $\alpha_1, \alpha_2, \ldots, \alpha_n$ на някакво разширение на полето P са алгебрични над P, разширението $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$ е крайно и следователно алгебрично.

Решение. Да положим $P_0=P$ и $P_i=P(\alpha_1, \ldots, \alpha_i)$. Имаме

$$P_0=P\subset P_1\subset P_1\subset P_2\subset \ldots \subset P_n$$

и $P_{i+1}=P_i(\alpha_{i+1})$. Съгласно зад. 41

$$(P_n:P)=(P_n:P_{n-1})(P_{n-1}:P_{n-2})\ldots(P_1:P).$$

По-нататък ще отбележим, че за всяко i елементът α_{i+1} е алгебричен над P_i (тъй като той е алгебричен над P и $P\subset P_i$). Следователно $(P_{i+1}:P_i)<\infty$, откъдето и $(P_n:P)<\infty$.

56. Нека Q е разширение на полето P. Покажете, че сбор, разлика, произведение и частно на алгебрични над P елементи на Q също са алгебрични елементи над P. С други думи, множеството P от елементи на Q, алгебрични над P, е подполе на Q (което очевидно съдържа P).

Решение. Съгласно предната задача, ако елементите $\alpha, \beta \in Q$ са алгебрични над P, то и разширението $P(\alpha, \beta)$ е алгебрично. Но очевидно $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, $\alpha\beta^{-1} \in P(\alpha, \beta)$.

57.* Нека $P \subset Q \subset R$ са полета, при което Q е алгебрично над P. Покажете, че всеки елемент $\alpha \in R$, който е алгебричен над Q, е алгебричен също и над P. С други думи, ако един елемент на R е корен на полином, чиито коефициенти са алгебрични над P, то и този елемент е алгебричен над P. В частност, ако предположим, че разширението R е алгебрично над Q, то е алгебрично и над P (транзитивност на алгебричните разширения).

Решение. Нека $\alpha_0, \alpha_1, \ldots, \alpha_n$ са коефициентите на минималния полином на елемента α над полето Q. Тогава елементите α_i са алгебрични елементи над P, следователно съгласно зад. 55 полето $Q_0=P(\alpha_0, \ldots, \alpha_n)$ е крайно разширение на P. Очевидно елементът α остава алгебричен и над Q_0, откъдето $Q_0(\alpha)$ е крайно разширение на Q_0. Но и Q_0 е крайно разширение на P, следователно $Q_0(\alpha)$ е крайно разширение на P. Съгласно зад. 49 всеки елемент на $Q_0(\alpha)$, в частност и α, е алгебричен над P.

58. Покажете, че разширението Q на полето P е алгебрично тогава и само тогава, когато всеки пръстен R, за който $P \subset R \subset Q$, е поле.

Решение. Ако Q е алгебрично разширение на полето P и R е подпръстен на Q, за който $P \subset R$, за всяко $\alpha \in R$ ще имаме $P[\alpha] \subset R$. Но $P[\alpha]=P(\alpha)$ и следователно $\alpha^{-1} \in P[\alpha]$, така че $\alpha^{-1} \in P$, откъдето следва, че R е поле. Обратно, за всяко $\alpha \in Q$ пръстенът $P[\alpha]$ трябва да е поле, което точно означава, че α е алгебричен елемент над P.

Определение. Нека Q_1 и Q_2 са две прости разширения на полето P. Един изоморфизъм φ на Q_1 в Q_2 се нарича *P-изоморфизъм* (*изоморфизъм над P*), когато оставя неподвижни елементите на P, т. е. $\varphi(a)=a$ за всяко $a \in P$.

59. Нека $Q_1=P(\alpha)$ и $Q_2=P(\beta)$ са две прости алгебрични разширения на полето P, при което минималните полиноми на α и β над P съвпадат. Покажете, че съществува единствен P-изоморфизъм φ на Q_1 върху Q_2, за който $\varphi(\alpha)=\beta$.

Решение. Нека $f \in P[x]$ е общият минимален полином на α и β и n е неговата степен. Съгласно зад. 50 елементите $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, съответно $1, \beta, \beta^2, \ldots, \beta^{n-1}$, образуват базис на пространството Q_1, съответно Q_2. Съществува единствен линеен изоморфизъм φ на Q_1 върху Q_2, за който $\varphi(\alpha^i)=\beta^i$. Непосредствено се проверява, че изображението φ запазва и произведението, т. е. $\varphi(\xi\eta)=\varphi(\xi)\varphi(\eta)$.

60. Нека P е поле и Q, Ω са две негови разширения, при което Q е алгебрично, а Ω е алгебрически затворено. Покажете, че съществува P-изоморфизъм на Q в Ω.

Решение. Нека Σ означава множеството от всички двойки (R, φ), където R е подразширение на Q, а φ е P-изоморфизъм на R в Ω. Множеството Σ нареждаме така: считаме, че $(R_1, \varphi_1) < (R_2, \varphi_2)$, когато $R_1 \subset R_2$ и $\varphi_2(\alpha) = \varphi_1(\alpha)$ при $\alpha \in R_1$. Очевидно така дефинираната релация $<$ е наредба в Σ и удовлетворява условията на лемата на Цорн. Следователно в Σ съществува максимален елемент (R, φ). Остава да покажем, че $R = Q$. В противен случай нека $\alpha \in Q$, $\alpha \notin R$; Елементът α е алгебричен над R. Нека f е минималният му полином. Да означим с $\bar{f}$ полинома, чиито коефициенти са образите на коефициентите на полинома f при изоморфизма φ. Тогава полиномът $\bar{f}$ ще бъде неразложим над полето $\bar{R} = \varphi(R)$. Но Ω е алгебрически затворено, следователно $\bar{f}$ ще има корен β в Ω. Очевидно $\bar{f}$ ще бъде минималният полином на β над $\bar{R}$. Като обобщим метода от предната задача, виждаме, че съществува единствен изоморфизъм ψ на $R(\alpha)$ в Ω, който продължава φ и изобразява α в β. Но тогава $(R, \varphi) \leq (R(\alpha), \psi)$, което противоречи на максималността на (R, φ).

61. Покажете, че ако Ω е алгебрически затворено разширение на полето P и Ω_0 е полето от елементи на Ω, алгебрични над P, то Ω_0 е също алгебрически затворено.

Решение. Трябва да покажем, че всеки полином $f \in \Omega_0[x]$, $f \neq \text{const}$ има корен в Ω_0. Но f има корен α в Ω и очевидно α е алгебричен над Ω_0. Съгласно зад. 57 α е алгебричен и над P, следователно $\alpha \in \Omega_0$.

62. Нека P е поле. Покажете, че съществува такова разширение P_1 на P, в което всеки полином $f \in P[x]$, $f \neq \text{const}$ има корен.

Решение. Първо ще отбележим, че ако $f_1, f_2, \ldots, f_n$ са краен брой полиноми с коефициенти от P, то съществува разширение на P, в което всичките $f_i(x)$ имат поне по един корен. За един полином това е ясно (взимаме $P[x]/(\varphi)$, където φ е неразложим делител на f_1) и по-нататък процедираме по индукция.

Сега да разгледаме пръстена R от полиноми с коефициенти в P на безброй много променливи x_f, индексирани с различните от константи елементи на $P[x]$. Нека I е идеалът в R, породен от всички елементи $f(x_f)$. Идеалът е собствен, защото в противен случай ще бъде изпълнено равенство от вида

$$g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \ldots + g_n f_n(x_{f_n}) = 1.$$

Да вземем такова разширение Q на P, в което f_i да има корен α_i, $i = 1, 2, \ldots, n$ и в това равенство да положим $x_{f_i} = \alpha_i$. Получаваме $0 = 1$, което е невъзможно. Следователно идеалът I е собствен. Нека M е максимален идеал, който съдържа I, и P_1 е полето R/M. Тогава всеки различен от константа полином $f \in P[x]$ има корен в P_1, а именно класът $\overline{x_f}$ на променливата x_f.

Определение. Нека P е поле. Разширението Ω на P се нарича *алгебрична обвивка* на P, ако е алгебрически затворено и е алгебрично над P.

63. Теорема. Всяко поле P притежава алгебрична обвивка, която е еднозначно определена с точност до P-изоморфизъм.

Доказателство. Прилагайки многократно предната задача, можем да построим такава редица от полета

$$P = P_0 \subset P_1 \subset P_2 \subset \ldots \subset P_n \subset \ldots,$$

че всеки полином с коефициенти в P_n да има корен в P_{n+1}. Нека $E = \bigcup P_n$. Очевидно E може да се превърне в поле по такъв начин, че всяко P_n да е подполе на E. При това полето E е алгебрически затворено. Наистина, ако $f \in E[x]$, $f \neq \text{const}$, всичките коефициенти на f ще принадлежат на P_n за достатъчно голямо n. Следователно f ще има корен в $P_{n+1} \subset E$.

Сега да означим с Ω подполето на E, съставено от всички алгебрични над P елементи на E. По дефиниция Ω е алгебрично над P, а от зад. 61 следва, че Ω е алгебрически затворено, така че Ω е алгебрична обвивка на P.

Нека Ω_1 и Ω_2 са алгебрични обвивки на P. Съгласно зад. 60 съществува P-изоморфизъм φ_1 на Ω_1 в Ω_2, при което очевидно Ω_2 ще бъде алгебрично разширение на $\varphi(\Omega)$. Но $\varphi(\Omega_1)$ е алгебрически затворено и следователно то няма никакви собствени алгебрични разширения, т. е. $\varphi(\Omega_1)=\Omega_2$, с което теоремата е доказана.

Забележка. Ако P е поле, Q е алгебрично разширение на P и Ω е алгебрична обвивка на P (съгласно зад. 60 винаги можем да вложим Q в Ω). Ще отбележим обаче, че може да има няколко такива влагания.

Определение. Нека P е поле и $f \in P[x]$. Разширението Q на P се нарича *поле на разлагане* на f над P, ако полиномът f се разлага над Q на линейни множители и $Q=P(\alpha_1, \alpha_2, \ldots, \alpha_n)$, където α_i са всички корени на f в Q.

64. Теорема. Нека P е поле. Всеки полином $f \in P[x]$ има поле на разлагане, което е определено еднозначно с точност до P-изоморфизъм.

Доказателство. Нека Ω е алгебрична обвивка на P. Тогава полиномът f се разлага на линейни множители в Ω. Нека $\alpha_1, \alpha_2, \ldots, \alpha_n$ са всичките корени на f в Ω. Очевидно полето $Q=P(\alpha_1, \ldots, \alpha_n)$ ще бъде поле на разлагане на f. Нека R е какво да е друго поле на разлагане на полинома f. Тогава, ако $\beta_1, \ldots, \beta_n$ са корените на полинома f в R, имаме $R=P(\beta_1, \ldots, \beta_n)$. Съгласно зад. 63 съществува P-изоморфизъм φ на R в Ω. При това очевидно $\varphi(R)=P(\varphi(\beta_1), \ldots, \varphi(\beta_n))$.

От разлагането $f(x)=\prod_{i=1}^{n}(x-\beta_i)$ в R получаваме

$$f(x)=\prod_{i=1}^{n}(x-\varphi(\beta_i))$$

в Ω. Но също $f(x)=\prod_{i=1}^{n}(x-\alpha_i)$, откъдето поради еднозначността на представянето на $f(x)$ като произведение на неразложими множители следва, че с точност до реда на записване корените α_i съвпадат с $\varphi(\beta_i)$. Следователно $\varphi(R)=Q$, т. е. φ е изоморфизъм на R върху Q.

Забележка. От направените разсъждения в частност следва, че в дадена алгебрична обвивка на P полиномът f има единствено поле на разлагане.

65. Теорема за примитивния елемент. Всяко крайно разширение на поле с характеристика 0 е просто.

Доказателство. Нека $Q=P(\alpha_1, \alpha_2, \ldots, \alpha_s)$ е крайно разширение на полето P. Трябва да докажем, че съществува елемент $\theta \in Q$, така че $Q=P(\theta)$. Достатъчно е да разгледаме случая $s=2$. Нека $f(x)$ и $g(x)$ са минималните полиноми на α_1 и α_2 и $\beta_1=\alpha_1, \beta_2, \ldots, \beta_n$, $\gamma_1=\alpha_2, \gamma_2, \ldots, \gamma_m$ са съответно техните корени (в някакво подходящо разширение на полето Q). Тъй като по предположение характеристиката на P е 0, корените $\beta_1, \ldots, \beta_n$ (съответно $\gamma_1, \ldots, \gamma_m$) са два по-два различни (един неразложим полином над поле с характеристика 0 не може да има кратни корени), следователно можем да образуваме елементите

$$\frac{\beta_1-\beta_i}{\gamma_1-\gamma_j}, \quad i=1, 2, \ldots, n, \ j=2, 3, \ldots, m.$$

Това са краен брой елементи на Q и тъй като полето P е безкрайно, съществува елемент $c \in P$, различен от всички тях. Да положим $\theta=\alpha_1+c\alpha_2$. Ще покажем, че $Q=P(\theta)$. Най-напред $\theta \in Q$, откъдето $P(\theta) \subset Q$. Ще отбележим, че от избора на c следва, че $\theta \neq \beta_i + c\gamma_j$, $i=1, 2, \ldots, n$, $j=2, \ldots, m$. Да положим $h(x)=f(\theta-cx)$. Това е полином с коефициенти в $P(\theta)$. Имаме $h(\alpha_2)=f(\theta-c\alpha_2)=f(\alpha_1)=0$, следователно α_2 е общ корен на $g(x)$ и $h(x)$. Друг общ корен тези два полинома не могат да имат, защото това би бил някой γ_j, $j=2, \ldots, m$. Но $h(x_j)=0$ означава, че $f(\theta-c\gamma_j)=0$, т. е. $\theta-c\gamma_j$ съвпада с някой β_i, което противоречи на избора на c. И така можем да запишем

$$(g(x), h(x))=x-\alpha_2.$$

Тъй като коефициентите на $g(x)$ и $h(x)$ лежат в $P(\theta)$, то и коефициентите на техния НОД лежат в това поле, откъдето следва, че $\alpha_2 \in P(\theta)$. Аналогично се доказва, че и $\alpha_1 \in P(\theta)$, откъдето следва $P(\alpha_1, \alpha_2) \subset P(\theta)$. С това доказателството е завършено.

Ще отбележим, че теоремата за примитивния елемент престава да бъде вярна в случая, когато характеристиката на P е различна от 0 без допълнителни предположения за P.

66. Намерете примитивен елемент θ на полето $P(\sqrt{2}, \sqrt{3})$ където P е полето на рационалните числа, и съставете минималния полином на θ.

Отг. Напр. $\theta=\sqrt{2}+\sqrt{3}$ и x^4-10^2+1.

67. Също за полето $P(\sqrt{2}; \sqrt[3]{3})$.

Отг. Напр. $\theta=\sqrt{2}+\sqrt[3]{3}$, с минимален полином $x^6-6x^4+12x^2-12x+1$.

В следващите няколко задачи ще разглеждаме крайни полета, като с $Z_p=F_p$ ще означаваме простото поле с характеристика p и с Ω_p — фиксирано алгебрически затворено разширение на F_p.

68. Покажете, че за всяко естествено число n в Ω_p съществува единствено подполе F_q с $q=p^n$ елемента. Полето F_q може да се дефинира като множество от всички x, за които $x \in \Omega_p$ и представлява поле на разлагане на полинома x^q-x над полето F_p.

Решение. Да разгледаме полинома $f(x)=x^q-x$. Неговата производна е равна на -1, следователно уравненията $f(x)=0$ и $f'(x)$ нямат общи корени. И така уравнението $f(x)=0$ има точно q различни корена в Ω_p. Нека F_p означава множеството от корените на това уравнение. Лесно се вижда, че F_q е поле. Наистина, ако $a^q-a=0$ и $b^q-b=0$, то $(a+b)^q=a+b$ и $(ab)^q=ab$, $(a^{-1})^q=(a^q)^{-1}=a^{-1}$. Следователно F_q е подполе на Ω_p с точно q елемента. Сега ще покажем, че F_q е единственото подполе на Ω_p с q елемента. Наистина, ако подполето $P \subset \Omega_p$ има q елемента, за всяко $x \in P$ имаме $x^q=x$ и следователно $P \subset F_q$, откъдето $P=F_q$, тъй като P и F_q имат еднакъв брой елементи.

69. В означенията от предната задача нека $q_1=p^n$ и $q_2=p^m$. Покажете, че $E_{q_1}\subset F_{q_2}$ тогава и само тогава, когато n/m.

Упътване. Използувайте факта, че $F_q=\{x : x^q=x\}$ при $q=p^k$.

70. Нека $f(x)\in F_q[x]$ е неразложим полином от степен m над крайното поле F_q с q на брой елемента. Покажете, че полиномът $f(x)$ дели $x^{q^n}-x$ тогава и само тогава, когато m дели n.

Решение. Най-напред ще отбележим, че ако α е корен на полинома $f(x)$, то разширението $F_q(\alpha)$ съвпада с крайното поле F_{q^m}; действително имаме $(F_q(\alpha):F_q)=m$, т. е. $F_q(\alpha)$ е m-мерно линейно пространство над полето F_q и следователно $F_q(\alpha)$ има точно q^m на брой елемента, откъдето ще следва, че $F_q(\alpha)=F_{q^m}$. Нека сега $f(x)$ дели $x^{q^n}-x$. Ако α е корен на $f(x)$, имаме $\alpha\in F_{q^n}$ и следователно $F_q(\alpha)\subset F_{q^n}$, т. е. $F_{q^m}\subset F_{q^n}$, откъдето m дели n. Обратно ако m дели n, за всеки корен α на $f(x)$ имаме $\alpha\in F_{q^n}$, т. е. α е корен на полинома $x^{q^n}-x$. Тъй като корените на $f(x)$ са прости, оттук следва, че $f(x)$ дели $x^{q^n}-x$.

Забележка. Използуваният факт, че корените на $f(x)$ са прости, следва от това, че ако $f(x)$ има кратен корен, този корен ще бъде корен и на производната $f'(x)$, откъдето поради неразложимостта на $f(x)$ ще следва, че $f(x)$ дели $f'(x)$, т. е. $f'(x)$ е нулевият полином. Но тогава $f(x)$ ще трябва да има вида $f(x)=\sum a_\nu x^{p\nu}$ и понеже всяко a_ν може да се представи като $a_\nu=b_\nu^p$, $b_\nu\in F_q$, то $f(x)=\sum b_\nu^p x^{p\nu}=\left(\sum b_\nu x^\nu\right)^p$, което противоречи на условието, че полиномът $f(x)$ е неразложим.

71. Докажете, че е в сила разлагането

$$x^{q^n}-x=\prod_{d/n}\left(\prod f_d(x)\right),$$

където $f_d(x)$ означават всички неразложими полиноми над F_q от степен d със старши коефициент 1.

§ 3. СВОЙСТВА НА ПОЛИНОМИТЕ НАД ОСНОВНИТЕ ЧИСЛОВИ ПОЛЕТА

1. Полиноми с комплексни коефициенти

Основна теорема на алгебрата на комплексните числа (теорема на Даламбер). Полето на комплексните числа е алгебрически затворено, т. е. всяко алгебрично уравнение с комплексни коефициенти има поне един комплексен корен.

Следствие. Единствените неразложими полиноми над полето на комплексните числа са полиномите от първа степен.

Следователно, ако

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

е полином от степен $n\geq 1$ с произволни комплексни коефициенти, той се разлага еднозначно над полето на комплексните числа на линейни множители:

$$f(x)=a_0(x-x_1)^{k_1}(x-x_2)^{k_2}\dots(x-x_r)^{k_r},$$

където числата $x_1, x_2, \dots, x_r$ означават различните корени на уравнението $f(x)=0$ съответно от кратности $k_1, k_2, \dots, k_r$; $k_1+k_2+ + \dots+k_r=n$.

2. Полиноми с реални коефициенти

Ако $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$ е произволен полином с реални коефициенти $a_0, a_1, a_2, \dots, a_n$, $a_0\neq 0$, $n\geq 1$ и комплексното число c е корен на уравнението $f(x)=0$, то комплексно спрегнатото на c число $\bar{c}$ също е корен на това уравнение. Оттук следва, че всеки полином с реални коефициенти, който е от степен $n>2$, е разложим над полето на реалните числа. Единствените неразложими полиноми над полето D на реалните числа са полиномите от първа степен и полиномите от втора степен ax^2+bx+c с отрицателни дискриминанти $b^2-4ac<0$.

И така *над полето на реалните числа полиномът $f(x)$ еднозначно се разлага на линейни и квадратни множители:*

$$f(x)=a_0(x-\alpha_1)^{k_1}\dots(x-a_r)^{k_r}.(x^2+p_1x+q_1)^{l_1}\dots(x^2+p_sx+q_s)^{l_s}$$

$$p_\nu^2-4q_\nu<0;\ \nu=1, 2, \dots, s;$$

$$k_1+k_2+\dots+k_r+2(l_1+l_2+\dots+l_s)=n.$$

Следствие. Комплексно спрегнатите корени на алгебрични уравнения с реални коефициенти имат еднакви кратности.

Следствие. Всяко алгебрично уравнение с реални коефициенти и от нечетна степен има нечетен брой реални корени (броени съобразно техните кратности). В частност уравнението ще има поне един реален корен.

3. Полиноми с рационални коефициенти

Теорема. Ако $x=\frac{p}{q}$, p, q — цели и взаимно прости, е рационален корен на уравнението с цели коефициенти

$$(1)\qquad a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n=0,$$

то p дели a_n и q дели a_0.

В частност при $a_0=1$ всички рационални корени на уравнението (1) са цели и са измежду делителите на свободния член a_n.

При $a_0 \neq 1$ чрез субституцията $a_0 x = y$ въпросът за намиране на рационалните корени на уравнението (1) се свежда до въпроса за намиране на целите корени на уравнението

$$y^n + a_1 y^{n-1} + a_0 a_1 y^{n-2} + \ldots + a_0^{n-1} a_n = 0.$$

За намиране на целите корени на уравнения с цели коефициенти е удобно да се използува още следното твърдение: ако α е цял корен на уравнението $f(x) = 0$, то $\alpha - 1$ дели $f(1)$ и $\alpha + 1$ дели $f(-1)$.

Определение. Един полином с цели коефициенти се нарича *примитивен*, когато коефициентите му нямат общ делител, различен от ± 1.

Лема на Гаус. Произведение от примитивни полиноми е примитивен полином.

Следствие. Ако един полином с цели коефициенти е разложим над полето на рационалните числа, той е разложим и над пръстена на целите числа.

Критерий на Айзенщайн. Нека

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

е полином с цели коефициенти и p е просто число, такова, че:

а) p дели $a_1, a_2, \ldots, a_n$;

б) p не дели a_0;

в) p^2 не дели a_n.

Тогава полиномът $f(x)$ е неразложим над полето на рационалните числа.

Следствие. При всяко естествено число n съществуват неразложими полиноми над полето Q на рационалните числа, които са от степен n. Например полиномите $x^n + 2$, $n = 1, 2, 3, \ldots$ са неразложими над Q.

Пример. Полиномът

$\dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$, p—просто, е неразложим над Q.

Наистина, като положим $x - 1 = y$, получаваме полинома

$$\varphi(y) = \frac{(1+y)^p - 1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \ldots + \binom{p}{p-1},$$

който е неразложим над Q съгласно критерия на Айзенщайн. Следователно даденият полином $f(x) = \varphi(x - 1)$ също е неразложим над Q.

1. Разложете на неразложими над полето на комплексните числа множители следните полиноми:

а) $f(x) = x^2 + 5x + 6$;

б) $f(x) = 2x^2 + 4x + 4$;

в) $f(x)=x^2+(1+i)x+i$;
г) $f(x)=x^4+16$;
д) $f(x)=x^4+4i$;
е) $f(x)=x^4+2x^2+(1-2i)$;
ж) $f(x)=x^4+8x^3+8x-1$;
з) $f(x)=x^3+x+2$;
и) $f(x)=x^4+2x^3+3x^2+2x-3$;
к) $f(x)=x^5+x^4+x^3+x^2+x+1$;
л) $f(x)=x^{12}+2x^6+1$.

Отг. а) $(x+2)(x+3)$; б) $2(x+1+i)(x+1-i)$; в) $(x+1)(x+i)$; г) $[x-\sqrt{2}(1+i)][x-\sqrt{2}(1-i)][x+\sqrt{2}(1+i)]x[x+\sqrt{2}(1-i)]$; д) полиномът се разлага на линейни множители от вида

$$x\pm\frac{\sqrt{2-\sqrt{2}}+i\sqrt{2+\sqrt{2}}}{\sqrt{2}},\quad x\pm\frac{\sqrt{2+\sqrt{2}}-i\sqrt{2-\sqrt{2}}}{\sqrt{2}};$$

е) полиномът се разлага на линейни множители от вида

$x\pm\frac{1+i}{\sqrt{2}}$, $x\pm\frac{\sqrt{\sqrt{5}-2}-i\sqrt{\sqrt{5}+2}}{\sqrt{2}}$;

ж) $(x-i)(x+i)(x+4-\sqrt{17})(x+4+\sqrt{17})$;

з) $(x+1)\left(x-\frac{1+i\sqrt{7}}{2}\right)\left(x-\frac{1-i\sqrt{7}}{2}\right)$;

и) $\left[x-\frac{1}{2}(\sqrt{5}-1)\right]\left[x+\frac{1}{2}(\sqrt{5}+1)\right]\left[x+\frac{1}{2}(1+i\sqrt{11})\right]\left[x+\frac{1}{2}(1-i\sqrt{11})\right]$;

к) $\left[x-\frac{1}{2}(1+i\sqrt{3})\right]\left[x-\frac{1}{2}(1-i\sqrt{3})\right]\left[x+\frac{1}{2}(1+i\sqrt{3})\right]\left[x+\frac{1}{2}(1-i\sqrt{3})\right](x+1)$;

л) $(x-i)^2(x+i)^2\left[x-\frac{1}{2}(\sqrt{3}+i)\right]^2\left[x-\frac{1}{2}(\sqrt{3}-i)\right]^2\left[x-\frac{1}{2}(\sqrt{3}+i)\right]^2\left[x+\frac{1}{2}(\sqrt{3}-i)\right]^2$.

2. Разложете на линейни множители над полето на комплексните числа полиномите:

а) $f(x)=(x+\cos\theta+i\sin\theta)^n+(x+\cos\theta-i\sin\theta)^n$;

б) $f(x)=x^m-\binom{2m}{2}x^{m-1}+\binom{2m}{4}x^{m-2}-\ldots+(-1)^m\binom{2m}{2m}$.

Отг. а) $2\prod_{k=1}^{n}\left(x+\frac{\sin\left(\theta+\frac{2k-1}{2n}\pi\right)}{\sin\frac{2k-1}{2n}\pi}\right)$; б) $\prod_{k=1}^{m}\left[x-\operatorname{tg}^2\frac{(2k-1)\pi}{4m}\right]$.

3. Разложете на неразложими над полето на реалните числа множители следните полиноми:

а) $f(x)=x^2+2x+3$;
б) $f(x)=x^3+x+2$;
в) $f(x)=x^4+16$;
г) $f(x)=x^4+8x^3+8x-1$;
д) $f(x)=x^4+2x^3+3x^2+2x-3$;
е) $f(x)=x^4-ax^2+1$, $|a|<2$;
ж) $f(x)=x^4+x^3+x^2+x+1$;
з) $f(x)=x^{10}-2x^5+2$.

Отг. а) неразложим; б) $(x+1)(x^2-x+2)$; в) $(x^2-2x\sqrt{2}+4)(x^2+2x\sqrt{2}+4)$

г) $(x^2+1)(x+4-\sqrt{17})(x+4+\sqrt{17})$; д) $[x-\frac{1}{2}(\sqrt{5}-1)][x+\frac{1}{2}(\sqrt{5}+1)](x^2+x+3)$; е) $(x^2-x\sqrt{a+2}+1)(x^2+x\sqrt{a+2}+1)$;

ж) $\left[x^2-\frac{1}{2}(\sqrt{5}-1)x+1\right]\left[x^2+\frac{1}{2}(\sqrt{5}+1)x+1\right]$;

з) $\prod_{k=0}^{4}\left(x^2-2\sqrt[10]{2}\cos\frac{8k+1}{20}\pi+\sqrt[5]{2}\right)$.

4. Разложете на линейни и квадратни множители с реални коефициенти полиномите:

а) $f(x)=\sum_{k=0}^{n}\binom{2n+1}{2k}x^{2n-2k+1}(x^2-1)^k$;

б) $f(x)=\sum_{k=0}^{n}\binom{2n}{2k}x^{2n-2k}(x^2-1)^k$.

Упътване. Положете $x=\cos t$ и намерете корените на тригонометричното уравнение $\varphi(t)=0$, където $\varphi(t)=f(\cos t)$.

Отг. а) $2^{2n}x\prod_{k=0}^{n-1}\left(x^2-\cos^2\frac{2k+1}{4n+2}\pi\right)$; б) $2^{2n-1}\prod_{k=0}^{n-1}\left(x^2-\cos^2\frac{2k+1}{4n}\pi\right)$.

5. Разложете полинома $x^4-2x^2\cos 2\alpha+1$ на два реални квадратни множителя.

Отг. $(x^2-2x\cos\alpha+1)(x^2+2x\cos\alpha+1)$.

6. Разложете полинома $(x^2+x+1)^2+1$ на два реални квадратни множителя.

Отг. $(x^2+1)(x^2+2x+2)$.

7. Намерете полином с реални коефициенти и от възможно най-ниска степен, за който числото 1 е прост корен, а числото $3+i$ е двоен корен.

Отг. $a_0(x^5-13x^4+68x^3-176x^2+220x-100)$, $a_0\neq 0$.

8. Намерете полином с реални коефициенти и от възможно най-ниска степен, за който числата i и $1+i$ са двойни корени

Отг. $x^8-4x^7+10x^6-16x^5+21x^4-20x^3+16x^2-8x+4$.

9. Намерете полином от възможно най-ниска степен, за който числото 1 е корен, 2 и $1-i$ са прости корени на производната му, а i е двукратен корен на същата производна.

Отг. $12x^5-15(3+i)x^4+20(3+4i)x^3-30(1+5i)x^2-120(1-i)x+123-35i$.

10. Намерете необходимо и достатъчно условие полиномът

$$x^3+a_1x^2+a_2x+a_3$$

с положителни коефициенти да има два чисто имагинерни корена $\pm bi$.

Отг. $a_3=a_1a_2$.

11. Докажете, че уравнението $x^3+a_1x^2+a_2x+a_3=0$, с реални коефициенти, има всичките си корени с отрицателни реални части тогава и само тогава, когато

$$a_1>0,\ a_2>0,\ a_3>0,\ a_3<a_1a_2.$$

Решение. Нека реалните части на всички корени на даденото уравнение са отрицателни. Тогава поне един от корените е реален и отрицателен. Да го означим с x_1. Сборът от другите два корена x_2 и x_3 да означим с $2l$. Очевидно $2l$ е реално отрицателно число. Да положим $m=x_2x_3$. Очевидно $m>0$. Съгласно формулите на Виет получаваме: $a=-x_1-x_2-x_3=-x_1-2l>0$, $a_2=$ $=x_1x_2+x_2x_3+x_3x_1=2lx_1+m>0$, $a_3=-x_1x_2x_3=-mx_1>0$. По-нататък имаме $a_2-m=2lx_1>0$ или още $a_2-m=a_2+\frac{a_3}{x_1}>0$, понеже $m=-\frac{a_3}{x_1}$, откъдето a_2x_1+ $+a_3<0$ или $-a_2(a_1+2l)+a_3<0$, $a_3<a_1a_2+2la_2<a_1a_2$. Обратно, нека $a_1>0$, $a_2>0$, $a_3>0$ и $a_3<a_1a_2$. Тогава уравнението няма положителни корени. Ако всички корени са отрицателни, твърдението на задачата е очевидно. Нека един от корените е отрицателен, а останалите два $x_2=\alpha+\beta i$ и $x_3=\alpha-\beta i$ са комплексно спрегнати. Съгласно предната задача имаме $\alpha\neq 0$ и следователно $\beta\neq 0$. Както и по-горе, получаваме $a_2-m=2lx_1$, като тук $l=\alpha$. Трябва да покажем, че $\alpha<0$. Ако допуснем, че $\alpha>0$, ще имаме $a_2-m<0$ или $a_2+\frac{a_3}{x_1}<0$, $a_2x_1+a_3>0$, $a_3>a_1a_2+2la_2>a_1a_2$, което противоречи на условието $a_3<a_1a_2$.

Забележка. Резултатът е частен случай от един критерий на Хурвиц, който ни дава необходими и достатъчни условия нулите на произволен реален полином да лежат вляво от имагинерната ос (вж. уводните бележки към § 5).

12. Да разгледаме кривата с уравнение

$$y=x^4+ax^3+bx^2+cx+d$$

(a, b, c, d — реални числа). Намерете такава права, която да пресича кривата в четири точки M_1, M_2, M_3, M_4, така че $M_1M_2=M_2M_3=M_3M_4$. При какво условие задачата има решение.

Упътване. Задачата се свежда до намирането на реалните числа λ и μ, така че корените на уравнението

$$x^4+ax^3+bx^2+cx+d=\lambda x+\mu$$

да са реални и да образуват аритметична прогресия.

Отг. Търсената права има уравнение $y=\lambda x+\mu$, където $\lambda=\frac{1}{8}(a^3-4ab+8c)$,

$$\mu=d-\frac{1}{1600}(36b-1)(4b+a^2) \text{ при условие, че } 3a^2-8b>0.$$

13. Нека $f(x)$ е произволен полином с комплексни коефициенти от степен $\leqq n-1$. Докажете, че

$$f(0)=\frac{1}{n}\sum_{k=0}^{n-1} f(\omega_k),$$

където $\omega_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$, $k=0, 1, \ldots, n-1$.

Упътване. Използувайте равенствата

$$\sum_{k=0}^{n-1}\omega_k^\nu=0 \text{ при } 1\leqq\nu\leqq n-1.$$

14. Нека $f(x)$ е полином с комплексни коефициенти и $f(x)\neq\text{const}$. Докажете, че

$$|f(a)|<\max_{|x-a|=r}|f(x)|.$$

15. Разложете на неразложими над полето на рационалните числа следните полиноми:

а) $f(x)=5x^3+3x-48$;
б) $f(x)=x^3-11x^2+38x-40$;
в) $f(x)=6x^4+x^3+2x^2-4x+1$;
г) $f(x)=8x^5-14x^4-77x^3+128x^2+45x-18$;
д) $f(x)=10x^5+17x^4+13x^3+2x^2-5x-1$;
е) $f(x)=8x^5+28x^4-2x^3-67x^2-12x+45$;
ж) $f(x)=24x^5-110x^4+199x^3-196x^2+110x-21$.

Отг. а) неразложим; б) $f(x)=(x-2)(x-4)(x-5)$
в) $f(x)=(2x-1)(3x+1)(x^2+x+1)$;
г) $f(x)=(x-2)(x-3)(x+3)(2x+1)(4x+1)$;
д) $f(x)=(x+1)(2x-1)(5x+1)(x^2+x+1)$;
е) $f(x)=(x-1)^2(2x+3)(2x+5)(2x-3)$;
ж) $f(x)=(3x-1)(2x-3)(4x-7)(x^2-x+1)$.

16. Нека

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

е полином с цели коефициенти и p е просто число, така че:

1°. $p \times a_0$;
2°. $p/a_{k+1}, a_{k+2}, \ldots, a_n$;
3°. $p^2 \times a_n$.

Докажете, че полиномът $f(x)$ притежава неразложим множител от степен $\geqq n-k$.

Решение. Нека $f(x)=p_1(x)\,p_2(x)\ldots p_s(x)$ е разлагането на $f(x)$ на неразложими над полето на рационалните числа множители, които съгласно лемата на Гаус можем да предполагаме с цели коефициенти, и с $g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m$ да означим един от тях, свободният член на който се дели на p. (Съществуването на такъв полином следва от условието 2°.) Ще докажем, че $m \geqq n-k$. За целта да означим с $q(x)$ частното от делението на $f(x)$ с $g(x)$:

$$q(x)=c_0x^l+c_1x^{l-1}+\ldots+c_l.$$

Нека b_i означава последния от коефициентите на $g(x)$, който не се дели на p, т. е. $p \times b_i$, $p/b_{i+1}, b_{i+2}, \ldots, b_m$. Очевидно $p \times c_l$. Но тогава и коефициентът

$$a_{l+i}=b_ic_l+b_{i+1}c_{l-1}+\ldots$$

не се дели на p, откъдето следва, че $l+i \leqq k$. И така

$$m \geqq m+l+i-k=n+i-k \geqq n-k.$$

При $k=1$ получаваме следното интересно твърдение: нека $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a^n$ е полином с цели коефициенти (и p е просто число, така че $p \times a_0$, $p/a_2, a_3, \ldots, a_n$) и $p^2 \times a_n$; тогава полиномът $f(x)$ или е неразложим, или има рационален корен, в който случай полиномът се разлага на два неразложими множителя, съответно от първа и $(n-1)$-ва степен.

17. Нека $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ е полином с цели коефициенти, $s>1$ е естествено число и p е просто число, за което:

1°. $p \times a_0$;
2°. $p/a_1, a_2, \ldots, a_n$;
3°. $p^s \times a_n$.

Докажете, че полиномът $f(x)$ се разлага най-много на $s-1$ на брой неразложими (над полето на рационалните числа) множители.

Решение. Да допуснем, че

$$f(x)=p_1(x)\,p_2(x)\ldots p_k(x),$$

където $k \geqq s$ и $p_i(x)$, $i=1, 2, \ldots, k$ са неразложими над полето на рационалните числа полиноми. Вследствие лемата на Гаус можем да предполагаме, че тези неразложими множители на $f(x)$ са с цели коефициенти. Ще извършим редукция по модул p. Ако $\varphi(x)$ е произволен полином с цели коефициенти, с $\overline{\varphi}(x)$ ще означаваме съответния му полином от $Z_p[x]$. Имаме

$$f(x)=\overline{p_1}(x)\overline{p_2}(x)\ldots\overline{p_k}(x).$$

Но съгласно условието 2° получаваме $\overline{f}(x)=\overline{a_0}\,x^n$, където $\overline{a_0}\in Z_p$, $\overline{a_0}\neq\overline{0}$ е класът от остатъци по модул p с представител a_0. Съгласно основната теорема за еднозначност на разлагането на неразложими множители ще имаме

$$\overline{p_i}(x)=\overline{\alpha_i}\,x^{l_i},\ i=1,\ 2,\ldots,k;\ \alpha_i\in Z_p,\ \overline{\alpha_i}\neq\overline{0}.$$

Лесно се вижда, че $l_i\neq 0$, $i=1,\ 2,\ldots,k$. Можем да пишем

$$p_i(x)\equiv\alpha_i\,x^{l_i}\pmod{p},\ \alpha_i\in Z,$$

т. е.

$$p_i(x)=\alpha_i x^{l_i}+pg_i(x),\ i=1,\ 2,\ldots,k,$$

където $g_i(x)$ са полиноми с цели коефициенти. От

$$f(x)=\prod_{i=1}^{k}[\alpha_i x^{l_i}+pg_i(x)]$$

при $x=0$ получаваме

$$a_n=f(0)=p^k\prod_{i=1}^{k}g_i(0),$$

откъдето следва, че $p^k|a_n$. Последното обаче при $k\geq s$ противоречи на условието 3°.

18. Покажете, че ако $f(x)$ е неразложим над полето на рационалните числа и α, β са произволни рационални числа, $\alpha\neq 0$, **полиномът $f(\alpha x+\beta)$ е също неразложим над полето на рационалните числа.**

19. Като използувате критерия на Айзенщайн (вж. уводните бележки и зад. 16, зад. 17) и при необходимост — и резултата от предната задача, покажете, че всеки един от следните полиноми е неразложим над полето на рационалните числа:

а) $f(x)=3x^4-15x^3+10x^2-20x+35$;
б) $f(x)=2x^5+14x^3-35x^2-56x+63$;
в) $f(x)=x^4-2x+3$;
г) $f(x)=2x^4+9x^3+20x^2+15x+32$;
д) $f(x)=x^p-px+(2p-1)$, p — просто;
е) $f(x)=x^p+px^{p-1}+px+(3p+1)$, p — просто;

ж) $f(x)=\dfrac{x^{p^k}-1}{x^{p^{k-1}}-1}$, p — просто.

20. Покажете с подходящи примери, че условията от критерия на Айзенщайн са съществени.

21. Като използувате метода на неопределените коефициенти, изследвайте за неразложимост следните полиноми и в случай на разложимост извършете разлагането:

а) $f(x)=x^4-3x^2+6x+6$;
б) $f(x)=x^4+12x^3+38x^2+44x+5$;
в) $f(x)=x^4+4x^3+\frac{11}{2}x^2+x-\frac{23}{16}$;
г) $f(x)=x^4+2x^3+3x^2+4x+5$;
д) $f(x)=x^4-4x^3+x^2-8x-2$.

Отг. а) неразложим; б) $f(x)=(x^2+8x+1)(x^2+4x+5)$; в) неразложим; г) неразложим; д) $f(x)=(x^2+2)(x^2-4x-1)$.

22. Намерете необходимо и достатъчно условие за неразложимост над полето на рационалните числа на полинома

$$f(x)=x^4+px^2+q$$

(p, q — рационални числа).

23. Нека $f(x)=a_0x^4+a_1x^3+a_2x^2+a_3x+a_4$ е полином с рационални коефициенти и уравнението $f(x)=0$ да няма реални корени. Нека $f(x)$ е разложен над полето на реалните числа на произведение от два полинома от втора степен със старши коефициенти 1, при което не всички коефициенти на тези полиноми са рационални числа. Покажете, че полиномът $f(x)$ е неразложим над полето на рационалните числа.

24. Докажете, че полиномът $f(x)=x^4+ax^3+bx^2+cx+d$, $c^2\neq a^2d$ с цели коефициенти е неразложим над полето на рационалните числа, когато няма рационални корени и не се дели на полиноми от вида

$$x^2+\frac{cm-am^2}{d-m^2}x+m,$$

какъвто и да бъде делителят m на свободния член d.

Решение. Да допуснем, че $f(x)$ няма рационален корен и
$$x^4+ax^3+bx^2+cx+d=(x^2+\lambda x+m)(x^2+\mu x+n)$$
(λ, μ, m, n — цели числа). Като приравним коефициентите пред x^3 и x, получаваме

$$\begin{cases}\lambda+\mu=a\\ n\lambda+m\mu=c.\end{cases}$$

От $c^2\neq a^2d$ следва $m\neq n$ и тогава, като решим системата спрямо λ и μ, ще имаме $\lambda=\frac{c-am}{n-m}$. Ясно е, че m е делител на d, понеже $d=mn$. Получаваме окончателно

$$\lambda=\frac{cm-m^2}{d-m^2},$$

откъдето следва, че $f(x)$ се дели на тричлен от указания в задачата вид.

25. Покажете, че полиномът

$$x^5+ax^4+bx^3+cx^2+dx+e$$

с цели коефициенти е неразложим над полето на рационалните числа, когато няма рационален корен и не се дели на полиноми от вида

$$x^2+\frac{am^3-cm^2-dn+be}{m^3-n^2+ae-bm}x+m,$$

където m е произволен делител на e и $n=\frac{e}{m}$.

26. Като използувате резултатите от предните две задачи, разложете на неразложими множители над полето на рационалните числа полиномите:

а) $f(x)=x^4-3x^3+2x^2+3x-9$;
б) $f(x)=x^4-3x^3+2x^2+2x-6$;
в) $f(x)=x^4+4x^3-6x^2-23x-12$;
г) $f(x)=x^5+x^4-4x^3+9x^2-6x+6$.

Отг. а) $(x^2-2x+3)(x^2-x-3)$; б) неразложим;
в) $(x^2-x-4)(x^2+5x+3)$; г) $(x^2-2x+2)(x^3+3x+3)$.

27. Докажете, че ако полиномът $f(x)$ от степен n с цели коефициенти приема стойности ± 1 за повече от $2\left[\frac{n}{2}\right]$ цели стойности на x, той е неразложим над полето на рационалните числа.

Решение. Ако полиномът $f(x)$ от степен n при $n=2m$ или $n=2m+1$ е разложим, то един от множителите му $g(x)$ ще бъде от степен $\leq m$. Ако $f(x)$ приема стойности ± 1 за повече от $2m$ цели стойности на x, то $g(x)$ също ще приема стойности ± 1 за тези значения на x. Но тогава или уравнението $g(x)=1$, или уравнението $g(x)=-1$ би трябвало да има повече от m корена. Последното води до противоречие.

28. Нека $f(x)$ е полином с цели коефициенти, който приема стойност 1 за повече от 3 цели стойности на x. Докажете, че за всяко цяло x имаме $f(x)\neq -1$.

29. Нека $f(x)$ **е полином от степен n с цели коефициенти,** който приема стойност 1 за повече от $\frac{n}{2}$ цели стойности на x. Докажете, че при $n\geq 12$ полиномът $f(x)$ е неразложим над полето на рационалните числа.

30. Нека ax^2+bx+1 е полином с цели коефициенти, който е неразложим над полето на рационалните числа. Да положим, $\varphi(x)=(x-a_1)(x-a_2)\dots(x-a_n)$, където $a_1, a_2, \dots, a_n$ са различни цели числа. Докажете, че при $n\geq 7$ полиномът

$$a[\varphi(x)]^2+b[\varphi(x)]+1$$

е неразложим над полето на рационалните числа.

Решение. Нека

$$a[\varphi(x)]^2+b[\varphi(x)]+1=g(x)h(x).$$

Един от множителите $g(x)$ и $h(x)$, напр. $g(x)$, е от степен $\leq n$. Полиномът $g(x)$ приема стойности ± 1 при $x=a_1, a_2, \ldots, a_n$. Съгласно зад. 28 или всичките тези стойности са равни на 1, или най-много 3 от тях са равни на 1. Аналогично може да се покаже, че или всички тези стойности са равни на -1, или най-много 3 от тях са равни на -1. Понеже $n\geqq 7$, ясно е, че всичките тези стойности трябва да бъдат с еднакъв знак. Следователно

$$g(x)=\pm 1+\alpha(x-a_1)(x-a_2)\ldots(x-a_n)=\pm 1+\alpha\varphi(x).$$

Ако $\alpha\neq 0$, то $h(x)$ има също степен n и $h(x)=\pm 1\pm\beta\varphi(x)$. Но тогава ще имаме

$$a[\varphi(x)]^2+b[\varphi(x)]+1=(\pm 1+\alpha\varphi(x))(\pm 1\beta\varphi(x)),$$

което е невъзможно, понеже по условие полиномът ax^2+bx+c е неразложим.

31. Нека $a_1, a_2, \ldots, a_n$ са различни цели числа. Докажете, че полиномът

$$f(x)=(x-a_1)(x-a_2)\ldots(x-a_n)-1$$

е неразложим над полето на рационалните числа.

Решение. Нека $f(x)=g(x)h(x)$, където $g(x)$ и $h(x)$ са с цели коефициенти. Тъй като $f(a_i)=-1$, то $g(a_i)=1$, $h(a_i)=-1$ или $g(a_i)=-1$, $h(a_i)=1$. И в двата случая ще имаме

$$g(a_i)+h(a_i)=0.$$

Ако $g(x)$ и $h(x)$ са от положителни степени, степента на $g(x)+h(x)$ ще бъде $<n$, откъдето следва, че $g(x)+h(x)$ е нулевият полином, т. е. $h(x)=-g(x)$. Следователно $f(x)=-[g(x)]^2$. Последното равенство обаче е невъзможно, тъй като старши коефициентът на $f(x)$ е положителен.

32. Нека $a_1, a_2, \ldots, a_n$ са различни цели числа. Изследвайте полинома

$$f(x)=(x-a_1)(x-a_2)\ldots(x-a_n)+1$$

по отношение на неразложимостта му над полето на рационалните числа.

Отг. Полиномът е неразложим във всички случаи освен в следните два:

$f(x)=(x-a)(x-a-2)+1=(x-a-1)^2$; $f(x)=(x-a)(x-a-1)(x-a-2)(x-a-3)+1=[(x-a-1)(x-a-2)-1]^2$.

33. Докажете, че полиномът

$$f(x)=(x-a_1)^2(x-a_2)^2\ldots(x-a_n)^2+1,$$

където $a_1, a_2, \ldots, a_n$ са различни цели числа, е неразложим над полето на рационалните числа.

Решение. Очевидно уравнението $f(x)=0$ няма реални корени. Следователно, ако $f(x)=g(x)h(x)$, полиномите $g(x)$ и $h(x)$ също нима да имат реални корени, поради което ще приемат стойности с еднакви знаци за всяко реално x. Нека например $g(x)>0$, $h(x)>0$ (x — произволно реално число). Тъй като $f(a_k)=1$, то $g(a_k)=h(a_k)=1$, $k=1,2,\ldots,n$. Ако степента на $g(x)$ (или на $h(x)$) е $<n$, то $g(x)=1$ (или $h(x)=1$) за всяко x. Следователно всяка от степените на $g(x)$ и $h(x)$ е равна на n. Тогава ще имаме

$$g(x)=1+\alpha(x-a_1)\ldots(x-a_n),\ h(x)=1+\beta(x-a_1)\ldots(x-a_n),$$

където α и β са цели числа. В такъв случай за $f(x)$ получаваме
$f(x)=(x-a_1)^2(x-a_2)^2\ldots(x-a_n)^2+1=1+(\alpha+\beta)(x-a_1)\ldots(x-a_n)+$
$+\alpha\beta(x-a_1)^2\ldots(x-a_n)^2$.

Като сравним коефициентите пред x^{2n} и x^n, за α и β ще получим системата уравнения $\alpha\beta=1$, $\alpha+\beta=0$, която очевидно няма цели решения. Следователно полиномът $f(x)$ е неразложим над полето на рационалните числа.

34. Докажете, че полиномът

$$f(x)=(x-a_1)^4(x-a_2)^4\ldots(x-a_n)^4+1,$$

където $a_1, a_2, \ldots, a_n$ са различни цели числа, е неразложим над полето на рационалните числа.

Решение. Да положим

$$p_0(x)=(x-a_1)(x-a_2)\ldots(x-a_n).$$

Ако полиномът $p_0^4(x)+1$ е разложим, лесно се вижда, че той може да се представи във вида

$$(1)\qquad p_0^4(x)+1=[1-p_0(x)p_{-1}(x)][1-p_0(x)p_1(x)],$$

където $p_{-1}(x)$ и $p_1(x)$ са полиноми с цели коефициенти и със старши коефициенти -1. От (1) следва

$$(2)\qquad p_{-1}(x)+p_1(x)=-p_0(x)t(x).$$

Наистина, тъй като

$$p_0^4(x)=-[p_{-1}(x)+p_1(x)]p_0(x)+p_{-1}(x)p_0^2(x)p_1(x),$$

можем да положим $t(x)=p_0^2(x)-p_1(x)p_{-1}(x)$
и очевидно $t(x)$ ще бъде полином с цели коефициенти. От (1) и (2) получаваме

$$(3)\qquad p_0^2(x)=t(x)+p_{-1}(x)p_1(x).$$

Да допуснем най-напред, че степените n_{-1} и n_1 на полиномите $p_{-1}(x)$ и $p_1(x)$ са равни; тогава съгласно (1) ще имаме $n_{-1}=n_1=n$. Като приравним старшите коефициенти в (2), намираме $t(x)=2$. По-нататък от (2) следва, че $p_{-1}(a_\nu)=-p_1(a_\nu)$ и следователно съгласно (3) ще имаме $p_1^2(a)=2$. Последното обаче е невъзможно, понеже числата $p_1(a_\nu)$ са цели числа. И така степените на $p_{-1}(x)$ и $p_1(x)$ са различни, т. е. $n_1\neq n_1$. Нека сега $n_{-1}>n_1$. Имаме

$$1\equiv p_1^4(x)p_0^4(x)\ [\mathrm{mod}\ (1-p_1(x)p_0(x))]$$

и тогава от (1) получаваме

$$p_1^4(x)+1\equiv p_1^4(x)+p_1^4(x)p_0^4(x)\equiv 0\ (\mathrm{mod}\ (1-p_1(x)p_0(x))],$$

$$(4)\qquad p_1^4(x)+1=[1-p_1(x)p_0(x)][1-p_1(x)p_2(x)],$$

където $p_2(x)$ е полином с цели коефициенти. По-нататък с $p_\lambda(x)$ и $t_\lambda(x)$ ще означаваме полиноми с цели коефициенти. При извеждането на (A) от (I) не използувахме свойствата на корените на полинома $p_0(x)$, така че по аналогичен начин можем да получим

$$(5)\qquad p_\lambda^4(x)+1=[1-p_\lambda(x)p_{\lambda-1}(x)][1-p_\lambda(x)p_{\lambda+1}(x)],$$

$$(6)\qquad p_{\lambda-1}(x)+p_{\lambda+1}(x)=-p_\lambda(x)t_\lambda(x),$$

$$(7)\qquad p_\lambda^2(x)=t_\lambda(x)+p_{\lambda-1}(x)p_{\lambda+1}(x)\quad(\lambda=0,\ 1,\ 2\ldots).$$

Като елиминираме $p_{\lambda-1}(x)$, съответно $p_{\lambda+1}(x)$ от (6) и (7), ще получим

$$\frac{p_\lambda^2(x)+p^2_{\lambda+1}(x)}{1-p_\lambda(x)p_{\lambda+1}(x)}=t_\lambda(x)=\frac{p_\lambda^2(x)+p^2_{\lambda-1}(x)}{1-p_\lambda(x)p_{\lambda-1}(x)}=t_{\lambda-1}(x)=\cdots=t(x).$$

Степените n_λ на полиномите $p_\lambda(x)$ намаляват с едно и също число, защото от (5), вследствие неравенството $n_{-1}>n_1$, имаме

$$2n_\lambda=n_{\lambda-1}+n_{\lambda+1},\quad n_{\lambda-1}-n_\lambda=n_\lambda-n_{\lambda+1},\quad n_{\lambda+1}<n_\lambda.$$

Ето защо ще съществува нулев полином $p_{\nu+1}(x)$. Да положим $y=p_\nu(x)$ и нека $p_\nu(x)\neq 0$ (т. е. $p_\nu(x)$ е последният нулев полином от разглеждания вид). От (7) при $\lambda=\nu$ получаваме $y^2=t(x)$ и следователно съгласно (6) ще имаме

$$p_{\nu-1}(x)=-y^3,\quad p_{\nu-2}(x)=-p_{\nu-1}(x)\,y^2-p_\nu(x)=y^5-y,\ldots$$

От равенствата (6) следва още, че всички $p_\lambda(x)$ са полиноми на y. Да положим $p_\lambda(x)=q^\lambda(x)$; при това степенните показатели в $q_\lambda(y)$ са сравними по модул 4. Поради това, ако α е корен на уравнението $q_\lambda(y)=0$, то и $i\alpha$ е корен на същото уравнение. С изключение на $q_\nu(y)$ и $q_{\nu-1}(y)$ всички полиноми $q_\lambda(y)$ имат различни от нула корени, а следователно и нереални корени. Същото се отнася и до полиномите $p_\lambda(x)$, тъй като $y(x)$ е с рационални коефициенти. Тъй като $p_0(x)$ има само реални нули, то ν трябва да бъде равно на 1 или 0. Първата възможност отпада, понеже в този случай бихме имали $p_0(x)=-p_1^2(x)$, което е невъзможно, понеже всички нули на полинома $p_0(x)$ са различни.

35. Нека $p=4\lambda-1$ е просто число и $\varphi(x)$ да означава полином с цели коефициенти от степен $<2n$. Докажете, че полиномът

$$f(x)=(x^2+1)^n+p\varphi(x)$$

е неразложим над полето на рационалните числа при $p^2\times|\varphi(i)|^2$.

Решение. Да допуснем, че

$$(1)\qquad f(x)=g(x)\,h(x),$$

където без ограничение на общността съгласно лемата на Гаус можем да считаме, че $g(x)$ и $h(x)$ са полиноми с цели коефициенти и степените им са $<2n$. За всеки полином $\phi(x)$ с цели коефициенти с $\bar\phi(x)$ да означим полинома, който се получава от $\phi(x)$, като редуцираме коефициентите му по модул p. Ще разглеждаме $\bar\phi(x)$ като полином от пръстена $Z_p[x]$. От (1) получаваме

$$(2)\qquad \bar f(x)=\bar g(x)\,\bar h(x).$$

Очевидно $\bar f(x)=(1+x^2)^n$, където за краткост 1 означава единицата в полето Z_p. И така съгласно (2) имаме

(3) $$(x^2+1)^n=\bar{g}(x)\bar{h}(x).$$

Понеже простото число p има вида $4\lambda-1$, полиномът x^2+1 е неразложим над Z_p. Наистина в противен случай уравнението $x^2+1=0$ трябва да има корен $x_0\in Z_p$ и съгласно теоремата на Ферма от $x_0^2=-1$ би следвало $(x_0^2)^{\frac{p-1}{2}}=x_0^{p-1}=1$, което противоречи на $(-1)^{\frac{p-1}{2}}=(-1)^{2\lambda-1}=-1$.

Съгласно основната теорема за еднозначност на разлагането на неразложими множители ще имаме

$$\bar{g}(x)=\bar{a}(x^2+1)^k,\quad \bar{h}(x)=\bar{b}(x^2+1)^l,$$

където k и l са естествени числа (не е възможно някое от тези числа да е равно на 0, понеже $\varphi(x)$ е от степен $<2n$), $k+l=n$ и $\bar{a}\,\bar{b}=1$ (т.е. a и b са цели числа, удовлетворяващи сравнението $ab\equiv 1 \pmod{p}$). Можем да пишем

$$g(x)=a(x^2+1)^k+pg_1(x),\quad h(x)=b(x^2+1)^l+ph_1(x),$$

където $g_1(x)$ и $h_1(x)$ са полиноми с цели коефициенти. От (1) получаваме

$$f(x)=[a(x^2+1)^k+pg_1(x)]\,[b(x^2+1)^l+ph_1(x)],$$

откъдето при $x=i$ имаме

$$p\varphi(i)=p^2g_1(i)h_1(i).$$

Аналогично

$$p\varphi(-i)=p^2g_1(-i)h_1(-i).$$

От последните две равенства получаваме

$$|\varphi(i)|^2=p^2|g_1(i)|^2|h_1(i)|^2,$$

откъдето би следвало, че $p^2/|\varphi(i)|^2$. И така направеното допускане за разложимост на полинома $f(x)$ ни доведе до противоречие с условието на задачата.

36. Нека p е просто число. Докажете, че полиномът

$$f(x)=x^p-a$$

(a — рационално число) е разложим над полето на рационалните числа тогава и само тогава, когато a е p-та степен на рационално число (т. е. когато уравнението $x^p-a=0$ има рационален корен).

Решение. Ще докажем по-общо, че полиномът $f(x)=x^p-a$, разглеждан над произволно поле P, е разложим над P тогава и само тогава, когато уравнението $x^p-a=0$ има корен в P. Да допуснем, че полиномът $f(x)$ е разложим над P, т. е.

$$x^p-a=g(x)h(x),\ g(x),\ h(x)\in P[x]$$

и нека степента r на полинома $g(x)$ удовлетворява неравенството $0<r<p$. Да означим с b свободния член $g(x)$. Нека ω е корен на полинома $f(x)$ и $\alpha_1, \alpha_2, \ldots, \alpha_p$ да са корените на уравнението $x^p-1=0$ ($\omega, \alpha_1, \alpha_2, \ldots, \alpha_p$ са елементи на подходящо разширение на основното поле P). Тогава всичките корени на полинома $f(x)$ ще са

(1) $$\alpha_1\omega,\ \alpha_2\omega, \ldots, \alpha_p\omega.$$

Корените на $g(x)$ са измежду (1). Нека например това са първите r:

$$\alpha_1\omega,\ \alpha_2\omega, \ldots, \alpha_r\omega.$$

По последната формула на Виет за b намираме

$$b=(-1)^r\alpha_1\alpha_2\ldots\alpha_r\omega^r.$$

Оттук получаваме

$$b^p=(-1)^{pr}\omega^{pr}=(-1)^{pr}a^r.$$

Числото r е по-малко от простото число p и следователно $(r,p)=1$. Съществуват цели числа u, v, такива че

$$ur+pv=1.$$

Тогава ще имаме

$$a=a^{ru+pv}=(a^r)^u(a^v)^p=(a^v)^p(-1)^{pru}(b^p)^u=[(-1)^r a^v b^u]^p,$$

т. е. $x_0=(-1)^{ru}a^v b^u\in P$ и x_0 е корен на $f(x)$.

37. Нека p е просто число и a е цяло число, което не се дели на p. Докажете, че полиномът

$$x^p-x+a$$

е неразложим над полето на рационалните числа.

Решение. Ще докажем предварително следното твърдение. Нека P е поле с характеристика $p>0$ и $a\in P$; тогава полиномът $x^p-x+a=f(x)$ е неразложим над P или има корен в P. Нека ω е корен на $f(x)$ в подходящо разширение на P и нека $0, 1, 2, \ldots, p-1$ са елементите на простото поле Z_p, разглеждано като подполе на P. Тогава корените на полинома $f(x)$ са

$$(1)\qquad \omega, \omega+1, \ldots, \omega+(p-1).$$

Нека $f(x)$ е разложим над P, т. е.

$$f(x)=g(x)h(x),\ g(x),\ h(x)\in P[x]$$

и нека например степента r на полинома $g(x)$ удовлетворява условието $0<r<p$. Корените на $g(x)$ са измежду елементите (1). Нека те са

$$i_1+\omega, \omega+i_2, \ldots, \omega+i_r.$$

За коефициента b пред $(r-1)$-вата степен на x в $g(x)$ получаваме

$$-b=r\omega+i_1+i_2+\ldots+i_r,$$

откъдето $r\omega\in P$. Но тъй като $0<r<p$, то r е обратим елемент в Z_p и следователно $\omega\in P$.

Сега, за да установим твърдението на задачата, да допуснем, че полиномът $f(x)=x^p-x+a$ е разложим над полето на рационалните числа. Нека

$$f(x)=g(x)h(x),$$

където $g(x)$ и $h(x)$ са полиноми с цели коефициенти, от степени $r>0$ и $p-r$. Ще извършим редукция по модул p. Получаваме

$$\bar f(x)=\bar g(x)\bar h(x),$$

където $\bar f(x)$, $\bar g(x)$, $\bar h(x)$ са съответните на $f(x)$, $g(x)$, $h(x)$ полиноми от $Z_p[x]$. И така полиномът $\bar f(x)$ се оказа разложим над Z_p. Съгласно доказаното по-горе твърдение това е възможно само когато $\bar f(x)$ има корен в Z_p. Ако този корен е $\bar x_0\in Z_p$, ще имаме $\bar x_0^p-\bar x_0+\bar a=0$, т. е.

$$x_0^p-x_0+a\equiv 0\ (\mathrm{mod}\ p).$$

Според теоремата на Ферма $x_0^p\equiv x_0$. (mod p), така че бихме имали $a\equiv 0$ (mod p). Последното обаче противоречи на условието, че a не се дели на p.

38. Нека p е просто число и a е цяло число, което не се дели на p. Докажете, че полиномът

$$f(x)=x^p-x+p\varphi(x)-a,$$

където $\varphi(x)$ е полином с цели коефициенти от степен $\leq p$, е неразложим над полето на рационалните числа.

Упътване. Използвайте решението на предната задача.

39. Нека $f(x)$ е полином с цели коефициенти от степен n, със старши коефициент 1 и свободен член $f(0)\neq 0$. Докажете, че ако $f(x)$ има точно $n-1$ корена в кръга $|x|<1$, или ако има точно $n-2$ корена в кръга $|x|<1$, а останалите два корена са комплексно спрегнати, то полиномът $f(x)$ е неразложим над полето на рационалните числа.

Решение. Нека $f(x)=g(x)h(x)$, където $g(x)$ и $h(x)$ са полиноми с цели коефициенти, $g(x)\neq\text{const}$, $h(x)\neq\text{const}$. От направените предположения следва, че всички нули на поне един от тези полиноми, например $g(x)$, лежат в кръга $|x|<1$. Тогава по формулите на Виет за свободния член b на $g(x)$ получаваме $|b|<1$, откъдето следва, че цялото число b е равно на 0. Следователно $f(0)=0$, с което достигаме до противоречие с условието на задачата.

40. Нека $f(x)$ е полином с цели коефициенти и при някое цяло N да имаме $f(N)=p$, p — просто и $f(N-1)\neq 0$. Да предположим още, че всички нули на $f(x)$ лежат в полуравнината R е $x<N-\frac{1}{2}$. Докажете, че полиномът $f(x)$ е неразложим над полето на рационалните числа.

Решение. Да допуснем, че $f(x)=g(x)h(x)$, където $g(x)$ и $h(x)$ са целочислени полиноми най-малко от първа степен. От $f(N)=p$ следва, че или $g(N)$, или $h(N)$ е равно на ± 1. Нека напр. $g(N)=1$. Тъй като корените на $g(x)$ са измежду тези на $f(x)$, ще имаме

$$g(x)=c(x-x_1)(x-x_2)\ldots(x-x_k),$$

където

$$\operatorname{Re} x_i<N-\frac{1}{2},\quad i=1, 2,\ldots, k.$$

Понеже $g(N-1)$ е цяло число, различно от 0, то $\left|\frac{g(N)}{g(N-1)}\right|\leq 1$. Обаче от разлагането на $g(x)$ на линейни множители следва

$$\prod_{i=1}^{k}\left|\frac{N-x_i}{N-1-x_i}\right|\leq 1.$$

Очевидно от $\operatorname{Re} x_i<N-\frac{1}{2}$ следва $\left|\frac{N-x_i}{N-1-x_i}\right|>1$, така че

$$\prod_{i=1}^{k}\left|\frac{N-x_i}{N-1-x_i}\right|>1.$$

Полученото противоречие доказва твърдението на задачата.

41. Нека p е просто число, което в бройна система с основа $N>2$ има представянето

$$p=\alpha_n+\alpha_{n-1}N+\alpha_{n-2}N^2+\ldots+\alpha_0N^n$$

$(0\leq\alpha_i\leq N-1,\ i=1, 2,\ldots,n)$. Докажете, че полиномът

$$f(x)=\alpha_n+\alpha_{n-1}x+\alpha_{n-2}x^2+\ldots+\alpha_0x^n$$

е неразложим над полето на рационалните числа.

Решение. Очевидно $f(N-1)\neq 0$ и $f(N)=p$ — просто. Да приложим критерия от предната задача. Достатъчно е да покажем, че всички нули на полинома $f(x)$ лежат в полуравнината $\operatorname{Re} x<N-\frac{1}{2}$. Нека x_0 е кой да е корен на уравнението $f(x)=0$.

Имаме

$$\alpha_0+\alpha_1\frac{1}{x_0}+\alpha_2\frac{1}{x_0^2}+\ldots+\alpha_n\frac{1}{x_0^n}=0.$$

Получаваме

$$\left|\alpha_0+\alpha_1\frac{1}{x_0}\right|=\left|\alpha_2\frac{1}{x_0^2}+\ldots+\alpha_n\frac{1}{x_0^n}\right|,$$

$$\left|\operatorname{Re}\left(\alpha_0+\alpha_1\frac{1}{x_0}\right)\right|\leq\left|\alpha_0+\alpha_1\frac{1}{x_0}\right|\leq\frac{\alpha_2}{|x_0|^2}+\ldots+\frac{\alpha_n}{|x_0|^n}\leq$$

$$\leq(N-1)\left(\frac{1}{|x_0|^2}+\ldots+\frac{1}{|x_0|^n}\right)=(N-1)\frac{1}{|x_0|^2}\frac{1-|x_0|^{-(n-1)}}{1-|x_0|^{-1}}.$$

Без ограничение на общността можем да считаме, че $|x_0|>1$. Получаваме

$$\left|\operatorname{Re}\left(\alpha_0+\alpha_1\frac{1}{x_0}\right)\right|<(N-1)\frac{1}{|x_0|^2}\frac{1}{1-|x_0|^{-1}}.$$

Да положим за краткост $|x_0|=\rho$. Имаме

$$\left|\operatorname{Re}\left(\alpha_0+\alpha_1\frac{1}{x_0}\right)\right|<(N-1)\frac{1}{\rho^2}\frac{1}{\rho-1}.$$

От друга страна, при $\operatorname{Re}(x_0)\geq 0$ е в сила неравенството

$$\operatorname{Re}\left(\alpha_0+\alpha_1\frac{1}{x_0}\right)=\operatorname{Re}\alpha_0+\alpha_1\frac{\operatorname{Re}x_0}{\rho^2}\geq 1.$$

Очевидно условието $\operatorname{Re} x_0\geq 0$ не ограничава общността на разглежданията. И така имаме

$$1<(N-1)\frac{1}{\rho^2}\frac{\rho}{\rho-1}.$$

Полученото квадратно неравенство за ρ е несъвместимо с неравенството $\rho\geq N-\frac{1}{2}$. Следователно $\rho<N-\frac{1}{2}$, откъдето $\operatorname{Re} x_0<N-\frac{1}{2}$.

§ 4. БИНОМНИ УРАВНЕНИЯ. АЛГЕБРИЧНО РЕШАВАНЕ НА УРАВНЕНИЯТА

1. Биномни уравнения

Уравненията от вида

(1) $$x^n-a=0$$

наричат биномни. Корените от биномното уравнение

$$x^n-1=0$$

се наричат ***корени на единицата.*** Ако $\omega_1, \omega_2, \ldots, \omega_n$ са всичките корени на (2) и x_0 е произволен корен на (1), то

(2) $$\omega_1 x_0, \omega_2 x_0, \ldots, \omega_n x_0$$

са всичките корени на (1).

В полето C на комплексните числа корените на (2) се получават по формулата на Моавър:

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

Очевидно произведение и частно на корени на единицата при дадено n също са корени на единицата при същото n.

Определение. Казваме, че един корен α на уравнението (2) *принадлежи на показател* k, когато k е най-малкото естествено число, за което $\alpha^k=1$. Когато $k=n$, коренът α се нарича *примитивен* n-ти корен на единицата.

Ако α е примитивен корен на (2), всичките корени на (2) са

$$1=\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

Също ако α принадлежи на показател k и за някое цяло s имаме $\alpha^s=1$, то k дели s.

Нека a и b са взаимно прости естествени числа. Тогава корените на уравнението

(3) $$x^{ab}=1$$

се получават, като умножим всеки корен на уравнението

(4) $$x^a=1$$

с всеки корен на уравнението

(5) $$x^b=1.$$

Примитивните корени на (3) също се получават, като се умножат всевъзможните примитивни корени на (4) с примитивните корени на (5). Следователно, ако $\varphi(n)$ означава броя на примитивните n-ти корени на единицата, ще имаме:

(6) $$\varphi(ab)=\varphi(a)\,\varphi(b) \text{ при } (a, b)=1.$$

Освен това имаме

(7) $$\varphi(p^\lambda)=p^\lambda-p^{\lambda-1}$$

при всяко просто число p и произволно естествено число λ.

От (6) и (7) получаваме формулата

$$\varphi(n)=n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots,$$

където p, q, r,... са всичките различни прости делители на n.

Функцията $\varphi(n)$ съвпада с известната функция на Ойлер, т. е. $\varphi(n)$ е равна на броя на естествените числа, които са по-малки от n и са взаимно прости с n.

Уравнението, което се удовлетворява от всичките примитивни корени при дадено n, има вида $\Phi_n(x)=0$, където

$$\Phi_n(x)=\frac{(x^n-1)\left(x^{\frac{n}{pq}}-1\right)\left(x^{\frac{n}{pr}}-1\right)\cdots}{\left(x^{\frac{n}{p}}-1\right)\left(x^{\frac{n}{q}}-1\right)\cdots\left(x^{\frac{n}{pqr}}-1\right)\cdots}.$$

В горната формула в числителя фигурират показателите n, $\frac{n}{pq}$, ..., $\frac{n}{pqrs}$, ..., отговарящи на четен брой прости множители, а в знаменателя — на нечетен брой такива множители.

Определение. Казваме, че дадено уравнение $f(x)=0$ се *решава алгебрично (в радикали)*, когато полето на разлагане на $f(x)$ се получава от основното поле P (в което се съдържат коефициентите на $f(x)$) чрез последователно присъединяване на корените на биномни уравнения.

Теорема на Абел — Руфини. Общото уравнение от n-та степен е алгебрично нерешимо при $n>4$.

Теорема на Гаус. Биномното уравнение

$$x^p=1,$$

при p просто число, е решимо в квадратни радикили тогава и само тогава, когато p има вида $p=2^{2^k}+1$. (Простите числа от този вид се наричат числа на Ферма.)

Следствие. Окръжността може да се раздели на n равни части с линийка и пергел само когато естественото число n се разлага на произведените от прости числа на Ферма и на степен на 2.

2. Алгебрично решаване на уравненията от трета степен. Формула на Кардано

Всяко уравнение от трета степен

$$a_0y^3+a_1y^2+a_2y+a_3=0$$

може да се сведе чрез субституцията

$$x=y+\frac{a_1}{3a_0}$$

към уравнение от вида

$$x^3+px+q=0. \tag{8}$$

Корените на уравнението (8) се дават от следната формула на Кардано:

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

Когато уравнението (8) е с реални коефициенти, разграничаваме следните три случая съобразно знака на числото

$$\Delta=\frac{q^2}{4}+\frac{p^3}{27}.$$

а) При $\Delta>0$ уравнението (8) има един реален корен x_1 и два комплексно спрегнати корена x_2, x_3. Ако A и B са двете реални стойности на кубичните корени

$$A=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},\quad B=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$

ще имаме:

$$x_1=A+B$$

$$x_2=-\frac{A+B}{2}+i\frac{A-B}{2}\sqrt{3},$$

$$x_3=-\frac{A+B}{2}-i\frac{A-B}{2}\sqrt{3}.$$

б) При $\Delta=0$ уравнението има корен

$$x_1=2\sqrt[3]{-\frac{q}{2}}$$

и двоен корен

$$x_2=x_3=\sqrt[3]{\frac{q}{2}}.$$

в) При $\Delta<0$ трите корена са реални и могат да се представят в тригонометрична форма по следния начин:

$$x_k=2\sqrt{-\frac{p}{3}}\cos\frac{\varphi+2k\pi}{3},\quad k=1, 2, 3,$$

където

$$\cos\varphi=-\frac{q}{2\sqrt{-\frac{p^3}{27}}},\quad 0\leq\varphi\leq\pi.$$

3. Алгебрично решаване на уравненията от четвърта степен

Всяко уравнение от вида

$$a_0 y^4 + a_1 y^3 + a_2 y^2 + a_3 y + a_4 = 0$$

може да се сведе посредством субституцията

$$y = x - \frac{a_1}{4a_0}$$

към уравнението

$$x^4 + px^2 + qx + r = 0. \tag{9}$$

По метода на Декарт уравнението (9) се представя във вида

$$(x^2 + ux + v)\,(x^2 - ux + v_1) = 0,$$

където

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

а u се определя от кубичното уравнение

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

и равенството $u^2 = y$. По такъв начин уравнението (9) се свежда към квадратните уравнения

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

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

Забележка. По-горе отбелязахме, че общото уравнение от степен $n > 4$ е нерешимо в радикали. Обаче теорията на Галуа дава възможност във всеки конкретен случай да се отговори на въпроса, дали дадено уравнение се решава алгебрично или не. Може да се докаже например, че уравнението

$$x^3\,(x-2)\,(x-4)\ldots(x-2n+6) - 2 = 0$$

е нерешимо алгебрически при всяко просто n.

4. Уравнението от вида $f(x) = 0$, където

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

и $a_{n-k} = a_k$, $k = 0, 1, \ldots, m, n = 2m$ се свежда към уравнение от по-ниска степен посредством субституцията

$$x + \frac{1}{x} = y.$$

При $P_i=x^i+\frac{1}{x^i}$ имаме

$$P_i=yP_{i-1}-P_{i-2},\ i=1,\ 2,\ 3,\dots .$$

Следователно P_i е полином на y от степен i. Тогава уравнението $f(x)=0$ ще приеме вида

$$a_0P_m+a_1P_{m-1}+\cdots+a_{m-1}P_1+a_m=0$$

и ще бъде от m-та степен спрямо y.

Пример. Да се реши в квадратни радикали уравнението:

$$x^5=1.$$

След отстраняване на корена $x=1$ получаваме реципрочното уравнение

$$x^4+x^3+x^2+x+1=0$$

или

$$x^2+\frac{1}{x^2}+x+\frac{1}{x}+1=0,$$

т. е.

$$P_2+P_1+1=0.$$

Имаме

$$P_2=x^2+\frac{1}{x^2}=yP_1-P_0=y^2-2.$$

Така че даденото уравнение се свежда до уравненията

$$y^2+y+1=0$$

и

$$x^2-xy+1=0.$$

Оттук получаваме окончателно:

$$y=-\frac{1}{2}\pm\frac{1}{2}\sqrt{5}$$

и

$$x=\frac{y}{2}\pm\sqrt{\frac{y^2}{4}-1}.$$

1. Решете биномните уравнения и намерете примитивните им корени:

а) $x^3=1$; г) $x^8=1$;

б) $x^4=1$; д) $x^{12}=1$;

в) $x^6=1$; е) $x^{24}=1$.

Отг. а) $1,\ -\frac{1}{2}\pm\frac{i\sqrt{3}}{2}$; б) $\pm1,\ \pm i$; в) $\pm1,\ \pm\frac{1}{2}\pm\frac{i\sqrt{3}}{2},\ -\frac{1}{2}\pm\frac{i\sqrt{3}}{2}$;

г) ± 1, $\pm i$, $\frac{\sqrt{2}}{2}(1\pm i)$, $-\frac{\sqrt{2}}{2}(1\pm i)$; д) ± 1, $\pm i$, $\frac{1}{2}\pm\frac{i\sqrt{3}}{2}$, $-\frac{1}{2}\pm$ $\pm i\frac{\sqrt{3}}{2}$, $\frac{\sqrt{3}}{2}\pm\frac{i}{2}$, $-\frac{\sqrt{3}}{2}\pm\frac{i}{2}$; е) ± 1, $\pm i$, $\frac{1}{2}\pm i\frac{\sqrt{3}}{2}$, $-\frac{1}{2}\pm\frac{i\sqrt{3}}{2}$, $\frac{\sqrt{2}}{2}(1\pm i)$, $-\frac{\sqrt{2}}{2}(1\pm i)$, $\frac{\sqrt{3}}{2}\pm\frac{i}{2}$, $-\frac{\sqrt{3}}{2}\pm\frac{i}{2}$, $\frac{\sqrt{6}+\sqrt{2}}{4}\pm i\frac{\sqrt{6}-\sqrt{2}}{4}$, $-\frac{\sqrt{6}+\sqrt{2}}{4}\pm i\frac{\sqrt{6}-\sqrt{2}}{4}$, $\frac{\sqrt{6}-\sqrt{2}}{4}\pm i\frac{\sqrt{6}+\sqrt{2}}{4}$, $-\frac{\sqrt{6}-\sqrt{2}}{4}\pm i\frac{\sqrt{6}+\sqrt{2}}{4}$.

Примитивните корени са:

а) $-\frac{1}{2}\pm i\frac{\sqrt{3}}{1}$; б) $\pm i$; в) $\frac{1}{2}\pm i\frac{\sqrt{3}}{2}$; г) $\frac{\sqrt{2}}{2}(1\pm i)$, $-\frac{\sqrt{2}}{2}(1\pm i)$;

д) $\frac{\sqrt{3}}{2}\pm\frac{i}{2}$; $-\frac{\sqrt{3}}{2}\pm\frac{i}{2}$; е) $\frac{\sqrt{6}+\sqrt{2}}{4}\pm i\frac{\sqrt{6}-\sqrt{2}}{4}$, $-\frac{\sqrt{6}+\sqrt{2}}{4}\pm i\frac{\sqrt{6}-\sqrt{2}}{4}$, $\frac{\sqrt{6}-\sqrt{2}}{4}\pm i\frac{\sqrt{6}+\sqrt{2}}{4}$, $-\frac{\sqrt{6}-\sqrt{2}}{4}\pm i\frac{\sqrt{6}+\sqrt{2}}{4}$.

2. Решете биномните уравнения:

а) $x^2=-1$; в) $x^4=-1$;

б) $x^3=-1$; г) $x^{12}=-1$.

Отг. а) $\pm i$; б) -1, $\frac{1}{2}\pm i\frac{\sqrt{3}}{2}$; в) $\frac{\sqrt{2}}{2}(1\pm i)$, $-\frac{\sqrt{2}}{2}(1\pm i)$; г) $\frac{\sqrt{2}}{2}(1\pm i)$, $-\frac{\sqrt{2}}{2}(1\pm i)$, $\frac{\sqrt{6}+\sqrt{2}}{4}\pm i\frac{\sqrt{6}-\sqrt{2}}{4}$, $-\frac{\sqrt{6}+\sqrt{2}}{4}\pm i\frac{\sqrt{6}-\sqrt{2}}{4}$, $\frac{\sqrt{6}-\sqrt{2}}{4}\pm$ $\pm i\frac{\sqrt{6}+\sqrt{2}}{4}$, $-\frac{\sqrt{6}-\sqrt{2}}{4}\pm i\frac{\sqrt{6}+\sqrt{2}}{4}$.

3. Решете уравненията:

а) $(x+a)^m-(x-a)^m=0$;

б) $x^n-nax^{n-1}-\binom{n}{2}a^2x^{n-2}-\dots-a^n=0$.

Упътване. Представете първото уравнение във вида

$$\left(\frac{x+a}{x-a}\right)^m=1,$$

а второ — във вида $2x^n=(x+a)^n$.

Отг. а) $x_k=ia\operatorname{ctg}\frac{k\pi}{m}$, $k=1, 2, \dots, m-1$;

б) $x_k=a\,(\omega_k\sqrt[n]{2}-1)^{-1}$, $\omega_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$, $k=0, 1, \dots, n-1$.

4. Покажете, че корените на уравнението

$$\lambda(x-a)^n+\mu(x-b)^n=0$$

при произволни комплексни числа a, b, λ, μ лежат върху окръжност (в частност — права), зависеща от тези числа.

5. Решете уравнението

$$\cos\varphi+\binom{n}{1}\cos(\varphi+\alpha)x+\binom{n}{2}\cos(\varphi+2\alpha)x^2+\cdots+\binom{n}{n}\cos(\varphi+n\alpha)x^n=0.$$

Решение. Да положим

$$S(x)=\cos\varphi+\binom{n}{1}\cos(\varphi+\alpha)x+\cdots+\binom{n}{n}\cos(\varphi+n\alpha)x^n,$$

$$T(x)=\sin\varphi+\binom{n}{1}\sin(\varphi+\alpha)x+\cdots+\binom{n}{n}\sin(\varphi+n\alpha)x^n.$$

Имаме $S(x)+iT(x)=\mu(1+\lambda x)^n$ и $S(x)-iT(x)=\bar{\mu}(1+\bar{\lambda}x)^n$, където $\mu=\cos\varphi+$ $+i\sin\varphi$ и $\lambda=\cos\alpha+i\sin\alpha$. Намираме

$$S(x)=\frac{1}{2}[\mu(1+\lambda x)^n+\bar{\mu}(1+\bar{\lambda}x)^n].$$

Следователно даденото уравнение приема вида

$$\mu(1+\lambda x)^n+\bar{\mu}(1+\bar{\lambda}x)^n=0.$$

Като решим последното уравнение, получаваме

$$x_k=-\frac{\sin\frac{(2k+1)\pi-2\varphi}{2n}}{\sin\frac{(2k+1)\pi-2\varphi-2n\alpha}{2n}},\quad k=0,1,\ldots,n-1.$$

6. Намерете показателя на всеки един от следните корени на единицата:

а) $\omega_k=\cos\frac{2k\pi}{180}+i\sin\frac{2k\pi}{180}$ при $k=27,\ 99,\ 137;$

б) $\omega_k=\cos\frac{2k\pi}{144}+i\sin\frac{2k\pi}{144}$ при $k=10,\ 35,\ 60.$

Отг. а) 20, 20, 180; б) 72, 144, 12.

7. Намерете всички корени на единицата от 28-ма степен, които принадлежат на показател 7.

Отг. $\omega_k=\cos\frac{2k\pi}{7}+i\sin\frac{2k\pi}{7}$, $k=1,\ 2,\ 3,\ 4,\ 5,\ 6.$

8. Нека ω е примитивен корен на единицата от степен $2n$. Пресметнете сбора

$$1+\omega+\omega^2+\cdots+\omega^{n-1}.$$

Отг. $2(1-\omega)^{-1}$.

9. Намерете сбора $S_k=\sum_{i=0}^{n-1}\omega_i^k$, където ω_i са корените на уравнението $x^n=1$.

Отг. $S_k=\begin{cases}0 \text{ при } k\not\equiv 0 \pmod n,\\ n \text{ при } k\equiv 0 \pmod n\end{cases}$

10. Покажете, че

$$\sum_{i=1}^{n-1}(x+\omega_i)^n=n(x^n+1),$$

където ω_i са корените на уравнението $x^n=1$.

11. Нека ω е корен на уравнението $x^n=1$. **Пресметнете:**

а) $1+2\omega+3\omega^2+\cdots+n\omega^{n-1}$;

б) $1+4\omega+9\omega^2+\cdots+n^2\omega^{n-1}$.

Отг. а) $n(\omega-1)^{-1}$ при $\omega\neq 1$ и $\frac{n(n+1)}{2}$ при $\omega=1$;

б) $-[n^2(1-\omega)+2n](1-\omega)^{-2}$ при $\omega\neq 1$ и $\frac{n(n+1)(2n+1)}{6}$ при $\omega=1$.

12. Нека ω е корен на единицата, който принадлежи на показател k. Покажете, че ако $\omega^n=1$, то k дели n.

Решение. Нека $n=kq+r$, където $0\leq r<k$; тогава

$$\omega^n=\omega^{kq}\omega^r=\omega^r=1$$

и от дефиницията на показател следва $r=0$, т. е. k дели n.

13. Нека ω е корен на единицата, принадлежащ на показател k, и n е произволно естествено число. Покажете, че ω^n принадлежи на показател $\frac{k}{(k,n)}$. В частност при $(k,n)=1$; ω^n също принадлежи на показател k, откъдето следва, че ако биномното уравнение $x^m=1$ има един примитивен корен, то има точно $\varphi(m)$ на брой примитивни корени.

Забележка. Съществуването на примитивен корен на биномното уравнение $x^m=1$, разглеждано над полето на комплексните числа, следва директно от формулата на Моавър (примитивен корен е например $\xi=\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}$). Съществуването на примитивен корен в случая на произволно поле ще бъде доказано по-нататък.

Решение. Нека $d=(k,n)$, $k=k_1d$, $n=n_1d$ и l е показателят, на който принадлежи ω^n. Имаме $\omega^{nl}=1$ и съгласно предната задача k дели nl, т. е. k_1 дели n_1l. Но $(k_1,n_1)=1$ и следователно k_1 дели l. От друга страна, $(\omega^n)^{k_1}=\omega^{nk_1}=\omega^{kn_1}=1$, откъдето $l\leq k_1$ и следователно $l=k_1$.

14. Покажете, че ако ω_1 и ω_2 са корени на единицата, принадлежащи на показатели съответно m и n, $(m,n)=1$, произведението $\omega=\omega_1\omega_2$ принадлежи на показател mn.

Решение. Нека l е показателят, на който принадлежи ω. Очевидно $\omega^{mn}=1$, откъдето $l \leq mn$. По-нататък имаме $1=\omega^{lm}=\omega_1^{lm}\omega_2^{lm}=\omega_2^{lm}$ и съгласно зад. 13 n дели lm. Но $(m, n)=1$ и следователно n дели l. Аналогично се доказва, че m дели l. Понеже $(m, n)=1$, ще имаме mn дели l. И така $l=mn$.

15. Покажете, че ако $(m, n)=1$, всеки корен ω на уравнението $x^{mn}=1$ еднозначно се представя във вида $\omega=\omega_1\omega_2$, където ω_1 е корен на уравнението $x^n=1$, а ω_2 — на уравнението $x^m=1$.

Решение Нека u, v са цели числа, за които $un+vm=1$. Да положим $\omega_1=\omega^{vm}$ и $\omega_2=\omega^{un}$. Очевидно $\omega=\omega_1\omega_2$ и $\omega_1^n=1$, $\omega_2^m=1$. От друга страна, нека $\omega=\varepsilon_1\varepsilon_2$, където $\varepsilon_1^n=1$ $\varepsilon_2^m=1$. Тогава $\omega^m=\varepsilon_1^m$ и $\omega^m=\omega_1^m$, откъдето $\varepsilon_1^m=\omega_1^m$ и следователно $\varepsilon_1^{vm}=\omega_1^{vm}$, т. е. $\omega_1^{1-un}=\varepsilon_1^{1-un}$. Тъй като $\omega_1^{-un}=\varepsilon_1^{-un}=1$, ще имаме $\varepsilon_1=\omega_1$. Аналогично получаваме $\varepsilon_2=\omega_2$.

16. Покажете, че ако характеристиката на основното поле е $p>0$, единственият корен на единицата от степен p^λ е 1. По-общо, ако $n=p^\lambda m$, $(p, m)=1$, корените на биномното уравнение $x^n=1$ съвпадат с корените на биномното уравнение $x^m=1$ и последното уравнение има m различни корена.

Упътване. Използувайте тъждеството $(x^m-1)^{p^\lambda}=x^n-1$.

17. Нека P е поле и n е естествено число. Покажете, че в полето на разлагане на полинома $x^n-1 \in P[x]$ съществува примитивен n-ти корен на единицата. Тук предполагаме, че в случая на поле P с характеристика $p>0$ е изпълнено условието $(n, p)=1$.

Решение. Най-напред ще разгледаме случая, когато n има вида $n=q^\lambda$, q-просто, $\lambda>0$. Нека $\omega_1, \omega_2, \ldots, \omega_n$ са корените на уравнението $x^n=1$ в съответното поле на разлагане и $\mu \leq \lambda$ е най-големият възможен показател, за който някой от тези корени удовлетворява уравнението $x^{q^\mu}=1$. Но тогава и всички корени ω_i, $i=1, 2, \ldots, n$, ще удовлетворяват същото уравнение и понеже те са различни (тъй като производната $(x^n-1)'=nx^{n-1}$ не се анулира за тези корени), то $q^\mu \geq n$, т. е. $\mu=\lambda$. И така съществува корен, принадлежащ на показател n, т. е. примитивен корен.

В общия случай нека $n=q_1^{\lambda_1}q_2^{\lambda_2}\ldots q_k^{\lambda_k}$ е каноничното разлагане на n. Съгласно доказаното по-горе за всяко i съществува корен ω_i, който принадлежи на показател $q_i^{\lambda_i}$. Като вземем пред вид резултата от зад. 14, получаваме, че произведението $\omega=\omega_1\omega_2\ldots\omega_k$ ще принадлежи на показател n.

18. Нека P е крайно поле. Покажете, че съществува елемент $\theta \in P$, такъв че всеки ненулев елемент на P е степен на θ.

Решение. Нека p да означава характеристиката на полето P и $q=p^\lambda$ е броят на елементите на P. Знаем, че всеки ненулев елемент на P удовлетворява уравнението $x^{q-1}=1$ и тъй като ненулевите елементи са $q-1$ на брой, то P е поле на разлагане на полинома $x^{q-1}-1 \in Z_p[x]$, следователно в P съществува корен на единицата от степен $q-1$.

19. Нека P е крайно поле с q на брой елемента. Покажете, че за всяко естествено число k, което дели $q-1$, съществуват точно $\varphi(k)$ елемента на P, принадлежащи на показател k.

Упътване. Използувайте това, че полиномът x^k-1 е делител на $x^{q-1}-1$ и следователно неговото поле на разлагане (също както и в предната задача) съвпада с P.

Определение. Казваме, че цялото число *а принадлежи на показател k по модул n*, когато $(a, n)=1$ и k е най-малкото естествено число, за което $a^k \equiv 1 \pmod{n}$.

Да отбележим, че a принадлежи на показател k по прост модул p тогава и само тогава, когато съответният клас $\bar{a}$ принадлежи на същия показател k.

При $k=\varphi(n)$ ще казваме, че a е примитивен корен по модул n. От резултата на зад. 19 следва, че за всяко просто число p съществува примитивен корен по модул p. Като вземем пред вид и резултата от зад. 13, достигаме до следното важно твърдение: *сравнението $x^{p-1} \equiv 1 \pmod{p}$ има точно $\varphi(p-1)$ примитивни корена по простия модул p.*

20. Намерете всички примитивни корени по модул p, където:

а) $p=5$; б) $p=7$; в) $p=11$; г) $p=13$;
д) $p=17$; е) $p=19$; ж) $p=61$; з) $p=73$.

Отг. а) 2, 3; б) 3, 5; в) 2, 6, 7, 8; г) 2, 6, 7, 11; д) 3, 5, 6, 7, 10, 11, 12, 14; е) 2, 3, 10, 13, 14, 15; ж) 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59; з) 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68.

21. Пресметнете сбора на всички примитивни корени на единицата от степен n, където:

а) $n=15$; б) $n=24$; в) $n=30$; г) $n=60$.

Отг. а) 1; б) 0; в) -1; г) 0

22. Докажете, че сборът на всички примитивни корени от степен n е равен на $\mu(n)$, където $\mu(n)$ е функцията на Мьобиус, дефинирана по следния начин:

$$\mu(n)=\begin{cases} 0, \text{ ако } n \text{ се дели на квадрат на просто число,} \\ 1, \text{ ако } n \text{ е произведение на четен брой различни прости} \\ \text{числа, в частност } M(1)=0, \\ -1, \text{ ако } n \text{ е произведение на нечетен брой различни} \\ \text{прости числа.} \end{cases}$$

Р е ш е н и е. Функцията на Мьобиус притежава следното свойство: ако $n \neq 1$ то $\sum_{d/n} \mu(d)=0$. Да означим с A_n сбора на всички примитивни корени от степен n. Очевидно имаме $A_1=1=\mu(1)$. По-нататък да допуснем, че за всяко $m<n$ имаме $A_m=\mu(m)$.

Тъй като всеки корен от n-та степен принадлежи на показател, който дели n, и обратно, то сумата $\sum_{d/n} A_d$ е равна на сбора на всички корени на единицата от степен n. Съгласно формулите на Виет тя е 0, т. е. $\sum_{d/n} A_d=0$ или

$$A_n=\sum_{\substack{d/n \\ d<n}} Ad=\sum_{\substack{d/n \\ d<n}} \mu(d).$$

Но също така $\mu(n) = -\sum_{\substack{d|n \\ d<n}} \mu(d)$ следователно $A_n = \mu(n)$.

23. Покажете, че за сбора A_{p-1} от примитивните корени по простия модул p е в сила сравнението

$$A_{p-1} \equiv \mu(p-1) \pmod{p}.$$

Проверете последния резултат за примерите от зад. 20.

24. Докажете равенството

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

където $\Phi_k(x)$ е k-тият циклотомичен полином, т. е.

$$\Phi_k(x) = \prod_{i=1}^{\varphi(k)} (x - \xi_i),$$

и ξ_i са примитивните корени на единицата от степен k.

25. Докажете че коефициентите на циклотомичните полиноми $\Phi_n(x)$ са цели числа.

26. Докажете, че ако p е просто число, то

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

27. Докажете, че ако $n = p^\lambda$ е степен на простото число p, то

$$\Phi_n(x) = \Phi_p\left(x^{p^{\lambda-1}}\right).$$

Решение. Непримитивните корени на уравнението $x^{p^\lambda} = 1$ са точно онези корени, които удовлетворяват уравнението $x^{p^{\lambda-1}} = 1$. Следователно

$$\Phi_n(x) = \frac{x^{p^\lambda} - 1}{x^{p^{\lambda-1}} - 1} = \Phi_p\left(x^{p^{\lambda-1}}\right).$$

28. Докажете, че ако $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ е каноничното разлагане на n на прости множители, то

$$\Phi_n(x) = \Phi_{p_1 p_2 \ldots p_k}\left(x^{p_1^{\alpha_1-1} p_2^{\alpha_2-1} \ldots p_k^{\alpha_k-1}}\right).$$

Упътване. Покажете, че полиномите от двете страни на равенството имат едни и същи корени.

29. Покажете, че ако n е нечетно число, то

$$\Phi_{2n}(x) = \Phi_n(-x).$$

30. Покажете, че ако p е просто число и p не дели n, то

$$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

31. Докажете равенството

$$\Phi_n(x)=\frac{(x^n-1)\left(x^{\frac{n}{pq}}-1\right)\left(x^{\frac{n}{pr}}-1\right)\left(x^{\frac{n}{qr}}-1\right)\dots}{\left(x^{\frac{n}{p}}-1\right)\left(x^{\frac{n}{q}}-1\right)\left(x^{\frac{n}{r}}-1\right)\dots\left(x^{\frac{n}{pqr}}-1\right)\dots},$$

където $p,\ q,\ r,\dots$ са различните прости делители на n или все едно

$$\Phi_n(x)=\prod_{d/n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}.$$

Решение. Нека коренът ω от n-та степен принадлежи на показател m; тогава множителят $x-\omega$ ще влиза само в онези биноми x^d-1, за които m/d. При това, ако d пробягва всички делители на n, които се делят на m, $\frac{n}{d}$ ще пробягва всички делители на $\frac{n}{m}$. По такъв начин се убеждаваме, че $x-\omega$ влиза в дясната част $\prod_{d/n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}$ на разглежданото равенство с показател $\sum_{d/\frac{n}{m}}\mu(d)$. Този сбор е равен на нула при $\frac{n}{m}\neq 1$ и на 1 при $n=m$.

32. Намерете в явен вид полиномите:
$\Phi_1(x)$, $\Phi_2(x)$, $\Phi_3(x)$, $\Phi_4(x)$, $\Phi_6(x)$, $\Phi_8(x)$, $\Phi_9(x)$, $\Phi_{10}(x)$, $\Phi_{12}(x)$, $\Phi_{15}(x)$, $\Phi_{105}(x)$.

Отг. $\Phi_1=x-1$, $\Phi_2=x+1$, $\Phi_3=x^2+x+1$, $\Phi_4=x^2+1$, $\Phi_6=x^2-x+1$, $\Phi_8=x^4+1$, $\Phi_9=x^6+x^3+1$, $\Phi_{10}=x^4-x^3+x^2-x+1$, $\Phi_{12}=x^4-x^2+1$, $\Phi_{15}=x^8-x^7+x^5-x^4+x^3-x+1$, $\Phi_{105}=x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39}+x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+x^{31}-x^{28}-x^{26}-x^{24}-x^{22}-x^{20}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}-x^9-x^8-2x^7-x^6-x^5+x^2+x+1$.

33. Пресметнете $\Phi_n(1)$.

Решение. При $n=p$ — просто имаме $\Phi_p(1)=p$. По-нататък нека $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Съгласно зад. 28 в сила е равенството $\Phi_n(1)=\Phi_m(1)$, където $m=p_1p_2\dots p_k$. При $k=1$, т. е. $n=p^\alpha$, получаваме $\Phi_n(1)=p$. Нека $k\geq 2$. Ще покажем, че $\Phi_n(1)=1$. Наистина

$$\Phi_m(x)=\prod_{d/m}(x^d-1)^{\mu\left(\frac{n}{d}\right)}=\prod_{d/m_1}(x^d-1)^{\mu\left(\frac{n}{d}\right)}\cdot\prod_{d/m_1}\left(x^{p_kd}-1\right)^{\mu\left(\frac{h}{dp_k}\right)}$$

$$=\Phi_{m_1}\left(x^{p_k}\right)^{-1}\Phi_{m_1}(x),$$

където $m_1=\frac{m}{p_k}$, и ако $k=2$, имаме $\Phi_{m_1}(1)=p_1$, и следователно $\Phi_m(1)=1$, а при $k>2$ по индукция от $\Phi_{m_1}(1)=1$ получаваме $\Phi_m(1)=1$.

И така: $\Phi_n(1)=p$ при $n=p^\alpha$ и $\Phi_n(1)=1$ за всички n, които не са степени на просто число.

34. Пресметнете $\Phi_n(-1)$.

Решение. При n нечетно $n>1$ съгласно зад. 29 имаме $\Phi_n(-1)=\Phi_{2n}(1)=1$. Нека $n=2^k$; тогава съгласно зад. 28

$$\Phi_n(x)=\frac{x^{2^k}-1}{x^{2^{k-1}}-1}=x^{2^{k-1}}+1,$$

откъдето $\Phi_n(-1)=0$ при $k=1$ и $\Phi_n(-1)=2$ при $k>1$. Нека сега $n=2m$, където $m>1$ е нечетно. Тогава съгласно зад. 29 е в сила равенството $\Phi_n(-1)=\Phi_m(1)$ и следователно, ако $m=p$ е просто, $\Phi_n(-1)=p$ и ако m е съставно, $\Phi_n(-1)=1$. Накрая нека $n=2^k m$, $k>1$ и $m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_l^{\alpha_l}$, където $p_1, p_2, \dots, p_l$ са различни нечетни прости числа. В този случай имаме $\Phi_n(1)=\Phi_{2p_1p_2\dots p_l}(1)$ и следователно $\Phi_n(-1)=\Phi_{2p_1p_2\dots p_k}(-1)$. По такъв начин случаят се свежда към предишния.

35. Докажете, че циклотомичните полиноми $\Phi_n(x)$ са неразложими над полето на рационалните числа.

Решение. Нека $f(x)$ е неразложим делител на $\Phi_n(x)$ със старши коефициент 1 и нека $\Phi_n(x)=f(x)g(x)$. Съгласно лемата на Гаус полиномите $f(x)$ и $g(x)$ са с цели коефициенти. Ще покажем, че $f(x)=\Phi_n(x)$, за което ще бъде достатъчно да установим, че всеки примитивен n-ти корен на единицата е корен и на $f(x)$. Нека ξ е произволен корен на уравнението $f(x)=0$ и p е просто число, взаимно просто с n. Ще покажем, че ξ^p е корен на същото уравнение $f(x)=0$. Да допуснем, че $f(\xi^p)\neq 0$. Тогава $g(\xi^p)=0$, защото ξ^p е примитивен корен и следователно $\Phi_n(\xi^p)=0$. И така ξ е корен на полинома $h(x)=g(x^p)$. Полиномите $f(x)$ и $h(x)$ имат общ корен ξ и понеже полиномът $f(x)$ по предположение е неразложим, следва, че $f(x)$ дели $h(x)$. Сега ще извършим редукция по модул p, като ще означаваме с $\bar{\varphi}(x)\in Z_p[x]$ образа на произволен целочислен полином $\varphi(x)$. Най-напред да отбележим, че полиномите $\bar{f}(x)$ и $\bar{g}(x)$ са взаимно прости. Наистина произведението $f(x)g(x)$ дели полинома x^n-1, така че $\bar{f}(x)\bar{g}(x)$ ще дели същия този полином, разглеждан като елемент на $Z_p[x]$. Ако $\bar{f}(x)$ и $\bar{g}(x)$ не са взаимно прости, последният полином $x^n-1\in Z_p[x]$ ще има кратни корени в някакво разширение на полето Z_p, което обаче е невъзможно, тъй като той е взаимно прост с производната си $(x^n-1)'=nx^{n-1}$ при $(p, n)=1$. И така полиномите $\bar{f}(x)$ и $\bar{g}(x)$ са взаимно прости. По-нататък, понеже $f(x)$ дели $h(x)$, то и $\bar{f}(x)$ ще дели $\bar{h}(x)$. Но $\bar{h}(x)=\bar{g}(x^p)=(\bar{g}(x))^p$ и следователно полиномът $\bar{f}(x)$ не може да бъде взаимно прост с $\bar{g}(x)$. И така от $f(\xi)=0$ следва $f(\xi^p)=0$ за всяко просто p, което не дели n. Оттук следва, че всеки примитивен n-ти корен на единицата е корен на $f(x)=0$, понеже може да бъде получен от кой да е корен на $f(x)=0$ чрез последователно повдигане в степени с прости показатели, неделящи n. Ще отбележим, че при $n=p$—просто, неразложимостта на полинома $\Phi_p(x)=x^{p-1}+x^{p-2}+\dots+x+1$ следва от критерия на Айзенщайн.

36. Разложете полинома x^n-1 на неразложими множители над полето на рационалните числа и напишете явно това разлагане при $n=24$.

Решение. Имаме $x^n-1=\prod_{d|n}\Phi_d(x)$. При $n=24$ получаваме

$$x^{24}-1=(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)(x^4+1)(x^8-x^4+1).$$

37. Разложете полинома x^n-1 на неразложими над полето на реалните числа множители и напишете тези разлагания при $n=5,6,8$.

Отг. $x^5-1=(x-1)(x^2-\frac{\sqrt{5}-1}{2}x+1)(x^2+\frac{\sqrt{5}+1}{2}x+1)$,

$x^6-1=(x-1)(x+1)(x^2-x+1)(x^2+x+1)$,

$x^8-1=(x-1)(x+1)(x^2+1)(x^2+\sqrt{2}\cdot x+1)(x^2-\sqrt{2}\cdot x+1)$.

В общия случай

$$x^{2m}-1=(x^2-1)\prod_{k=1}^{m-1}(x^2-2x\cos\frac{2k\pi}{m}+1),$$

$$x^{2m+1}-1=(x-1)\prod_{k=1}^{m}(x^2-2x\cos\frac{2k\pi}{2m+1}+1).$$

38. Нека $f(x)$ е полином с цели коефициенти и старши коефициент 1, всички корени на който са различни от нула и лежат в единичния кръг $|x|\leq 1$. Покажете, че всички корени на полинома $f(x)$ са корени на единицата, с други думи, $f(x)$ има вида $f(x)=\Phi_{n_1}(x)\Phi_{n_2}(x)\ldots\Phi_{n_k}(x)$, където n_i са някакви положителни числа.

Решение. Да означим корените на полинома $f(x)$ с $x_1, x_2, \ldots, x_n$ и нека

$$f_k(x)=x^n+a_1^k x^{n-1}+\ldots+a_n^{(k)},\quad k=1, 2, 3, \ldots$$

е полиномът с корени $x_1^k, x_2^k, \ldots, x_n^k$, т. е.

$$f_k(x)=\prod_{i=1}^{n}(x-x_i^k).$$

Ще отбележим, че полиномите $f_k(x)$ имат цели коефициенти, тъй като техните коефициенти са симетрични полиноми от корените на полинома $f(x)$, който е с цели коефициенти и със старши коефициент 1. По-нататък за коефициентите $a_i^{(k)}$ имаме

$$|a_i^{(k)}|=\left|\sum x_1^{k}\ldots x_i^k\right|\leq\sum\left|x_1^k\ldots x_i^k\right|\leq\binom{n}{i}\leq 2^n,$$

тъй като $|x_i|\leq 1$. И така коефициентите на полиномите $f_k(x)$ са цели числа, ограничени по модул с независещото от k число 2^n. От това следва, че тези полиноми не могат да бъдат всичките различни. Следователно за някои k и e, $k\neq e$, ще имаме

$$f_k(x)=f_e(x).$$

Тогава и корените на тези два полинома ще съвпадат с точност до реда на записване, с други думи, ще съществува субституция σ, така че $x_i^k=x_{\sigma(i)}^e$ за $i=1, 2, \ldots, n$. Нека p е редът на σ, т. е. $\sigma^p=1$, където 1 е единичната субституция. Последователно намираме

$$x^{k^p}=(x_i^k)^{k^{p-1}}=(x_{\sigma(i)})^{ek^{p-1}}=(x_{\sigma^2(i)})^{e^2k^{p-2}}=\ldots=(x_{\sigma^n(i)})^{e^n}=x_i^{e^n},$$

т. е.

$$x_i^{k^p}=x_i^{e^p}, \quad k=1,\ 2,\ldots,n$$

или

$$x_i^m=1, \quad k=1,2,\ldots,n,$$

където $m=k^p-e^p\neq 0$.

В следващите няколко задачи се разглеждат биномни уравнения над крайни полета и в частност в простите полета Z_p. В последния случай вместо уравнения можем да разглеждаме биномни сравнения от вида $x^n\equiv a \pmod p$. Цялото число a, $(a, p)=1$ наричаме *n-степенен остатък или неостатък* по модул p в зависимост от това, дали сравнението $x^n\equiv a \pmod p$ има решение или не. Когато $n=2$, говорим съответно за *квадратичен остатък* или *квадратичен неостатък*.

39. Нека P е крайно поле с нечетен брой елементи, който да означим с q, и нека $a\in P$, $a\neq 0$. Покажете, че уравнението $x^2=a$ има решение в P тогава и само тогава, когато $a^{\frac{q-1}{2}}=1$. В частност, ако p е нечетно просто число, числото a е квадратичен остатък по модул p тогава и само тогава, когато $a^{\frac{p-1}{2}}\equiv 1 \pmod p$, и a е квадратичен неостатък тогава и само тогава, когато $a^{\frac{p-1}{2}}\equiv -1 \pmod p$.

Решение. Най-напред ще отбележим, че за всяко $a\in P, a\neq 0$ имаме $a^{\frac{q-1}{2}}=1$ или $a^{\frac{q-1}{2}}=-1$, което следва от теоремата на Ферма:

$$0=a^{q-1}-1=(a^{\frac{q-1}{2}}-1)(a^{\frac{q-1}{2}}+1).$$

Ясно е, че двете равенства $a^{\frac{q-1}{2}}=1$ и $a^{\frac{q-1}{2}}=-1$ не могат да бъдат изпълнени едновременно, тъй като по предположение характеристиката на полето P е нечетно число. Ще покажем, че измежду ненулевите елементи на P има точно $\frac{q-1}{2}$ квадрата. Действително, ако $x_1, x_2,\ldots, x_{q-1}$ са всички ненулеви елементи на P, то квадратите в P са $x_1^2, x_2^2,\ldots, x^2_{q-1}$. Два по два елементите на втората редица са равни, защото $x^2=(-x)^2$ и $x\neq -x$ при $x\neq 0$. Но повече от два елемента на редицата от квадратите $x_1^2, x_2^2,\ldots, x^2_{q-1}$ не могат да бъдат равни, защото ако $x_i^2=x_j^2=x_k^2=a$, $i\neq j\neq k\neq i$, уравнението $x^2=a$ ще има три различни корена. Следователно в редицата от квадратите има точно $\frac{1}{2}(q-1)$ различни елемента. По-нататък, ако a е произволен квадрат, т. е. $a=x_i^2$, имаме

$a^{\frac{1}{2}(q-1)}=x_i^{q-1}=1$. Следователно всеки квадрат в P удовлетворява уравнението $x^{\frac{1}{2}(q-1)}=1$. Тъй като в P има точно $\frac{1}{2}(q-1)$ квадрата, а последното уравнение е от степен $\frac{1}{2}(q-1)$, ясно е, че неговите корени са точно онези елементи $a\in P$, за които $a\neq 0$ и уравнението $x^2=a$ има корен в P.

Определение. Нека p е нечетно просто число и a е цяло число, което не се дели на p. Да положим $\left(\frac{a}{p}\right)=1$, когато a е квадратичен остатък по модул p, и $\left(\frac{a}{p}\right)=-1$, когато a е квадратичен неостатък. Така дифенираната функция $\left(\frac{a}{p}\right)$ се нарича *функция на Лежандър* или *символ на Лежандър*.

40. Покажете, че $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ при $a\equiv b \pmod p$.

41. **Критерий на Ойлер.** За произволно число a, което не се дели на простото число p, е в сила сравнението

$$a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right) \pmod p.$$

Упътване. Вж. зад. 39.

42. Покажете, че

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Упътване. Използувайте критерия на Ойлер.

43. Покажете, че

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}},$$

т. е. числото -1 е квадратичен остатък по модул p тогава и само тогава, когато простото число p има вида $p=4\lambda+1$.

44. Покажете, че

$$\left(\frac{2}{p}\right)=(-1)^{\frac{1}{8}(p^2-1)},$$

т. е. числото 2 е квадратичен остатък по модул p за простите числа p от вида $p=8\lambda\pm 1$ и е квадратичен неостатък за простите числа p от вида $p=8\lambda\pm 3$.

Решение. Да разгледаме четните числа

$$(1)\qquad 2, 4, 6, \ldots, 2k, \ldots, p-1$$

и да означим с l броя на онези от тях, които са $>\frac{p-1}{2}$. Директно се проверява, че при $p=8\lambda\pm1$ числото l е четно, а при $p=8\lambda\pm3$ l е нечетно. По-нататък нека $2k\leq\frac{p-1}{2}$ и $2(k+1)>\frac{p-1}{2}$. Разглеждаме числата

(2) $$2,\ 4,\ 6,\ldots,2k,\ 2(k+1)-p,\ 2(k+2)-p,\ldots,(p-1)-p.$$

Не е трудно да се съобрази, че абсолютните стойности на числата (2) изчерпват всички числа от 1 до $\frac{p-1}{2}$, като при това точно l от тях са отрицателни. Следователно произведението на числата от редицата (2) е равно на

$$(-1)^l\left(\frac{p-1}{2}\right)!.$$

Произведението на числата от редицата (1) е равно на

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!.$$

Но числата от редицата (1) са съответно сравними по модул p с тези от редицата (2). Следователно

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv(-1)^l\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\ p)$$

или

$$2^{\frac{p-1}{2}}\equiv(-1)^l\ (\mathrm{mod}\ p).$$

Съгласно критерия на Ойлер получаваме окончателно

$$\left(\frac{2}{p}\right)\equiv(-1)^l\ (\mathrm{mod}\ p),$$

с което твърдението е доказано.

45. Покажете, че биномното сравнение

$$x^4+1\equiv0\ (\mathrm{mod}\ p)$$

има решение, когато простото число p има вида $p=8\lambda+1$ и няма решение, когато p не е от този вид.

Решение. Нека $x_0^4\equiv-1\ (\mathrm{mod}\ p)$. Тогава $x_0^8\equiv1\ (\mathrm{mod}\ p)$, откъдето следва, че x_0 следва, че x_0 принадлежи на показател 8 по модул p. Но по теоремата на Ферма $x_0^{p-1}\equiv1\ (\mathrm{mod}\ p)$ и следователно $8/p-1$, т. е. $p=8\lambda+1$. Обратно, нека $p=8\lambda+1$. Имаме

$$x^{p-1}=x^{8\lambda}=(x^4)^{2\lambda}.$$

Но $x^4\equiv-1\ (\mathrm{mod}\ x^4+1)$, откъдето $x^{8\lambda}\equiv1\ (\mathrm{mod}\ x^4+1)$. Последното сравнение означава, че полиномът $x^{p-1}-1$ се дели на полинома x^4+1. Тъй като $x^{p-1}-1$ се разлага на линейни множители в Z_p, то делителят x^4+1 също ще се разлага на линейни множители в Z_p и следователно уравнението $x^4+1=0$ ще има корен в Z_p. С други думи, сравнението $x^4+1\equiv0\ (\mathrm{mod}\ p)$ ще има решение.

46. Нека P е крайно поле с q на брой елемента, $a\in P$, $a\neq0$ и n е естествено число. Да положим $\delta=(n,\ q-1)$. Покажете, че уравнението $x^n=a$ има корен в P тогава и само тогава, когато $a^{\frac{q-1}{\delta}}=1$, и в този случай броят на корените му е равен на δ.

Решение. Съгласно зад. 18 в полето P съществува такъв елемент θ, че всеки ненулев елемент на P е степен на p. Очевидно θ принадлежи на показател $q-1$. Да разгледаме елементите

(1) $$\theta^n, (\theta^2)^n, \ldots, \left(\theta^{\frac{q-1}{\delta}}\right)^n.$$

Лесно се вижда, че членовете на горната редица са различни елементи на P. По-нататък да отбележим, че всяка n-та степен на елемент $a=x_0^n$, $a \in P$ удовлетворява уравнението $x^{\frac{q-1}{\delta}}=1$, тъй като по теоремата на Ферма ще имаме $a^{\frac{q-1}{\delta}}=x_0^{n\frac{q-1}{\delta}}=\left(x_0^{\frac{n}{\delta}}\right)^{q-1}=1$. Следователно всички елементи от редицата (1) са корени на уравнението $x^{\frac{q-1}{\delta}}=1$. Понеже степента на последното уравнение е $\frac{q-1}{\delta}$, елементите от редицата (1) са всичките му корени. И така уравнението $x^n=a$ има корен в P тогава и само тогава, когато $a^{\frac{q-1}{\delta}}=1$.

Що се отнася до броя на решенията, ясно е, че ако $x^n=a$ и $y^n=a$, то $y=\xi x$, където $\xi^n=1$, и, обратно, така че, ако уравнението $x^n=a$ има поне един корен в P, то ще има точно толкова корена, колкото е броят на корените на единицата от степен n, принадлежащи на P. Елементът θ^i е n-ти корен на единицата тогава и само тогава, когато $\theta^{in}=1$, т. е. $in\equiv 0 \pmod{q-1}$ или все едно $i\frac{n}{\delta}\equiv$ $\equiv 0\left(\mathrm{mod}\ \frac{q-1}{\delta}\right)$.

Като вземем предвид, че

$$\left(\frac{n}{\delta}, \frac{q-1}{\delta}\right)=1,\ i\equiv 0\left(\mathrm{mod}\ \frac{q-1}{\delta}\right),$$

за i получаваме

$$i=0, \frac{q-1}{\delta}, 2\frac{q-1}{\delta}, \ldots, (\delta-1)\frac{q-1}{\delta}.$$

Следователно в P има точно δ на брой n-ти корени на единицата.

Забележка. Ако сме намерили примитивен корен θ, решаването на биномни уравнения в крайни полета може да се сведе към решаване на линейни сравнения. Нека например $P=Z_p$ и g е примитивен корен по модул p. Да решим уравнението $x^n=a$ в Z_p, или все едно сравнението $x^n\equiv a \pmod p$. Нека $a\equiv g^\alpha \pmod p$ и $x\equiv g^\xi \pmod p$: тогава $g^{n\xi-\alpha}\equiv 1 \pmod p$, което е равносилно с $n\xi\equiv\alpha \pmod{p-1}$. Следователно, ако $\xi_1, \xi_2, \ldots, \xi_k$ са всички решения на сравнението $n\xi\equiv$ $\equiv\alpha \pmod{p-1}$, решенията на даденото сравнение $x^n\equiv a \pmod p$ ще бъдат g^{ξ_1}, $g^{\xi_2}, \ldots, g^{\xi_k}$.

47. Изведете резултата от зад. 45 като следствие от твърдението на предната задача.

Следващите няколко задачи са посветени на доказателството на забележителния закон на Гаус за реципрочност на квадратичните остатъци, който гласи: ***за всеки две различни нечетни прости числа p и q е в сила равенството***

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{4}(p-1)(q-1)}.$$

Ще направим някои предварителни бележки. Ако $x \in (Z_p^*$, където Z_p^*, е множеството от всички ненулеви елементи на полето Z_p, дефинираме символа на Лежандър $\left(\frac{x}{p}\right)$, като полагаме $\left(\frac{x}{p}\right)= =\left(\frac{a}{p}\right)$, където цялото число a е произволен представител на класа x. Нека p и q са нечетни прости числа и Q е поле с характеристика q, което съдържа примитивен корен ζ от степен p. (За Q можем да вземем например полето на разлагане на полинома x^p-1, разглеждан над Z_q.) За произволен елемент $x \in Z_p$ дефинираме ζ^x, като полагаме $\zeta^x=\zeta^a$, където a е произволен представител на класа x. За всяко $a \in Z_p^*$ разглеждаме т. нар. *гаусова сума*

$$\tau(a)=\sum_{x\in Z_p^*}\left(\frac{x}{p}\right)\zeta^{ax}.$$

Тези суми, въведени от Гаус, играят важна роля в теорията на алгебричните числа.

48. Покажете, че

$$\tau(a)=\left(\frac{a}{p}\right)\tau(1).$$

Решение. Имаме

$$\tau(a)=\sum_{x\in Z_p^*}\left(\frac{x}{p}\right)\zeta^{ax}=\sum_{x}\left(\frac{xa}{p}\right)\left(\frac{a}{p}\right)\zeta^{ax}=\left(\frac{a}{p}\right)\sum_{x}\left(\frac{xa}{p}\right)\zeta^{ax}.$$

Но когато x пробягва Z_p^*, то и ax пробягва Z_p^*, следователно

$$\sum_{x\in Z_p^*}\left(\frac{xa}{p}\right)\zeta^{ax}=\sum_{x\in Z_p^*}\left(\frac{x}{p}\right)\zeta^{x}=\tau(1).$$

49. Покажете, че

$$\tau^2=\tau(1)^2=\left(\frac{-1}{p}\right)p.$$

Решение. Имаме

$$\tau^2=\sum_{x,y\in Z_p^*}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{x+y}=\sum_{x,y\in Z_p^*}\left(\frac{xy}{p}\right)\zeta^{x+y};$$

Последната сума е разпространена върху всички двойки x, y елементи на Z_p^*; но когато (x, y) пробягва множеството от всички такива двойки, то и (xy, y) пробягва същото множество. Следователно

$$\tau^2=\sum_{x,y}\left(\frac{xy^2}{p}\right)\zeta^{(x+1)y}=\sum_{x,y}\left(\frac{x}{p}\right)\zeta^{(x+1)y}.$$

Да отделим събираемите, за които $x=-1$:

$$\tau^2=\sum_{y\in Z_p^*}\left(\frac{-1}{p}\right)+\sum_{x\neq-1}\left(\frac{x}{p}\right)\sum_{y\in Z_p^*}\zeta^{(x+1)y}=(p-1)\left(\frac{-1}{p}\right)+\sum_{x\neq-1}\left(\frac{x}{p}\right)\sum\zeta^{(x+1)y}.$$

При фиксирано $x\neq-1$ имаме $\sum_y\zeta^{(x+1)y}=-1$, тъй като $(x+1)y$ пробягва Z_p^* и $1+\zeta+\zeta^2+\ldots+\zeta^{p-1}=0$. И така

$$\tau^2=(p-1)\left(\frac{-1}{p}\right)-\sum_{x\neq-1}\left(\frac{x}{p}\right).$$

Но $\sum_{x\in Z_p^*}\left(\frac{x}{p}\right)=0$, защото броят на квадратичните остатъци е равен на броя на квадратичните неостатъци. Следователно

$$\sum_{x\neq-1}\left(\frac{x}{p}\right)=-\left(\frac{-1}{p}\right)$$

$$\tau^2=p\left(\frac{-1}{p}\right).$$

50. Закон за реципрочност на квадратичните остатъци. Нека p и q са две различни нечетни прости числа; тогава

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Доказателство. Понеже Q има характеристика q, имаме

$$\tau^q=\sum_x\left(\frac{x}{p}\right)^q\zeta^{qx}=\sum_x\left(\frac{x}{p}\right)\zeta^{qx}=\tau(q)=\left(\frac{q}{p}\right)\tau,$$

откъдето

$$\tau^{q-1}=\left(\frac{q}{p}\right)$$

($\tau\neq0$, понеже $\tau^2=p\left(\frac{-1}{p}\right)$ и $p\neq0$). От друга страна,

$$\tau^{q-1}=(\tau^2)^{\frac{q-1}{2}}=p^{\frac{q-1}{2}}\left(\frac{-1}{p}\right)^{\frac{q-1}{2}}.$$

Имаме $p^{\frac{q-1}{2}}=\left(\frac{p}{q}\right)$ и $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$, откъдето

$$\tau^{q-1}=\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Получаваме окончателно

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

51. Докажете по метода от предната задача равенството

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Решение. Нека $H=\{1, 3, 5, 7\}$ е множеството от обратимите елементи на пръстена Z_8. За произволен елемент $x\in H$ да положим $\theta(x)=(-1)^{\frac{x^2-1}{8}}$. Лесно се проверява, че

$$\theta(xy)=\theta(x)\,\theta(y).$$

По-нататък нека P е разширение на полето Z_p, което да съдържа примитивен корен ζ от осма степен. За всяко $a\in H$ да положим

$$\tau(a)=\sum_{x\in H}\theta(x)\,\zeta^{ax}.$$

По същия начин, както в решението на зад. 46, получаваме

$$\tau(a)=\theta(a)\,\tau(1).$$

Имаме

$$\tau=\tau(1)=\zeta-\zeta^3-\zeta^5+\zeta^7=(1-\zeta)^2(\zeta-\zeta^5)=\zeta(1-\zeta)^2(1-\zeta^4)=2\zeta(1-\zeta^2),$$

тъй като $\zeta^8=1$ и $\zeta^4=-1$. Получаваме

$$\tau^2=4\zeta^2(1-2\zeta^2+\zeta^4)=-8\zeta^4=8.$$

Понеже полето P има характеристика p по аналогичен начин, както в предната задача, получаваме $\tau^p=\theta(p)\,\tau$, откъдето $\tau^{p-1}=\theta(p)$. От друга страна, имаме

$$\tau^{p-1}=(\tau^2)^{\frac{p-1}{2}}=8^{\frac{p-1}{2}}=\left(\frac{8}{p}\right)=\left(\frac{2}{p}\right)^3=\left(\frac{2}{p}\right).$$

Получаваме окончателно $\left(\frac{2}{p}\right)=\theta\ p=(-1)^{\frac{p^2-1}{8}}$.

52. Покажете, че

$$\left(\frac{3}{p}\right)=\begin{cases}1 & \text{при } p=12\lambda\pm1,\\ -1 & \text{при } p=12\lambda\pm5.\end{cases}$$

Решение. Ще приложим закона за реципрочност на квадратичните остатъци. Имаме

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

Но $\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$ при $p\equiv1 \pmod 3$ и $\left(\frac{p}{3}\right)=\left(\frac{-1}{3}\right)=-1$ при $p\equiv-1 \pmod 3$.

От друга страна, имаме

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{при } p=4\lambda+1,\\ -1 & \text{при } p=4\lambda-1.\end{cases}$$

Получаваме окончателно

$$\left(\frac{3}{p}\right)=\begin{cases}1 & \text{при } p=12\lambda\pm1,\\ -1 & \text{при } p=12\lambda\pm5.\end{cases}$$

53. Пресметнете следните символи на Лежандър:

а) $\left(\frac{438}{593}\right)$; в) $\left(\frac{219}{383}\right)$;

б) $\left(\frac{2023}{1231}\right)$; г) $\left(\frac{365}{997}\right)$.

Решение. И четирите примера се решават по аналогичен начин, като се използва законът на Гаус за реципрочност на квадратичните остатъци и двете негови допълнения от зад. 43 и зад. 44. Да разгледаме решението на пример а). Имаме

$$438=2.3.73$$

и следователно

$$\left(\frac{438}{593}\right)=\left(\frac{2}{593}\right)\left(\frac{3}{593}\right)\left(\frac{73}{593}\right).$$

Да пресметнем всеки от множителите в дясната страна на горното равенство:

$$\left(\frac{2}{593}\right)=1,$$

защото $593\equiv1 \pmod 8$ (вж. зад. 44);

$$\left(\frac{3}{593}\right)=-1,$$

защото $593\equiv5 \pmod{12}$ (вж. напр. зад. 52);

$$\left(\frac{73}{593}\right)=\left(\frac{593}{73}\right)=\left(\frac{9}{73}\right)=\left(\frac{3^2}{73}\right)=1.$$

Следователно

$$\left(\frac{438}{593}\right)=-1.$$

Отг. а) -1; б) 1; в) 1; г) -1.

54. Има ли решение сравнението:

а) $x^2\equiv3 \pmod{37}$; в) $x^2\equiv68 \pmod{113}$;

б) $x^2\equiv 11 \pmod{59}$; г) $x^2\equiv15 \pmod{53}$.

Отг. а) да; б) не; в) не; г) да.

55. Намерете вида на всички прости числа p, за които числото a е квадратичен остатък:

а) $a=-2$; б) $a=-3$; в) $a=5$;
г) $a=72$; д) $a=360$; е) $a=384$.

Отг. а) $p=8\lambda+1$, $8\lambda+3$; б) $p=6\lambda+1$; в) $p=5\lambda\pm1$; г) $p=8\lambda\pm1$; д) $p=40\lambda\pm1$, $40\lambda\pm3$, $40\lambda\pm9$, $40\lambda\pm13$; е) $p=24\lambda\pm1$, $24\lambda\pm5$.

56. Докажете, че съществуват безбройно много прости числа от вида:

а) $4\lambda+1$; б) $6\lambda+1$.

Решение. а) Нека $p_1, p_2, \ldots, p_k$ са k на брой прости числа от вида $4\lambda+1$. Да положим

$$P=(2p_1p_2\ldots p_k)^2+1.$$

Нека p е някакъв прост делител на P. Очевидно >2 и $p\neq p_i$, $i=1, 2, \ldots, k$. Понеже

$$(2p_1p_2\ldots p_k)^2+1\equiv0 \pmod p,$$

имаме $\left(\frac{-1}{p}\right)=1$. Но тогава съгласно зад. 43 числото p трябва да има вида $p=4\lambda+1$. И така, като разполагаме с k на брой прости числа от вида $4\lambda+1$, получихме ново $(k+1)$-во просто число p по същия вид.

б) Задачата се решава по аналогичен начин, както в случая а), като се разгледа числото

$$P=(2p_1p_2\ldots p_k)^2+3,$$

където $p_1, p_2, \ldots, p_k$ са прости числа от вида $6\lambda+1$, и се използува резултатът от предната задача, пункт б).

57. Нека p е фиксирано нечетно просто число и $h(x)$ е функция, дефинирана за всички цели числа x, взаимно прости с p, която не е константа и приема стойности ±1. Да предположим, още че $h(x)$ удовлетворява следните условия:

$$h(xy)=h(x)h(y)$$

и $h(a)=h(b)$ при $a\equiv b \pmod p$.

Докажете, че за всяко x, $(x, p)=1$, е в сила равенството $h(x)=\left(\frac{x}{p}\right)$.

58. Решете кубичното уравнение

$$x^3+3x^2+9x+9=0.$$

Решение. Ще използуваме формулата на Кардано, като предварително ще извършим трансформацията $x=y-1$. Трансформираното уравнение е

$$y^3+6y+2=0.$$

Имаме

$$y_1=A+B,\ y_{2,3}=-\frac{1}{2}(A+B)\pm\frac{\sqrt{3}}{2}(A+B)\ i,$$

където $A=\sqrt[3]{-\frac{q}{2}+\sqrt{\Delta}}$, $B=\sqrt[3]{-\frac{q}{2}-\sqrt{\Delta}}$, $\Delta=\frac{q^2}{4}+\frac{p^3}{27}$

и при $p=6$, $q=2$ получаваме

$$y_1=\sqrt[3]{2}-\sqrt[3]{4},\ y_{2,3}=\frac{1}{2}\left(\sqrt[3]{4}-\sqrt[3]{2}\right)\pm\frac{\sqrt{3}}{2}\left(\sqrt[3]{2}+\sqrt[3]{4}\right)i.$$

Корените на даденото уравнение са

$$x_1=y_1-1=\sqrt[3]{2}-\sqrt[3]{4}-1,\ x_{2,3}=y_{2,3}-1=\frac{1}{2}\left(\sqrt[3]{4}-\sqrt[3]{2}\right)-1\pm\frac{\sqrt{3}}{2}\left(\sqrt[3]{2}+\sqrt[3]{4}\right)i.$$

59. Решете кубичното уравнение

$$x^3-3\sqrt[3]{3}\,x+\sqrt{6}=0.$$

Решение. Тук $p=-3\sqrt[3]{3}$, $q=\sqrt{6}$. За $\Delta=\frac{q^2}{4}+\frac{p^3}{27}$ получаваме $\Delta=-\frac{3}{2}<0$. Следователно налице е т. нар. неразложим случай, когато трите корена на уравнението са различни и реални. Тези корени пресмятаме по формулата

$$x_k=2\sqrt{\frac{-p}{3}}\cos\frac{\varphi+2k\pi}{3},\quad k=0,\ 1,\ 2,$$

където

$$\cos\varphi=-\frac{q}{2\sqrt{\frac{-p^3}{27}}},\quad 0\le\varphi\le\pi.$$

Намираме $\cos\varphi=-\frac{\sqrt{2}}{2}$, $\varphi=\frac{3\pi}{4}$. Окончателно имаме:

$$x_0=2\sqrt[6]{3}\cos\frac{3\pi}{12},\ x_1=2\sqrt[6]{3}\cos\frac{11\pi}{12},\ x_2=2\sqrt[6]{3}\cos\frac{19\pi}{12},$$

т. е.

$$x_0=\sqrt{2}\sqrt[6]{3},\ x_2=-\sqrt[6]{3}(1+\sqrt{3}),\ x_3=\sqrt[3]{6}(\sqrt{3}-1).$$

60. Решете кубичните уравнения:

а) $x^3+9x-26=0$; г) $x^3+6x^2+30x+25=0$;

б) $x^3+12x+63=0$; д) $x^3-3x^2-3x+11=0$;

в) $x^3-3x+1=0$; е) $x^3+3ix^2-3(1+2i)x+10-5i=0$

Отг. а) $x_1=2$, $x_{2,3}=1\pm2i\sqrt{3}$; б) $x_1=-3$, $x_{2,3}=\frac{1}{2}(3\pm i\sqrt{3})$;

в) $x_1=2\cos 40°=1{,}5320888,\dots, x_2=2\cos160°=-2\cos20°=$
$=-1{,}8793852,\dots, x_3=2\cos280°=-0{,}3472964\dots$; г) $x_1=-1$,
$x_{2,3}=\frac{5}{2}(-1\pm i\sqrt{3})$; д) $x_1=1-\sqrt[3]{2}-\sqrt[3]{4}$, $x_{2,3}=$
$=\frac{1}{2}\left(2+\sqrt[3]{2}+\sqrt[3]{4}\right)\pm\frac{i\sqrt{3}}{2}\left(\sqrt[3]{4}-\sqrt[3]{2}\right)$;

е) $x_1=x_2=-1-2i$, $x_3=2+i$.

61. Нека x_1, x_2, x_3 означават корените на уравнението $x^3+px+q=0$. Докажете, като използвате формулата на Кардано, че

$$(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2=-4p^3-27q^2.$$

62. Покажете, че кубичното уравнение $x^3+px+q=0$ може да се реши алгебрично, като се представи във вида

$$a(x+\alpha)^3+b(x+\beta)^3=0.$$

63. Решете следното уравнение от четвърта степен

$$x^4-4x^3+x^2-3=0.$$

Решение. Ще приложим метода на Декарт, като предварително извършим трансформацията $x=y+1$. Трансформираното уравнение е

$$y^4-5y^2-6y-5=0.$$

Имаме

$$y^4-5y^2-6y-5=(y^2+uy+v)(y^2-uy+v_1),$$

където u, v и v_1 се определят от системата

$$\begin{cases} v+v_1-u^2=-5 \\ u(v_1-v)\ =-6 \\ vv_1\ \ \ \ =-5. \end{cases}$$

Като елиминираме v и v_1, получаваме следното уравнение за u: $u^6-10u^4+45u^2-36=0$. Полагайки $u^2=z$, получаваме резолвентното уравнение

$$z^3-10z^2+45z-36=0.$$

Един от корените на последното уравнение е $z_1=1$, откъдето намираме $u=\pm 1$. Получаваме квадратните уравнения

$$y^2+y+1=0 \text{ и } y^2-y-5=0,$$

чиито корени $y_{1,2}=\frac{1}{2}(-1+i\sqrt{3})$, $y_{3,4}=\frac{1}{2}(1\pm\sqrt{21})$ удовлетворяват трансформираното уравнение $y^4-5y^2-6y-5=0$. И така корените на даденото уравнение са

$$x_{1,2}=y_{1,2}+1=\frac{1}{2}(1\pm i\sqrt{3}),\quad x_{3,4}=\frac{1}{2}(3\pm\sqrt{21}).$$

64. Решете уравненията:

а) $x^4+2x^3+x^2-1=0$; в) $x^4+3x^3+7x^2+9x+9=0$;

б) $x^4+8x^3+15x^2-4x-2=0$; г) $4x^4+16x^3+32x^2+8x-39=0$.

Отг. а) $x_{1,2}=-\frac{1}{2}(1\pm\sqrt{5})$, $x_{3,4}=-\frac{1}{2}(1\pm i\sqrt{3})$; б) $x_{1,2}=-2\pm\sqrt{6}$, $x_{3,4}=-2\pm\sqrt{3}$; в) $x_{1,2}=-\frac{1}{4}\left(3-\sqrt{5}\pm i\sqrt{34+6\sqrt{5}}\right)$, $x_{3,4}=-\frac{1}{4}(3+\sqrt{5}\pm i\sqrt{34-6\sqrt{5}})$; г) $x_{1,2}=-\frac{1}{2}(3\pm i\sqrt{17})$, $x_{3,4}=-\frac{1}{2}(1\pm i\sqrt{7})$.

65. Решете реципрочните уравнения:

а) $x^3+2x^2+2x+1=0$;

б) $12x^4+4x^3-21x^2+4x+12=0$;

в) $3x^6-11x^5-x^4+x^2+11x-3=0$;

г) $x^7-3x^5+2x^4+2x^3-3x^2+1=0$.

66. Докажете, че реципрочното уравнение

$$x^{2n}+a_1x^{2n-1}+\ldots+a_nx^n+\ldots+a_1x+1,\ n>2,$$

с реални коефициенти, за което $|a_n| \leq 2$, има поне една двойка нереални комплексно-спрегнати корени.

Решение. Лявата част на уравнението може да се представи във вида $\varphi(x)g(x)$, където

$$\varphi(x)=(x-x_1)(x-x_2)\ldots(x-x_n)=x^n+b_1x^{n-1}+\ldots+b_n$$

и

$$g(x)=\left(x-\frac{1}{x_1}\right)\left(x-\frac{1}{x_2}\right)\ldots\left(x-\frac{1}{x_n}\right)=x^n+\frac{b_{n-1}}{b_n}x^{n-1}+\frac{b_{n-2}}{b_n}x^{n-2}+\ldots+\frac{1}{b_n}.$$

Като приравним коефициентите пред x^n, ще имаме

$$b_1^2+b_2^2+\ldots+b_n^2+1=a_nb_n.$$

Последното равенство при реални $b_\nu, \nu=1, 2, \ldots, n$ и $|a_n|<2$ очевидно е невъзможно. Следователно не е възможно всичките корени $x_1, x_2, \ldots, x_n$ (а тогава и $b_1, b_2, \ldots, b_n$) да са реални числа. В случая, когато $a_n=\pm 2$, е необходимо да имаме $b_n=\pm 1$, $b_1=b_2=b_3=\ldots=b_{n-1}=0$ и твърдението е очевидно.

67. Нека $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ е полином с реални коефициенти. Докажете, че в интервала $(-2, 2)$ има поне една точка x_0, за която $|f(x_0)|>2$.

§ 5. РАЗПРЕДЕЛЕНИЕ НА КОРЕНИТЕ НА АЛГЕБРИЧНИ УРАВНЕНИЯ С КОМПЛЕКСНИ КОЕФИЦИЕНТИ

Горни граници за модулите на корените. Нека

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

е полином с комплексни коефициенти. Всяко едно от следните числа:

а) $1+\max\left|\frac{a_k}{a_0}\right|, \ k=1, 2, \ldots, n;$

б) $\rho+\max\left|\frac{a_k}{a_0\rho^{k-1}}\right|, \ k=1, 2, \ldots, n, \rho>0;$

в) $2\max\sqrt[k]{\left|\frac{a_k}{a_0}\right|}, \ k=1, 2, \ldots, n;$

г) $\left|\frac{a_1}{a_0}\right|+\max\sqrt[k-1]{\left|\frac{a_k}{a_1}\right|}, \ k=1, 2, \ldots, n,$

е горна граница за модулите на корените на уравнението

$$f(x)=0.$$

Въпросът за намиране на долна граница за модулите на корените се свежда към намиране на горна граница за модулите на корените на реципрочното уравнение

$$x^nf\left(\frac{1}{x}\right)=0.$$

Теорема на Гаус—Люка. Нека $f(x)$ е полином с комплексни коефициенти. Всяко изпъкнало множество в гаусовата равнина, което съдържа всички корени на уравнението

$$f(x)=0,$$

съдържа и корените на уравнението $f'(x)=0$.

Теорема на Лагер. Нека $f(x)$ е полином от степен $n \geq 1$ и ξ е произволна точка от гаусовата равнина. Всяка окръжност K, която минава през точките ξ и

$$\xi' = \xi - \frac{nf(\xi)}{f'(\xi)},$$

разделя нулите на $f(x)$, т. е. уравнението $f(x)=0$ има поне един корен вътре в K и поне един вън от K или пък всичките корени на това уравнение лежат върху K.

Забележка. В частност K може да бъде и права и тогава или всички корени на уравнението $f(x)=0$ ще лежат върху K, или то ще има корени и от двете страни на K. Например такъв е случаят, когато една от точките ξ или ξ' съвпада с безкрайната точка на гаусовата равнина.

Теорема на Грейс. Нека L е ненулев линеен функционал в линейното пространство на полиномите над полето на комплексните числа от степени $\leq n$. Да означим с $G_L(t)$ полинома

$$G_L(t) = L(t-x)^n = \sum_{\nu=0}^{n} (-1)^\nu \binom{n}{\nu} L(x^\nu) t^{n-\nu}.$$

(Този полином ще наричаме полином на Грейс относно функционала L). Нека $\varphi(x)$ е полином, за който $L(\varphi)=0$. Тогава всяка кръгова област D, която съдържа всички корени на уравнението $G_L(t)=0$, ще съдържа поне един корен на уравнението $\varphi(x)=0$.

Забележка. Както обикновено, тук под кръгова област се разбира външност или вътрешност на кръг или полуравнина. Освен това уславяме се да считаме, че ако един полином е от степен $k<n$, безкрайната точка $z=\infty$ му е $n-k$-кратна нула.

Понякога теоремата на Грейс се формулира така:

Нека

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

е полином от степен, ненадминаваща n, и между коефициентите на $\varphi(x)$ е в сила линейната връзка

$$a_0\gamma_n + a_1\gamma_{n-1} + \ldots + a_n\gamma_0 = 0,$$

където γ_ν са някакви комплексни числа, не всички равни на нула. Тогава всяка кръгова област D, която съдържа корените на уравнението

$$\sum_{\nu=0}^{n} (-1)^\nu \binom{n}{\nu} \gamma_\nu x^{n-\nu} = 0,$$

съдържа поне един корен на уравнението $\varphi(x)=0$.

Теорема на Хурвиц. За да има уравнението

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0$$

с реални коефициенти само корени с отрицателни реални части, е необходимо и достатъчно да бъдат изпълнени неравенствата

$$\begin{vmatrix} a_1 & a_0 & 0 & 0 & 0 & 0 & \dots \\ a_3 & a_2 & a_1 & a_0 & 0 & 0 & \dots \\ a_5, & a_4 & a_3 & a_2 & a_1 & a_0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{2\lambda-1} & a_{2\lambda-2} & \dots & & & & a_\lambda \end{vmatrix} > 0, \ \lambda=1,2,3,\dots,n,$$

където считаме, че $a_\lambda=0$ при $\lambda>n$.

1. Нека $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$ е полином с комплексни коефициенти, $a_0\neq 0$. Покажете, че корените на уравнението $f(x)=0$ не надминават по абсолютна стойност всяко едно от следните числа:

а) $1+\max\left|\frac{a_k}{a_0}\right|$, $k=1,2,\dots,n$;

б) $\rho+\max\left|\frac{a_k}{a_0\rho^{k-1}}\right|$, $k=1,2,\dots,n$, където ρ е произволно положително число;

в) $2\max\sqrt[k]{\left|\frac{a_k}{a_0}\right|}$ $k=1,2,\dots,n$;

г) $\left|\frac{a_1}{a_0}\right|+\max\sqrt[k-1]{\left|\frac{a_k}{a_1}\right|}$, $k=1,2,\dots,n$.

Решение. а) Нека $\max\left|\frac{a_k}{a_0}\right|=A$. Тогава при $|x|>1$ имаме

$$|f(x)|\geq|a_0x^n|\cdot\left(1-\frac{A}{|x|-1}\right)=|a_0x^n|\,\frac{|x|-1-A}{|x|-1},$$

следователно при $|x|>1+A$, $|f(x)|>0$.

б) Разглеждаме полинома $g(x)=a_0x^n+\frac{a_1}{\rho}x^{n-1}+\frac{a_2}{\rho^2}x^{n-2}+\dots+\frac{a_n}{\rho^n}$. Неговите корени са точно корените на $f(x)$, разделени с ρ. Като приложим а) за $g(x)$, получаваме желаната оценка.

в) Да положим $\rho=\max\sqrt[k]{\left|\frac{a_k}{a_0}\right|}$. Тогава

$$\left|\frac{a_k}{a_0}\right|\leq\rho^k,\ \left|\frac{a_k}{a_0\rho^{k-1}}\right|\leq\rho,\ \max\left|\frac{a_k}{a_0\rho^{k-1}}\right|\leq\rho.$$

Следователно модулите на корените не надминават

$$\rho+\rho=2\rho=2\max\sqrt[k]{\left|\frac{a_k}{a_0}\right|}.$$

г) Да положим $\rho=\max\sqrt[k-1]{\left|\frac{a_k}{a_0}\right|}$. Тогава

$$\left|\frac{a_k}{a_1}\right| \le \rho^{k-1}, \quad \left|\frac{a_k}{a_0\rho^{k-1}}\right| \le \left|\frac{a_1}{a_0}\right|,$$

следователно модулите на корените на $f(x)$ не надминават

$$\rho^{n-1} + \left|\frac{a_1}{a_0}\right| = \left|\frac{a_1}{a_0}\right| + \max \sqrt[k-1]{\left|\frac{a_k}{a_1}\right|}.$$

2. Нека $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ е полином с комплексни коефициенти и A, B да означават двете най-големи измежду числата $|a_1|, \sqrt{|a_2|}, \ldots, \sqrt[n]{|a_n|}$. Покажете, че корените на уравнението $f(x)=0$ лежат в кръга $|x|\le A+B$. (Сравнете с т. в) от предната задача.)

Решение. Нека числата $|a_1|, \sqrt{|a_2|}, \ldots, \sqrt[n]{|a_n|}$ са наредени в растяща редица $c_1, c_2, \ldots, c_n$. Тогава $A=c_{n-1}$ и $B=c_n$. Да положим $|a_{n-s}|=B^{n-s}$ $(0\le s\le \le n-1)$. От равенството $f(x)=0$ следва

$$\rho^{n-1}\le |a_1|\rho^{n-1}+|a_2|\rho^{n-2}+\ldots+|a_n|,$$

където $\rho=|x|$. От последното вследствие на неравенствата $|a_{n-k}|\le A^{n-k}$ при $k\ne s$ и $|a_{n-s}|=B^{n-s}$ получаваме, че

$$\rho^n\le A\rho^{n-1}+A^2\rho^{n-2}+\ldots+A^n+(B^{n-s}-A^{n-s})\rho^s.$$

Последното неравенство може да се запише още във вида

$$1\le Ar\frac{1-(rA)^n}{1-rA}+(B^l-A^l)r^l\ (1\le l\le n), \tag{1}$$

където $r=\rho^{-1}$ и $l=n-s$. (Без ограничение на общността можем да считаме, че $B>0$ и $\rho>0$.) За да завършим доказателството, ще бъде достатъчно да установим, че при $\rho>A+B$ (т. е. при $r<(A+B)^{-1}$) е в сила противоположното на (1) неравенство

$$1>Ar\frac{1-(rA)^n}{1-rA}+(B^l-A^l)r^l\ (1\le l\le n). \tag{2}$$

Последното неравенство е еквивалентно на неравенството

$$1>Ar+A^2r^2+\ldots+A^nr^n+(B^l-A^l)r^l. \tag{3}$$

Понеже дясната страна на (3) е монотонно растяща функция на r в интервала $(0, +\infty)$, достатъчно е да установим, че неравенството (3) е изпълнено при $r=r_0=(A+B)^{-1}$, откъдето ще последва, че то е вярно и при всяко $r\in(0, r_0)$. При $A=0$ и $r>B^{-1}$ (3) очевидно е изпълнено, така че можем да считаме, че $A>0$. При $r=r_0$ и $\frac{B}{A}=t\ge 1$, (3) след известни преобразувания добива вида

$$\frac{t-1}{t}>-\frac{1}{t}\frac{t^n}{(1+t)^n}+\frac{t^l-1}{(1+t)^l}. \tag{4}$$

За да докажем, че неравенството (5) е вярно при всяко $t\ge 1$ и $1\le l\le n$, ще отбележим, че вследствие неравенството

$$\left(\frac{t}{1+t}\right)^n\le\left(\frac{t}{1+t}\right)^l \tag{5}$$

задачата се свежда до доказателството на (4) при $n=l$. С други думи, (4) следва от (5) и от неравенството

$$\frac{t-1}{t}>-\frac{1}{t}\frac{t^l}{(1+t)^l}+\frac{t^l-1}{(1+t)^l},\ (t\ge 1, l\ge 1).$$

Последното неравенство очевидно е изпълнено при $t=1$, а при $t>1$, както лесно се вижда, е еквивалентно с очевидното неравенство

$$(1+t)^t-t^t>\frac{1}{t-1}.$$

С това доказателството е завършено.

3. Нека $f(x)=a_0x^n+a_rx^{n-r}+\ldots+a_n$, $a_0a_r\neq 0$, е полином с комплексни коефициенти. Покажете, че модулите на корените на уравнението $f(x)=0$ не надминават всяко едно от следните числа:

а) $1+\sqrt[r]{\max\left|\frac{a_k}{a_0}\right|}$, $k=r,\ldots,n$;

б) $\rho+\sqrt[r]{\max\left|\frac{a_k}{a_0\rho^{k-r}}\right|}$, $k=r,\ldots,n$, където $\rho>0$ е произволно;

в) $\sqrt[r]{\left|\frac{a_r}{a_0}\right|}+\max\sqrt[k-r]{\left|\frac{a_k}{a_r}\right|}$, $k=r,\ldots,n$.

Упътване. Вж. решението на зад. 1.

4. Покажете, че модулите на корените на уравнението

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n=0$$

не надминават единствения положителен корен на уравнението

$$\varphi(x)=b_0x^n-b_1x^{n-1}-\ldots-b_n=0,$$

където b_i са произволни числа, удовлетворяващи условията $0<b_0\leq|a_0|$, $b_i\geq|a_i|$, $i=1,2,\ldots,n$.

Решение. Имаме

$$\varphi(x)=b_0x^n\left(1-\frac{b_1}{b_0}\frac{1}{x}-\cdots-\frac{b_n}{b_0}\frac{1}{x^n}\right)=b_0x^n\psi(x),$$

откъдето се вижда, че изразът в скобите монотонно расте при $x>0$, като $\lim\limits_{x\to 0}\psi(x)=-\infty$, $\lim\limits_{x\to\infty}\psi(x)=1$. Следователно уравнението $\varphi(x)=0$ има точно един положителен корен ξ. (Това следва също и от теоремата на Декарт.) По-нататък при $|x|>\xi$ имаме

$$|f(x)|\geq\varphi(|x|)>0.$$

5. Докажете, че всички корени на уравнението

$$\frac{A_1}{z-a_1}+\frac{A_2}{z-a_2}+\ldots+\frac{A_n}{z-a_n}=0,$$

където комплексните числа A_k и a_k удовлетворяват условията $A_k\neq 0$, $k=1,2,\ldots,n$; $|a_k-a_1|\geq r>0$, $k=2,3,\ldots,n$, лежат в кръговата област

$$|z-a_1|\geq|A_1|r\left(\sum_{k=1}^{n}|A_k|\right)^{-1}.$$

Решение. За удобство да приемем, че $a_1=0$. Нека ξ е произволен корен на разглежданото уравнение. Тогава ще имаме

$$\frac{A_1}{\xi}=\sum_{k=2}^{n}\frac{A_k}{a_k}\cdot\frac{1}{1-\xi a_k^{-1}},$$

откъдето получаваме

$$\left|\frac{A_1}{\xi}\right|\leqq\sum_{k=2}^{n}\left|\frac{A_k}{a_k}\right|\cdot\frac{1}{1-|\xi| r^{-1}}.$$

Без ограничение на общността можем да допуснем, че $|\xi|<r$. При това предположение от горното неравенство следва

$$|\xi|\geqq |A_1| r\left(|A_1|+r\sum_{k=2}^{n}|A_k a_k^{-1}|\right)^{-1}\geqq |A_1| r\left(\sum_{k=1}^{n}|A_k|\right)^{-1},$$

с което доказателството е завършено.

6. Докажете, че корените на уравнението

$$\frac{1}{z}=\sum_{k=1}^{m}\frac{p_k}{z-a_k},$$

където комплексните числа p_k, a_k удовлетворяват условията

$$\sum_{k=1}^{m}p_k=1,\ |a_k|\geqq 1\ (k=1,2,\dots,m),$$

лежат в кръговата област

$$|z|\geqq\left(1+\sum_{k=1}^{m}|p_k|\right)^{-1}.$$

Упътване. Използувайте предната задача.

7. (Прецизиране на резултата от предната задача.) Всички корени на уравнението

$$\frac{1}{z}=\sum_{k=1}^{m}\frac{p_k}{z-a_k},$$

където комплексните числа p_k, a_k удовлетворяват условията

$$\sum_{k=1}^{m}p_k=1,\ |a_k|\geqq 1\ (k=1,2,\dots,m),$$

лежат в кръговата област

$$|z| \geq \left(\sum_{k=1}^{m} |p_k|\right)^{-1}.$$

Решение. Да допуснем, че не всички p_k са положителни, и да положим $\sigma = \sum_{k=1}^{m} |p_k|$. Тогава очевидно ще имаме $\sigma > 1$. Нека z_0 е корен на даденото уравнение и да допуснем, че $|z_0| < \sigma^{-1}$. Както ще видим по-нататък, това допускане ще ни доведе до противоречие. Условието, че z_0 е корен на даденото уравнение, може да се запише във вида

$$-1 = \sum_{k=1}^{m} p_k \xi_k,$$

където $\xi_k = (a_k w - 1)^{-1}$, $w = z_0^{-1}$. Да разгледаме трансформацията $\xi = (u-1)^{-1}$. Последната изобразява кръгова област $|u| > \sigma$ в кръга $|\xi - c| < r$, където $c = (\sigma^2 - 1)^{-1}$ и $r = \sigma(\sigma^2 - 1)^{-1}$. Според допускането $|z_0| < \sigma^{-1}$, т. е. $|w| > \sigma$ и вследствие на неравенствата $|a_k| \geq 1$, $k = 1, 2, \ldots, m$, имаме $|a_k w| > \sigma$. Следователно $|\xi_k - c| < r$. По-нататък лесно се получава, като се вземе пред вид още и $\sum_{k=1}^{m} p_k = 1$, че числото $V = \sum_{k=1}^{m} p_k \xi_k$ трябва да удовлетворява неравенството

$$|V - c| < r \sum_{k=1}^{m} |p_k| = \sigma^2(\sigma^2 - 1)^{-1}.$$

Но щом като z_0 е корен на разглежданото уравнение, то $V = -1$ и достигаме до абсурдното неравенство

$$|-1 - c| = \sigma^2(\sigma^2 - 1)^{-1} < \sigma^2(\sigma^2 - 1)^{-1}.$$

И така допускането, че даденото уравнение има корен в кръга $|z| < \left(\sum_{k=1}^{m} |p_k|\right)^{-1}$, ни доведе до противоречие.

Случаят, когато всички p_k са положителни, може да се разгледа аналогично на предишния или пък да се сведе към него чрез малки изменения на p_k, като се използуват съображения за непрекъснатост.

8. Нека $\varphi(x)$ е полином от степен, ненадминаваща $n-1$, и $P(x)$ е полином от степен n, чиито нули $a_1, a_2, \ldots, a_n$ са прости и лежат извън кръга $|z| < r$. Докажете, че корените на уравнението $\varphi(x) = 0$ лежат в кръговата област

$$|x| \geqq \left| \frac{\varphi(0)}{P(0)} \left(\sum_{k=1}^{n} \left| \frac{\varphi(a_k)}{P'(a_k)a_k} \right| \right)^{-1} \right| \cdot r.$$

Упътване. Използувайте резултата от предната задача, като вземете пред вид, че съгласно интерполационната формула на Лагранж корените на уравнението $\varphi(x)=0$, които не анулират $P(x)$, удовлетворяват уравнението

$$\sum_{k=1}^{n} \frac{\varphi(a_k)}{P'(a_k)} \cdot \frac{1}{x-a_k} = 0,$$

което от своя страна може да се запише във вида

$$\frac{1}{x} = \sum_{k=1}^{n} \frac{p_k}{x-a_k}$$

при

$$p_k = \frac{\varphi(a_k)}{P'(a_k)a_k} \left(\sum_{k=1}^{n} \frac{\varphi(a_k)}{P'(a_k)a_k} \right)^{-1} = \frac{\varphi(a_k)}{P'(a_k)a_k} \cdot \frac{P(0)}{\varphi(0)}.$$

9. Нека $f(x)$ е полином от степен, ненадминаваща $n-1$, и $\omega_0=1, \omega_1, \ldots, \omega_{n-1}$ са корените на биномното уравнение $x^n=1$. Докажете, че корените на уравнението $f(x)=0$ лежат в кръговата област

$$|x| \geqq |f(0)| \left(\frac{1}{n} \sum_{k=0}^{n-1} |f(\omega_k)| \right)^{-1}.$$

Упътване. Използувайте предната задача при $P(x)=x^n-1$.

10. Докажете, че всички корени на уравнението

$$\alpha_0 + \alpha_1 x + \ldots + \alpha_m x^m = 0$$

лежат в областта

$$|x| \geqq |\alpha_0| (|\alpha_0|^2 + |\alpha_1|^2 + \ldots + |\alpha_m|^2)^{-\frac{1}{2}}.$$

Упътване. Използувайте предната задача при $n=m+1$, като за $\sum_{k=0}^{n-1} |f(\omega_k)|$ приложите неравенството на Буняковски

$$\frac{1}{n} \sum_{k=0}^{n-1} |f(\omega_k)| \leq \frac{1}{n} \sqrt{\sum_{k=0}^{n-1} |f(\omega_k)|^2} \sqrt{\sum_{k=0}^{n-1} 1^2}$$

и вземете пред вид, че

$$\sum_{k=0}^{n-1}|f(\omega_k)|^2=n(|\alpha_0|^2+|\alpha_1|^2+\ldots+|\alpha_m|^2).$$

11. Нека q е произволно комплексно число. Докажете, че всички корени на уравнението

$$\alpha_0+\alpha_1x+\ldots+\alpha_mx^m=0$$

лежат в кръговата област

$$|x|\geqq\frac{(m+1)|\alpha_0|}{(m+1)\sqrt{\sum_{k=0}^{m}|\alpha_k-q|^2}+\left|\sum_{\nu=0}^{m}\alpha_\nu\right|-\left|\sum_{\nu=0}^{m}(\alpha_\nu-q)\right|}.$$

Упътване. Да положим $n=m+1$ и $\varphi(x)=f(x)-q(1+x+\ldots+x^m)$, където $f(x)$ означава лявата част на даденото уравнение. Очевидно при $\nu=1, 2,\ldots, n-1$ имаме $f(\omega_\nu)=\varphi(\omega_\nu)$ и $f(\omega_0)=\varphi(1)-nq$. Съгласно зад. 9 корените на уравнението $f(x)=0$ ще лежат в областта

$$|x|\geq\frac{n f(0)}{\sum_{\nu=0}^{n-1}|f(\omega_\nu)|}=\frac{(m+1)f(0)|}{\sum_{\nu=0}^{m}|\varphi(\omega_\nu)|-|\varphi(1)|+|f(1)|}.$$

Остава да се вземе пред вид, че

$$|f(1)|=\left|\sum_{\nu=0}^{m}\alpha_\nu\right|,\quad|\varphi(1)|=\left|\sum_{\nu=1}^{m}(\alpha_\nu-q)\right|$$

и

$$\sum_{\nu=0}^{m}|\varphi(\omega_\nu)|\leqq(m+1)\sqrt{\sum_{\nu=0}^{m}|\varphi(\omega_\nu)|^2}=(m+1)\sqrt{\sum_{\nu=0}^{m}|a_\nu-q|^2}.$$

12. Докажете, че корените на уравнението

$$\lambda x^m+x^{m-1}+\ldots+x+1=0$$

лежат в областта

$$|x|\geqq(m+1)(m|\lambda-1|+|m+\lambda|)^{-1}.$$

Упътване. Използувайте предната задача при $q=1$.

При разглеждане на въпроси, свързани с разпределение на нулите на полиноми, е удобно комплексната равнина да се разглежда допълнена с една несобствена безкрайна точка, която се означава с ∞. По дефиниция приемаме

$$a+\infty=\infty,\quad a\infty=\infty,\quad a\neq 0,\quad \frac{a}{\infty}=0,$$

където a е комплексно число. Изразите $0.\infty$, $\infty-\infty$, $\frac{\infty}{\infty}$ не се дефинират. Също така често си служим с т. нар. дробно-линейни трансформации. В следващите няколко задачи се разглеждат някои основни свойства на тези трансформации.

Определение. Всяко изображение на комплексната равнина в себе си от вида

$$\delta : x \to \frac{ax+b}{cx+d},$$

където $ad-bc\neq 0$, се нарича *дробно-линейна трансформация.*

Дробно-линейните трансформации се разглеждат като изображения на гаусовата равнина, допълнена с безкрайната точка. Имаме

$$\delta(\infty)=\frac{a}{c},\quad \delta\left(-\frac{d}{c}\right)=\infty.$$

13. Докажете, че дробно-линейните трансформации са обратими, и намерете обратната трансформация δ^{-1} на трансформацията

$$\delta : x \longrightarrow \frac{ax+b}{cx+d}.$$

Отг. $\delta^{-1} : x \longrightarrow \frac{dx-b}{-cx+a}$.

14. Покажете, че суперпозицията $\delta=\delta_1\delta_2$ (т. е. $\delta(x)=\delta_1(\delta_2(x))$) на дробно-линейните трансформации

$$\delta_1 : x \longrightarrow \frac{a_1x+b_1}{c_1x+d_1},\quad \delta_2 : x \longrightarrow \frac{a_2x+b_2}{c_2x+d_2}$$

е дробно-линейната трансформация

$$\delta : x \longrightarrow \frac{ax+b}{cx+d},$$

където $\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$.

15. Покажете, че всяка дробно-линейна трансформация може да се представи като суперпозиция на линейни изображения $x \longrightarrow ax$ (*хомотетия* с коефициент $|a|$, последвана от ротация на ъгъл $\operatorname{Arg} a$), $x \longrightarrow x+b$ (*транслация* на вектор b) и дробната трансформация $x \longrightarrow \frac{1}{x}$ (*инверсия* спрямо единичната окръжност, придружена от симетрия относно реалната ос).

Упътване. Използувайте тъждеството

$$\frac{ax+b}{cx+d}=\frac{a}{c}-\frac{ad-bc}{c(cx+d)}.$$

16. Покажете, че всяка дробно-линейна трансформация преобразува окръжност в окръжност (при това правите се разглеждат като окръжности, които минават през безкрайната точка)

Решение. Като вземем пред вид резултата от предната задача без ограничение на общността, можем да разгледаме само трансформацията $x \longrightarrow \frac{1}{x}$.

Нека K е окръжност с уравнение $|x-x_0|=r$. Последното уравнение може да се запише във вида $|x|^2-2\mathrm{Re}\, x\bar{x}_0+|x_0|^2=r^2$. Като заменим x с $\frac{1}{x}$ и се освободим от знаменателя, получаваме

$$1-|x|^2\, 2\,\mathrm{Re}\,\bar{x}_0\frac{1}{x}+(|x_0|^2-r^2)|x|^2=0,$$

т. е.

$$1-2\mathrm{Re}\, x_0x+(|x_0|^2-r^2)|x|^2=0.$$

При $|x_0|\neq r$, т. е. когато дадената окръжност не минава през началото, последното уравнение добива вида

$$|x^2|-2\mathrm{Re}\,\frac{x_0}{|x_0|^2-r^2}\cdot x+\frac{1}{|x|^2-r^2}=0.$$

Това е уравнение на окръжност с център $\frac{x_0}{|x_0|^2-r^2}$ и радиус $\frac{r}{|x_0^2|-r^2}$.

При $|x_0|=r$ дадената окръжност минава през началото и се трансформира в правата с уравнение $1-2\mathrm{Re}\, x_0x=0$.

По-нататък, ако K е права, нейното уравнение може да се запише във вида

$$1-2\mathrm{Re}x_0x=0$$

и с помощта на разсъждения, аналогични на горните, виждаме, че тя се трансформира в окръжността с уравнение $|x-x_0|=|x_0|$.

Накрая, ако K е права през началото, както лесно се вижда, тя се преобразува в симетричната ѝ относно реалната ос права.

17. Покажете, че при дробно-линейна трансформация всяка кръгова област се преобразува в кръгова област (при това под кръгова област се разбира вътрешност или външност на окръжност или полуравнина).

Следващите няколко задачи съдържат доказателства и някои приложения на теоремите на Гаус—Люка, Лагер и Грейс.

18. Теорема на Гаус—Люка. Нека $f(x)$ е произволен полином от степен $n\geq 1$. Всяко изпъкнало множество, което съдържа нулите на полинома $f(x)$, съдържа и нулите на производната $f'(x)$.

Доказателство. Нека c е произволна нула на $f'(x)$ и $x_1, x_2, \ldots, x_n$ са нулите на $f(x)$. Ако полиномът $f(x)$ има кратни нули и c съвпада с някоя от тях, твърдението е очевидно, поради това можем да предположим, че $c\neq x_i$, $i=1,2,\ldots,n$. От тъждеството

$$\frac{f'(x)}{f(x)}=\sum_{k=1}^{n}\frac{1}{(x-x_k)}$$

получаваме

$$\sum_{k=1}^{n}\frac{1}{c-x_k}=0.$$

Последното равенство може да се запише във вида

$$c=\sum_{k=1}^{n}p_k x_k, \tag{1}$$

където

$$p_k=\frac{1}{|c-x_k|^2}\left(\sum_{k=1}^{n}\frac{1}{|c-x_k|^2}\right)^{-1}.$$

Понеже $p_k>0$, $k=1, 2, \ldots, n$, и $\sum_{k=1}^{n}p_k=1$ съгласно (1) точката c ще принадлежи на всяко изпъкнало множество, което съдържа точките $x_1, x_2, \ldots, x_n$.

19. Докажете, че уравнението

$$cx^n-x+1=0$$

има поне един корен в кръга $|x-1|\leq 1$.

Решение. В даденото уравнение да извършим трансформацията $y=\frac{1}{x}$. Получаваме уравнението

$$y^n-y^{n-1}+c=0.$$

Да допуснем, че корените на даденото уравнение лежат в областта $|x-1|>1$. Лесно се вижда, че тази област се изобразява при трансформацията $y=x^{-1}$ в полуравнината $\operatorname{Re} x<\frac{1}{2}$. Съгласно теоремата на Гаус — Люка всички корени на производното уравнение

$$ny^{n-1}-(n-1)y^{n-2}=0$$

ще лежат в тази полуравнина. Един от корените обаче е равен на $1-\frac{1}{n}$ и очевидно той не лежи в полуравнината $\operatorname{Re} x<\frac{1}{2}$.

Методът на доказателството позволява да се твърди нещо повече, а именно, че уравнението има поне един корен в кръга $\left|x-\frac{n}{2(n-1)}\right|\leq\frac{n}{2(n-1)}$.

20. Теорема на Лагер. Нека $f(x)$ е полином от степен n. Всяка окръжност K, която минава през точките ξ и $\xi'=\xi-\frac{nf(\xi)}{f'(\xi)}$, където ξ е произволна точка от комплексната равнина, разделя нулите на $f(x)$, т. е. от двете страни на K има поне една нула на $f(x)$ или всичките нули на $f(x)$ лежат върху K.

Доказателство. Нека $x_1, x_2, \ldots, x_n$ да означават нулите на $f(x)$; тогава зависимостта между ξ и ξ' може да се запише във вида

$$\frac{1}{\xi-\xi'}=\frac{1}{n}\sum_{\nu=1}^{n}\frac{1}{\xi-x_\nu}$$

Чрез дробно-линейната трансформация

$$u(x)=\frac{1}{\xi-x}$$

окръжността K се изобразява в окръжност K', която минава през безкрайната точка, т. е. в права. Имаме

$$u(\xi')=\frac{1}{n}\sum_{\nu=1}^{n}u(x_\nu).$$

Остава да се вземе пред вид, че всяка права K, минаваща през центъра на тежестта $u(\xi')$ на точките $u(x_1), \ldots, u(x_n)$, разделя тези точки, т. е. от двете страни на правата K' има поне по една от разглежданите точки или всички те лежат върху K'.

21. При означенията от предната задача намерете ξ' при $\xi=\infty$.

Отг. $\xi'=\frac{1}{n}(x_1+x_2+\ldots+x_n)$.

22. Покажете като следствие от теоремата на Лагер, че всяка права, която минава през нула на полинома $f'(x)$, разделя нулите на $f(x)$, стига разглежданата нула на $f'(x)$ да не е нула на $f(x)$.

Упътване. Използувайте факта, че при $f'(\xi)=0$ и $f(\xi)\neq 0$ имаме $\xi'=\infty$.

23. Докажете теоремата на Гаус—Люка като следствие от предната задача.

24. Ако нулите на полинома $f(x)$ лежат в кръговата област D, то нулите на $f(x)-cf'(x)$ лежат в обединението на областта D и получената от нея чрез транслация на вектор nc област $D+nc$, където n е степента на полинома $f(x)$.

Решение. Ще използуваме теоремата на Лагер. Нека ξ е корен на уравнението $f(x)-cf'(x)=0$. Без ограничение на общността можем да считаме, че ξ не е нула на $f'(x)$ и следователно $f'(\xi)\neq 0$. За точката $\xi'=\xi-\frac{nf(\xi)}{f'(\xi)}$ съгласно равенството $f(\xi)-cf'(\xi)=0$ получаваме $\xi'=\xi-nc$. Ако допуснем, че $\xi\notin D$ и $\xi\notin D+nc$, вследствие на последното равенство ще имаме $\xi'\notin D$. Понеже двете точки ξ и ξ' са извън кръговата област D, през тях можем да прекараме окръжност K, която също да е извън D. Но по теоремата на Лагер окръжността K трябва да разделя нулите на $f(x)$, което противоречи на условието, че те лежат в D.

25. Покажете, че ако $f(x)$ е полином, всички нули на който са реални, уравнението $f(x)-cf'(x)=0$ също има само реални корени.

Упътване. Приложете резултата от предната задача веднъж за долната и веднъж за горната полуравнина, ограничена от реалната ос.

26. **Теорема на Пулен — Ермит.** Нека $f(x)$ и $\varphi(x)$ са два полинома, които имат само реални нули. Покажете, че уравнението

$$\varphi\left(\frac{d}{dx}\right) f(x) = 0$$

също има само реални корени.

Упътване. Приложете няколко пъти резултата от предната задача, като на c давате последователно стойности, равни на нулите на полинома $\varphi(x)$.

27. Докажете, че ако уравнението

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

има само реални корени, то и уравнението

$$a_0\frac{x^n}{0!} + a_1\frac{x^{n-1}}{1!} + \ldots + a_n\frac{1}{n!} = 0$$

има само реални корени.

Решение. Ще приложим теоремата на Пулен — Ермит, където $f(x) = x^n$ и $\varphi(x)$ е лявата страна на даденото уравнение. Имаме

$$\varphi\left(\frac{d}{dx}\right)f(x) = a_0 f^{(n)}(x) + a_1 f^{(n-1)}(x) + \ldots + a_n f(x) = n!\left(a_0\frac{1}{0!} + a_1\frac{x}{1!} + \ldots + a_n\frac{x^n}{n!}\right).$$

Съгласно теоремата на Пулен — Ермит последният полином има само реални нули, откъдето и реципрочният му полином има само реални нули.

28. Покажете, че всеки полином, който има само реални нули, може да се представи като средно аритметично на два непропорционални полинома от същата степен със само реални нули.

Решение. Нека α е произволно реално число. Съгласно зад. 25 полиномите $f(x) - \alpha f'(x)$ и $f(x) + \alpha f'(x)$ имат само реални нули при условие, че $f(x)$ има само реални нули. Имаме

$$f(x) = \frac{1}{2}\left(f_1(x) + f_2(x)\right), \text{ където } f_{1,2}(x) = f(x) \pm \alpha f'(x).$$

Ясно е, че полиномите $f_1(x)$ и $f_2(x)$ не са пропорционални на $f(x)$.

От решението се вижда, че ако полиномът $f(x)$ е нормиран със старши коефициент 1, то и полиномите $f_1(x)$, $f_2(x)$ имат същата нормировка. Освен това при достатъчно малко α полиномите $f_1(x)$ и $f_2(x)$ ще бъдат произволно близки до полинома $f(x)$.

29. Нека $f(x)$ е полином от степен n, всичките нули на който са по модул $\geqq 1$ и нека α_1, α_2 са произволни числа, подчинени на единственото условие $\frac{n\alpha_1}{\alpha_2} \neq 1$. Покажете, че всички корени на уравнението $\alpha_1 x f'(x) - \alpha_2 f(x) = 0$ лежат в областта $|x| \geqq \min\left(1, \left|1 - n\frac{\alpha_1}{\alpha_2}\right|^{-1}\right)$.

Решение. Нека ξ е корен на разглежданото уравнение, т. е.

$$\alpha_1 \xi f'(\xi)=\alpha_2 f(\xi).$$

Да допуснем, че

$$|\xi|<1 \text{ и } |\xi|<\left|1-n\frac{\alpha_1}{\alpha_2}\right|^{-1}.$$

От условието следва, че $f(\xi)\neq 0$ и тогава и $f'(\xi)\neq 0$. Ще използуваме теоремата на Лагер. За точката $\xi'=\xi-\frac{nf(\xi)}{f'(\xi)}$ получаваме

$$\xi'=\left(1-n\frac{\alpha_1}{\alpha_2}\right)\xi$$

и следователно

$$|\xi'|=\left|1-n\frac{\alpha_1}{\alpha_2}\right||\xi|<\left|1-n\frac{\alpha_1}{\alpha_2}\right|.\left|1-n\frac{\alpha_1}{\alpha_2}\right|^{-1}=1.$$

Понеже двете точки ξ и ξ' лежат в единичния кръг $|x|<1$, през тях можем да прекараме окръжност K, която също лежи в този кръг. Съгласно теоремата на Лагер тази окръжност трябва да разделя нулите на полинома $f(x)$, но това противоречи на условието, че всички те са извън единичния кръг.

30. Нека $f(x)$ е полином от степен n, всички нули на който лежат във венеца $r\leqq|x|\leqq R$, и нека α_1, α_2 са произволни числа, подчинени на условието $n\frac{\alpha_1}{\alpha_2}\neq 1$. Покажете, че всички корени на уравнението $\alpha_1 xf'(x)-\alpha_2 f(x)=0$ лежат във венеца

$$r\min\left(1,\left|1-n\frac{\alpha_1}{\alpha_2}\right|^{-1}\right)\leqq|x|\leqq R\max\left(1,\left|1-n\frac{\alpha_1}{\alpha_2}\right|^{-1}\right).$$

Упътване. Използувайте решението на предната задача.

31. Нека полиномът $f(x)$ има всичките си нули в единичния кръг $|x|\leqq 1$ и нека една от нулите му ξ лежи по контура на този кръг. Докажете, че производната $f'(x)$ има поне една нула в кръга $\left|x-\frac{\xi}{2}\right|\leqq\frac{1}{2}$.

Решение. Нека $f(x)=(x-\xi)\varphi(x)$. Нека n означава степента на $f(x)$. Имаме

$$f'(\xi)=\varphi(\xi),\ f''(\xi)=2\varphi'(\xi).$$

Ще приложим теоремата на Лагер за точката ξ и полинома $f'(x)$. За съответната точка ξ' имаме $\xi'=\xi-\frac{(n-1)f'(\xi)}{f''(\xi)}$, т. е.

$$\xi'=\xi-\frac{(n-1)\varphi(\xi)}{2\varphi'(\xi)}.$$

Ако ξ' лежи в разглеждания кръг $\left|x-\frac{\xi}{2}\right|\leqq\frac{1}{2}$, както лесно следва от теоремата на Лагер, полиномът $f'(x)$ ще има поне една нула в този кръг. Затова да допуснем, че $\left|\xi'-\frac{\xi}{2}\right|>1$. Сега да приложим теоремата на Лагер за полинома $\varphi(x)$ и за същата точка ξ. За съответната точка ξ'' имаме

$$\xi''=\xi-\frac{(n-1)\varphi(\xi)}{\varphi'(\xi)}.$$

Получаваме $2\xi'-\xi''=\xi$ и от допуснатото неравенство $\left|\xi'-\frac{\xi}{2}\right|>1$ ще следва, че $|\xi''|>1$. Тогава през точките ξ и ξ'' ще можем да прекараме окръжност K, която съдържа изцяло единичния кръг $|x|\leq 1$. Съгласно теоремата на Лагер извън тази окръжност (с изключение на тривиалния случай, когато всички нули на $\varphi(x)$ съвпадат с ξ и когато твърдението на задачата се проверява директно) ще има поне една нула на $\varphi(x)$, което противоречи на условието, че нулите на $\varphi(x)$ лежат в кръга $|x|\leq 1$.

В следващите няколко задачи с P_n ще означаваме линейното пространство над полето на комплексните числа, състоящо се от всички полиноми (с произволни комплексни коефициенти) от степени, ненадминаващи n.

32. Нека $\delta: x\to\frac{ax+b}{cx+d}$ е дробно-линейна трансформация. За произволно $f\in P_n$ да положим $\delta f(x)=(cx+d)^n f\left(\frac{ax+b}{cx+d}\right)$. Покажете, че изображението $\delta: f\to\delta f$ е линеен оператор в пространството P_n.

33. Нека δ_1 и δ_2 са дробно-линейни трансформации и $f\in P_n$. Докажете, че $(\delta_1\circ\delta_2)f=\delta_2(\delta_1 f)$. (Ще припомним, че $\delta_1\circ\delta_2$ означава суперпозицията на изображенията δ_1 и δ_2, т. е. $\delta_1\circ\delta_2(x)=\delta_1(\delta_2(x))$.)

34. Нека $f\in P_n$ и $x_1, x_2, \ldots, x_n$ са всички (собствени и несобствени) корени на уравнението $f(x)=0$. Покажете, че всичките корени на уравнението $\delta f(x)=0$ са $\delta^{-1}(x_1), \delta^{-1}(x_2), \ldots, \delta^{-1}(x_n)$.

Забележка. Ще припомним условието, че ако степента k на f е $<n$, то безкрайната точка ∞ е $(n-k)$-кратен корен на уравнението $f(x)=0$. Например при $f(x)=x$ корените са $x_1=0$, $x_2=x_3=\ldots=x_n=\infty$. Като направим трансформацията $\delta: x\to\frac{1}{x}$, имаме $\delta f=x^{n-1}$, и корените на трансформираното уравнение $x^{n-1}=0$ ще са $x_1'=\infty$, $x_2'=x_3'=\ldots=x'_n=0$.

35. Нека L е линеен функционал в пространството P_n. Покажете, че изображението $L_\delta=L\circ\delta$, дефинирано чрез

$$L_\delta: f\to L(\delta f),$$

също е линеен функционал.

36. Нека L е линеен функционал в пространството P_n. С G_L означаваме така наречения грейсов полином на функционала L, т. е.

$$G_L(t)=L((t-x)^n)=\sum_{\nu=0}^{n}(-1)^\nu\binom{n}{\nu}t^{n-\nu}L(x^\nu).$$

Докажете равенството

$$G_{L_\sigma}(t)=\Delta^n\delta^{-1}G_L(t),$$

където $\delta: x \to \frac{ax+b}{cx+d}$ е произволна дробно-линейна трансформация с детерминанта $\Delta = ad - bc$.

Решение. Имаме

$$G_{L_\delta}(t) = L_\delta (t-x)^n = L\left((cx+d)^n \quad \left(t - \frac{ax+b}{cx+d}\right)^n\right),$$

откъдето

$$\delta G_{L_\delta}(t) = L\left((ct+d)^n (cx+d)^n \left(\frac{at+b}{ct+d} - \frac{ax+b}{cx+d}\right)^n\right),$$

т. е.

$$\delta G_{L_\delta}(t) = \Delta^n L(t-x)^n = \Delta^n G_L(t).$$

Като умножим с δ^{-1} отляво, получаваме

$$G_{L_\delta}(t) = \Delta^n \delta^{-1} (t-x)^n.$$

37. Теорема на Грейс. Нека L е ненулев линеен функционал в пространството P_n и нека D е кръгова област, която съдържа всичките нули на грейсовия полином $G_L(t)$. Тогава всеки полином $f \in P_n$, за който $L(f) = 0$, има поне една нула в D.

Доказателство. При $n=1$ и $f(x) = ax+b$ имаме

$$L(f) = aL(x) + bL(1) \text{ и } G_L(t) = L(1)t - L(x),$$

откъдето следва, че при $L(f)=0$ уравненията $f(x)=0$ и $G_L(t)=0$ имат един и същ корен, така че в този случай твърдението е очевидно. Нека сега твърдението е доказано за $n-1$. Да допуснем, че твърдението не е вярно за n, т. е. съществува полином $f \in P_n$, за който $L(f)=0$, но всички корени $x_1, x_2, \ldots, x_n$ на уравнението $f(x)=0$ лежат извън кръговата област D, която съдържа всички нули $t_1, t_2, \ldots, t_n$ на $G_L(t)$. Нека δ е дробно-линейна трансформация, за която $\delta(x_n)=\infty$, например $\delta(x) = \frac{1}{x-x_n}$. Да положим

$$L_1 = L_\delta, \quad D_1 = \delta(D), \; f_1 = \delta^{-1} f.$$

От предната задача имаме

$$G_{L_1}(t) = \Delta^n \delta^{-1} G_L(t),$$

откъдето следва, че корените на уравнението $G_{L_1}(t)=0$ са точно $\delta(t_i)$ и следователно те принадлежат на кръговата област D_1. По-нататък корените на полинома $f_1(x)$ са $\delta(x_1), \delta(x_2), \ldots, \delta(x_n)=\infty$, които вследствие на направеното предположение не лежат в $D_1 = \delta(D)$. В частност D_1 не съдържа безкрайната точка и следователно кръговата област D_1 е изпъкнала. Имаме

$$L_1(f_1) = L(\delta f_1) = L(\delta\delta^{-1} f) = L(f) = 0.$$

Понеже полиномът f_1 има една нула в ∞, неговата степен е по-малка от n, т. е. можем да разглеждаме полинома f_1 като елемент на P_{n-1} с нули $\delta(x_1), \delta(x_2), \ldots, \delta(x_{n-1})$. Нека l означава линейния функционал L_1, разглеждан върху подпространството P_{n-1}. Да намерим грейсовия полином G_l. Имаме

$$G_l(t) = l(t-x)^{n-1} = L_1(t-x)^{n-1} = \frac{1}{n} L_1 \frac{d}{dt}(t-x)^n = \frac{1}{n} \frac{d}{dt} G_{L_1}(t).$$

Съгласно теоремата на Гаус — Люка всички нули на G_l лежат в изпъкналото множество D_1. Понеже $l(f_1)=0$, съгласно индукционното предположение f_1 трябва да има поне една нула в D_1, което е противоречие.

38. Друга формулировка на теоремата на Грейс. Нека за полиномите

$$f(x)=a_0+\binom{n}{1}a_1x+\ldots+\binom{n}{n}a_nx^n,$$
$$g(x)=b_0+\binom{n}{1}b_1x+\ldots+\binom{n}{n}b_nx^n$$

е изпълнено равенството

$$a_0b_n-\binom{n}{1}a_1b_{n-1}+\ldots+(-1)^{n-1}\binom{n}{n-1}a_{n-1}b_1+(-1)^na_nb_0=0.$$

(В такъв случай казваме, че полиномите $f(x)$ и $g(x)$ са аполарни.) Докажете, че всяка кръгова област, която съдържа всички нули на $g(x)$, съдържа поне една нула на $f(x)$.

Упътване. Разгледайте линейния функционал L, дефиниран с равенствата $L(x^\nu)=(-1)^\nu b_{n-\nu}$, $\nu=0, 1,\ldots, n$, и покажете, че $g(t)=G_L(t)$ и $L(f)=0$.

39. Нека

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

е полином от степен n, всички нули на който лежат в кръгова област D, и нека

$$g(x)=b_0+\binom{n}{1}b_1x+\binom{n}{2}b_2x^2+\ldots+\binom{n}{n-1}b_{n-1}x^{n-1}+b_nx^n$$

е полином с нули $\beta_1, \beta_2,\ldots, \beta_n$. Покажете, че всяка нула γ на „композирания" полином

$$h(x)=a_0b_0+\binom{n}{1}a_1b_1x+\binom{n}{2}a_2b_2x^2+\ldots+\binom{n}{n-1}a_{n-1}b_{n-1}x^{n-1}+a_nb_nx^n$$

има вида $\gamma=-\beta_\nu\xi$, където ν е някакъв индекс, а ξ е точка от D.

Упътване. Използувайте, че ако γ е нула на $h(x)$, то полиномите $f(x)$ и $x^ng\left(-\frac{\gamma}{x}\right)$ са аполарни.

40. При означенията от предната задача да предположим, че степените на $f(x)$ и $g(x)$ са точно n и че нулите им лежат в единичния кръг $|x|<1$. Покажете, че нулите на композирания полином $h(x)$ също лежат в кръга $|x|<1$.

41. При означенията от зад. 39 да предположим, че степените на полиномите $f(x)$ и $g(x)$ са точно n и че нулите на $f(x)$ лежат в някаква изпъкнала област D, която съдържа началото, а нулите на $g(x)$ са реални и лежат в интервала $[-1, 0]$. Покажете, че нулите на композирания полином лежат в областта D.

42. При предположение, че степените на $f(x)$ и $g(x)$ са точно n, нека нулите на $f(x)$ са реални и лежат в интервала $(-a, a)$, а нулите на $g(x)$ също са реални и лежат в интервала $(-b, 0)$ (или $(0, b)$). Покажете, че нулите на композирания полином $h(x)$ лежат в интервала $(-ab, ba)$ $(a>0,\ b>0)$.

43. Нека нулите на полинома

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n, \quad a_n\neq 0,$$

са реални, а нулите на полинома

$$g(x)=b_0+b_1x+b_2x^2+\ldots+b_nx^n, \quad b_n\neq 0$$

са реални и с еднакъв знак. Покажете, че нулите на полинома

$$h(x)=a_0b_0+a_1b_1x+a_2b_2x^2+\ldots+a_nb_nx^n$$

са реални.

Решение. Най-напред ще покажем, че полиномът $q(x)=\sum_{\nu=0}^{n}\binom{n}{\nu}^2 x^\nu$ има само реални нули. Ще използуваме резултата от зад. 27. Полиномът $\sum_{\nu=0}^{n}\binom{n}{\nu}x^\nu$ очевидно има само реални нули и следователно полиномът $\sum_{\nu=0}^{n}\binom{n}{\nu}\frac{1}{(n-\nu)!}x^\nu$ също има само реални нули. Тогава и реципрочният му полином $\sum_{\nu=0}^{n}\binom{n}{\nu}\frac{1}{(n-\nu)!}x^{n-\nu}$ има само реални нули. Като приложим още веднъж зад. 27, получаваме че полиномът $\sum_{\nu=0}^{n}\binom{n}{\nu}\frac{1}{\nu!(n-\nu)!}x^{n-\nu}$ има само реални нули. Но последният е точно $\frac{1}{n!}q(x)$. И така $q(x)$ има само реални нули. Очевидно всички нули на $q(x)$ са отрицателни. Като композираме $q(x)$ и $f(x)$ от предната задача, получаваме, че полиномът

$$a_0+\binom{n}{1}a_1x+\binom{n}{2}a_2x^2+\ldots+\binom{n}{n}a_nx^n$$

има само реални нули. Композираме последния полином с $g(x)$ и пак вследствие на предната задача виждаме, че полиномът

$$h(x)=a_0b_0+a_1b_1x+a_2b_2x^2+\ldots+a_nb_nx^n$$

има само реални нули.

44. Теорема на Грейс—Хейвуд. Нека $f(x)$ е полином от степен $n\geqq 2$, за който $f(a)=f(b)$. Тогава производният полином $f'(x)$ има поне нула в кръга $\left|x-\frac{a+b}{2}\right|\leq\frac{|a-b|}{2}\operatorname{ctg}\frac{\pi}{n}$.

Доказателство. В пространството P_{n-1} разглеждаме линейния функционал L, дефиниран чрез равенството

$$L(\varphi)=\int_a^b \varphi(x)\,dx.$$

За грейсовия полином на функционала L намираме

$$G_L(t)=L(t-x)^{n-1}=\int_a^b (t-x)^{n-1}dx=\frac{1}{n}((t-a)^n-(t-b)^n),$$

откъдето за нулите t_ν на G_L получаваме $t_\nu=\frac{a+b}{2}+\frac{a-b}{2}\operatorname{ctg}\frac{\nu\pi}{n}, \nu=1, 2, \ldots, n-1$. Съгласно теоремата на Грейс всяка кръгова област, която съдържа t_1, t_2, $\ldots$, t_{n-1}, ще съдържа поне една нула на $f'(x)$ (тъй като $L(f')=\int_a^b f'(x)dx=f(b)-$ $-f(a)=0$). В частност $f'(x)$ има поне една нула в разглеждания кръг.

45. Ако полиномът $f(x)$ от степен $n\geqq 2$ има две нули, които лежат в някакъв кръг с радиус R, производният полином ще има поне една нула в концентричния кръг с радиус $R\operatorname{cosec}\frac{\pi}{n}$.

Упътване. Покажете, че ако α и β са две произволни точки от разглеждания кръг с радиус R, кръгът $\left|x-\frac{\alpha+\beta}{2}\right|\leqq\frac{|\alpha-\beta|}{2}\operatorname{ctg}\frac{\pi}{n}$ се съдържа в концентричния на дадения кръг с радиус $R\operatorname{cosec}\frac{\pi}{n}$.

46. Нека $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ е полином от степен n, всичките нули на който лежат в някаква кръгова област D. Покажете, че за всяко z стойността на полинома $f(x)$ при $x=z$ може да се представи във вида $f(z)=a_0(z-\xi)^n$, където ξ е подходяща точка от D.

Решение. В пространството P_n дефинираме линеен функционал L, за който $L(t-x)^n=f(t)$, т. е. $f(t)$ съвпада с грейсовия полином $G_L(t)$ на функционала L. Да разгледаме полинома

$$\varphi(x)=f(z)-a_0(z-x)^n.$$

Имаме

$$L(\varphi)=f(z)\,L(1)-a_0L(z-x)^n=f(z)a_0-a_0f(z)=0.$$

Следователно съгласно теоремата на Грейс уравнението $\varphi(x)=0$ ще има поне един корен $x=\xi$ в D.

47. Нека h е комплексно число и D е областта, ограничена от две успоредни прави, сключващи с реалната ос ъгъл $\frac{\pi}{2}+\arg h$. Докажете, че ако нулите на полинома $f(x)$ лежат в D, нулите на полинома

$$f_1(x)=f(x+h)+\gamma f(x-h), \quad |\gamma|=1,$$

лежат също в D.

Решение. Ще използуваме теоремата на Грейс. Нека ξ е произволна нула на $f_1(x)$, т. е. $f(\xi+h)+\gamma f(\xi-h)=0$. Да разгледаме функционала L в P_n, дефиниран чрез равенството

$$L(\varphi)=\varphi(\xi+h)+\gamma\varphi(\xi-h), \quad \varphi(x)\in P_n.$$

Имаме $L(f)=0$. За грейсовия полином $G_L(t)$ получаваме

$$G_L(t)=L(t-x)^n=(t-\xi-h)^n+\gamma(t-\xi+h)^n.$$

Корените на уравнението $G_L(t)=0$ очевидно удовлетворяват условието $|t-\xi-h|=|t-\xi+h|$ и следователно лежат на симетралата на отсечката с краища $\xi-h$ и $\xi+h$. Ако допуснем, че $\xi\notin D$, ще можем да намерим полуравнина D', която съдържа всички нули на $G_L(t)$ и няма общи точки с D. Съгласно теоремата на Грейс в D' трябва да има поне една нула на $f(x)$, което обаче противоречи на условието, че всички нули на $f(x)$ лежат в D.

Задачата може да се реши директно и по следния начин. Нека $x_1, x_2, \ldots, x_n$ са нулите на $f(x)$. Тогава лесно се вижда, че отношението

$$\frac{f(x-h)}{f(x+h)}=\frac{x-(x_1+h)}{x-(x_1-h)}\cdot\frac{x-(x_2+h)}{x-(x_2-h)}\cdots\frac{x-(x_n+h)}{x-(x_n-h)}$$

е по модул >1 или <1, когато x се намира вън от D. Това е така, понеже същото твърдение е в сила (при една и съща посока на неравенствата) за всеки един от множителите

$$\frac{x-(x_k+h)}{x-(x_k-h)}, \quad k=1, 2, \ldots, n.$$

Следователно $f_1(x)$ не се анулира вън от D, защото в противен случай би съществувала точка $x=x_0\notin D$, така че $f(x_0+h)+\gamma f(x_0-h)=0$, т. е. $\left|\dfrac{f(x_0-h)}{f(x_0+h)}\right|=1$.

48. Нека h е комплексно число и l е права в гаусовата равнина, сключваща с реалната ос ъгъл $\dfrac{\pi}{2}+\arg h$. Тази права разделя равнината на две полуравнини D_1 и D_2 и нека D_1 е онази от тях, точките на която имат аргументи $>\dfrac{\pi}{2}+\arg h$. Докажете, че ако нулите на полинома $f(x)$ лежат в D, то и нулите на полинома

$$f_1(x)=f(x+h)+\gamma f(x-h), \quad |\gamma|\leqq 1$$

лежат в D_1.

Упътване. Използувайте решението на предната задача.

49. Нека нулите на полинома $f(x)$ лежат в полуравнината $\operatorname{Re} x\leqq 0$ и нулите на полинома

$$\varphi(x)=a_0+a_1x+\ldots+a_nx^n$$

лежат в кръга $|x|\leqq 1$. Докажете, че нулите на полинома

$$a_0 f(x-n)+\ldots+a_\nu f(x-n+2\nu)+\ldots+a_n f(x+n)$$

също лежат в полуравнината $\operatorname{Re} x\leq 0$.

Упътване. Приложете неколкократно резултата от предната задача, като давате последователно стойности на γ, равни на корените на уравнението $\varphi(x)=0$.

50. Нека $f(x)$ е полином от степен n, нулите на който лежат във венеца $K: r\leq|x|\leq R$ и $\alpha\neq 0$ е произволно комплексно число. Докажете, че нулите на полинома

$$f_1(x)=f(\alpha x)+\alpha^n\gamma f\left(\frac{x}{\alpha}\right),\quad |\gamma|=1,$$

лежат в същия венец.

Решение. Ще използуваме теоремата на Грейс. Нека ξ е произволна нула на $f_1(x)$, т. е.

$$f(\alpha\xi)+\alpha^n\gamma f\left(\frac{\xi}{\alpha}\right)=0.$$

За всеки полином $\varphi(x)\in P_n$ да положим

$$L(\varphi)=\varphi(\alpha\xi)+\alpha^n\gamma\varphi\left(\frac{\xi}{\alpha}\right).$$

Така получаваме линеен функционал L, за който $L(f)=0$. Да намерим полинома $G_L(t)$ на Грейс за функционала L. Имаме

$$G_L(t)=L(t-x)^n=(t-\alpha\xi)^n+\alpha^n\gamma\left(t-\frac{\xi}{\alpha}\right)^n.$$

Корените на уравнението $G_L(t)=0$ удовлетворяват условието

$$|t-\alpha\xi|=|\alpha|\left|t-\frac{\xi}{\alpha}\right|,\ \text{т. е. } |t-\alpha\xi|=|\bar{\alpha}t-\xi|.$$

Лесно се вижда, че последното равенство е равносилно с $|t|=|\xi|$. И така корените на уравнението $G_L(t)=0$ лежат върху окръжност с център в началото и радиус $|\xi|$. Ако допуснем, че ξ не лежи във венеца K, ще можем да намерим кръг, който съдържа всички нули на $G_L(t)$ и няма общи точки с K. Последното обаче съгласно теоремата на Грейс ще противоречи на условието, че всички нули на $f(x)$ лежат във венеца K.

Задачата може да се реши директно по следния начин. Нека $x_1, x_2, \ldots, x_n$ са нулите на $f(x)$. За всеки корен $x=z$ на уравнението $f_1(x)=0$ ще имаме

$$\left|\frac{\bar{a}^n f\left(\frac{\xi}{\alpha}\right)}{f(\alpha z)}\right|=1.$$

Последното равенство може да се запише във вида

$$\prod_{k=1}^{n}\left|\frac{z-\bar{\alpha}x_k}{\alpha z-x_k}\right|=1$$

или, като положим $z=x_k\,t_k$, ще имаме

$$(1) \qquad \prod_{k=1}^{n}\left|\frac{t_k-\bar{\alpha}}{\alpha t_k-1}\right|=1.$$

Лесно се вижда, че при $|t_k|>1$ имаме

$$\left|\frac{t_k-\bar{\alpha}}{\alpha t_k-1}\right| \begin{cases} >1, \text{ когато } |\alpha|<1, \text{ и} \\ <1, \text{ когато } |\alpha|>1. \end{cases}$$

Ако $|z|>R$, то $|t_k|>1$ и множителите в (1) са едновременно >1 или <1, т. е. за такива стойности на z равенството (1) не е удовлетворено. Аналогично разсъждаваме в случая $|z|<r$. Ако $|\alpha|=1$, то $\frac{1}{\bar{\alpha}}=\alpha$, $f_1(x)=f(\alpha x)(1+\alpha^n\gamma)$ и тогава твърдението на задачата е очевидно.

51. Нека нулите на полинома $f(x)$ от степен n лежат във венеца $r\leqq|x|\leqq R$ и нулите на полинома

$$\varphi(x)=a_0+a_1x+\ldots+a_nx^m$$

лежат върху единичната окръжност $|x|=1$. Докажете, че при всяко $\alpha\neq 0$ нулите на полинома

$$\psi(x)=a_0f(\alpha^m x)+a_1\alpha^n f(\alpha^{m-2}x)+\ldots+a_\nu\alpha^{n\nu}f(\alpha^{m-2\nu}x)+\ldots+a_m\alpha^{nm}f(\alpha^{-m}x)$$

лежат в същия венец.

Упътване. Приложете неколкократно резултата от предната задача, като на ν давате последователно стойности, равни на корените на уравнението $\varphi(x)=0$.

52. Нека $f(x)$ е полином от степен n, всичките нули на който лежат в полуравнина D с ограничителна права, успоредна на реалната ос. Да положим

$$\varphi(x)=x^2-2r\cos\alpha x+r^2,$$

където $r\geqq 0$ и $|\sin\alpha|\leqq\frac{1}{\sqrt{n}}$. Докажете, че корените на уравнението $\varphi\left(\frac{d}{dx}\right)f(x)=0$, т. е.

$$f''(x)-2r\cos\alpha f'(x)+r^2f(x)=0,$$

лежат също в D.

Решение. Нека ξ е произволен корен на разглежданото уравнение, т. е.

$$f''(\xi)-2r\cos\alpha f'(\xi)+r^2f(\xi)=0.$$

Да положим

$$L(\varphi)=\varphi''(\xi)-2r\cos\alpha\,\varphi'(\xi)+r^2\varphi(\xi),\quad \varphi(x)\in P_n.$$

Имаме $L(f)=0$ и за съответния полином на Грейс получаваме

$$G_L(t)=L(t-x)^n=n(n-1)(t-\xi)^{n-2}+2r\cos\alpha\, n(t-\xi)^{n-1}+r^2(t-\xi)^n.$$

Освен $(n-2)$-кратния корен $t=\xi$ уравнението $G_L(t)=0$ има корени $t_1=x_1+\xi$ и $t_2=x_2+\xi$, където x_1, x_2 удовлетворяват квадратното уравнение

$$r^2x^2+2rn\cos\alpha\, x+n(n-1)=0.$$

За дискриминантата на последното уравнение имаме

$$\Delta=r^2n^2\cos^2\alpha-n(n-1)r^2$$

и очевидно условието $|\sin|\leq\frac{1}{\sqrt{n}}$ е равносилно с $\Delta\geq 0$. Следователно числата x_1 и x_2 са реални. Ако допуснем, че $\xi\notin D$, ще можем да намерим полуравнина, съдържаща точките ξ, $\xi+x_1$ и $\xi+x_2$, като при това тази полуравнина няма общи точки с D. Съгласно теоремата на Грейс тя трябва да съдържа поне една нула на $f(x)$, което обаче противоречи на условието, че всички нули на $f(x)$ лежат в D.

53. Нека $f(x)$ е полином от степен n, всичките нули на който са реални. Докажете, че при $r\geq 0$ и $|\sin\alpha|\leq\frac{1}{\sqrt{n}}$ уравнението

$$f''(x)-2r\cos\alpha f'(x)+r^2f(x)=0$$

има само реални корени.

Упътване. Приложете двукратно предната задача, когато D съвпада с долната или с горната полуравнина, ограничена от реалната ос.

54. Теорема на Обрешков (прецизиране на теоремата на Пулен—Ермит от зад. 26). Нека $f(x)$ е полином от степен n, който има само реални нули, и $\varphi(x)$ е полином с реални коефициенти, нулите на който лежат в ъгловото пространство

$$|\arg(x)|\leq\arc\sin\frac{1}{\sqrt{n}}.$$

Тогава полиномът $\varphi\left(\frac{d}{dx}\right)f(x)$ има само реални нули.

Доказателство. Нека $\varphi(x)=\varphi_1(x)\varphi_2(x)$. Лесно се вижда, че $\varphi\left(\frac{d}{dx}\right)f(x)=\varphi_2\left(\frac{d}{dx}\right)f_1(x)$ където $f_1(x)=\varphi_1\left(\frac{d}{dx}\right)f(x)$. Следователно, ако теоремата е в сила за полиномите $\varphi_1(x)$ и $\varphi_2(x)$, тя ще бъде в сила и за полинома $\varphi(x)$. Понеже всеки полином с реални коефициенти се разлага в произведение на реални полиноми от първа и втора степен, ясно е, че общият случай на теоремата се свежда към разгледаните в зад. 26 и 53 частни случаи.

От метода на доказателство следва, че ако нулите на $f(x)$ лежат в полуравнината D с ограничителна права, успоредна на реалната ос, при същите предположения за $\varphi(x)$ нулите на полинома $\varphi\left(\frac{d}{dx}\right)f(x)$ ще лежат пак в D.

Определение. Нека D_1 и D_2 са две кръгови области; множеството от точки

$$z=\frac{\alpha_1 z_1+\alpha_2 z_2}{\alpha_1+\alpha_2},$$

където α_1 и α_2 са фиксирани положителни числа и точките z_1, z_2 независимо една от друга пробягват съответно кръговите области D_1 и D_2, ще наричаме *средна област* на D_1 и D_2 и ще означаваме с

$$D=\frac{\alpha_1 D_1+\alpha_2 D_2}{\alpha_1+\alpha_2}.$$

55. Докажете, че средната област

$$D=\frac{\alpha_1 D_1+\alpha_2 D_2}{\alpha_1+\alpha_2}$$

на кръговите области D_1 и D_2 е кръгова. Покажете при това, че:

а) когато D_1 и D_2 са два кръга с центрове съответно в c_1 и c_2 и радиуси r_1 и r_2, средната област D е кръг с център $c=\frac{\alpha_1 c_1+\alpha_2 c_2}{\alpha_1+\alpha_2}$ и радиус $r=\frac{\alpha_1 r_1+\alpha_2 r_2}{\alpha_1+\alpha_2}$;

б) когато D_1 и D_2 са две полуравнини с успоредни ограничителни прави l_1 и l_2, средната област $D=\frac{\alpha_1 D_1+\alpha_2 D_2}{\alpha_1+\alpha_2}$ е също полуравнина с ограничителна права l, успоредна на l_1 и l_2, като l дели разстоянието между l_1 и l_2 в отношение $\alpha_2:\alpha_1$.

56. Нека $f(x)=f_1(x)f_2(x)$, където $f_1(x)$ е полином от степен n_1 и $f_2(x)$ е полином от степен n_2. Нека освен това нулите на $f_1(x)$ да лежат в кръговата област D_1, а нулите на $f_2(x)$ — в кръговата област D_2. Докажете, че нулите на производната $f'(x)$ лежат или в D_1, или в D_2, или в средната област

$$D=\frac{n_2 D_1+n_1 D_2}{n_1+n_2}.$$

Решение. Ще приложим теоремата на Лагер. Нека ξ е нула на $f'(x)$, т. е.

$$f'_1(\xi)f_2(\xi)+f_1(\xi)f'_2(\xi)=0.$$

Да допуснем, че $\xi\notin D_1$, $\xi\notin D_2$ и $\xi\notin D=\frac{n_2 D_1+n_1 D_2}{n_2+n_1}$. За съответната точка ξ' от теоремета на Лагер, приложена на полинома $f_1(x)$, имаме

$$\xi'=\xi-\frac{n_1 f_1(\xi)}{f'_1(\xi)}.$$

Ясно е, че $\xi'\in D_1$, защото в противен случай съгласно теоремата на Лагер (като отделим $\xi\notin D_1$ и $\xi'\notin D_1$ от D_1 с подходяща окръжност без общи точки с D_1)

полиномът $f_1(x)$ би трябвало да има поне една нула навън D_1. Аналогично за точката

$$\xi''=\xi-\frac{n_2f_2(\xi)}{f'_2(\xi)},$$

имаме $\xi''\in D_2$. Получаваме $n_2\xi'+n_1\xi''=(n_2+n_1)\xi$, т. е.

$$\xi=\frac{n_2\xi'+n_1\xi''}{n_2+n_1}.$$

От $\xi'\in D_1$ и $\xi''\in D_2$ получаваме $\xi\in\frac{n_2D_1+n_1D_2}{n_2+n_1}$ в противоречие с допускането, че $\xi\notin D$.

57. Нека $f(x)$ е полином от степен n и a е k-кратна нула на $f(x)$. Нека нулите на $f(x)$, които са различни от a, да лежат извън кръга $|x-a|<r$. Да се докаже, че нулите на $f'(x)$, които са различни от a, лежат ихвън кръга $|x-a|<\frac{k}{n}r$.

Упътване. Използувайте предната задача.

58. В допълнение на теоремата на Гаус — Люка, която третира въпроса за разположението на нулите на производната на даден полином в изпъкнала област, докажете следното твърдение:

Нека $f(x)$ е полином от степен x, чиито нули лежат в кръговата област $|x-a|\geq r$ (a — дадено комплексно число, $r>0$); тогава нулите на $f'(x)$ ще лежат в областта

$$|x-a|\geq\frac{r^2}{n}\left|\frac{f'(a)}{f(a)}\right|.$$

Решение. Нека ξ е нула на $f'(x)$. Без ограничение на общността можем да положим, че $f(\xi)\neq0$. Тогава ξ ще бъде корен на уравнението

$$\sum_{k=1}^{n}\frac{1}{x-a_k}=0,$$

където $a_1, a_2, \ldots, a_n$ са нулите на $f(x)$. За удобство да положим $r=1$ и $a=0$ Като запишем горното уравнение във вида

$$\frac{1}{x}=\sum_{k=1}^{n}\frac{p_k}{x-a_k},$$

където

$$p_k=\frac{1}{a_k}\left(\sum_{k=1}^{n}\frac{1}{a_k}\right)^{-1},\qquad \sum_{k=1}^{n}p_k=1,$$

получаваме възможност да приложим резултата от зад. 7. И така корените на разглежданото уравнение ще лежат в областта

$$|x|\geq\frac{1}{\sum\limits_{k=1}^{n}|p_k|}=\frac{\left|\sum\limits_{k=1}^{n}a_k^{-1}\right|}{\sum\limits_{k=1}^{n}|p_k|\cdot\sum\limits_{k=1}^{n}|a_k^{-1}|}\geq\frac{1}{n}\left|\sum_{k=1}^{n}a_k^{-1}\right|=\frac{1}{n}\left|\frac{f'(0)}{f(0)}\right|$$

т. е.

$$|x|\geq\frac{1}{n}\left|\frac{f'(0)}{f(0)}\right|.$$

Да разгледаме два примера.

а) Нека $f(x)=x^n$ и $r=|a|$; тогава разглежданата област добива вида $|x-a|\geq|a|$ и очевидно оценката е точна.

б) Нека $f(x)=(x-\alpha)^p(x-\beta)^q$, където α и β са произволни комплексни числа, и да положим $a=\frac{1}{2}(\alpha+\beta)$ и $r=\frac{1}{2}|\alpha-\beta|$. Тогава за разглежданата област получаваме

(1) $|x-a|\geq\frac{1}{2n}|p-q|\,|\beta-\alpha|$, $n=p+q$, и за корените на уравнението $f'(x)=0$, които са различни от нулите на $f(x)$, имаме $x=\frac{q\alpha+p\beta}{n}$. За това x в (1) се достига равенство.

В следващите няколко задачи се съдържа доказателство на теоремата на Хурвиц. За краткост един полином ще наричаме *хурвицов*, когато всичките му нули имат отрицателни реални части.

59. Нека

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n.$$

Да положим

$$f^*(x)=\bar{a}_0-\bar{a}_1x+\bar{a}_2x^2-\ldots+(-1)^n\bar{a}_nx^n.$$

Проверете равенствата

$$[f^*(x)]^*=f(x),\ [\alpha f(x)]^*=\bar{\alpha}f^*(x),\ (f+g)^*=f^*+g^*,\ (fg)^*=f^*g^*.$$

60. При означенията от предната задача покажете, че ако x_1, x_2, ..., x_n са нулите на полинома $f(x)$, то нулите на полинома $f^*(x)$ са $-\bar{x}_1, -\bar{x}_2, \ldots, -\bar{x}_n$.

61. Нека полиномът $f(x)$ е хурвицов. Докажете, че

$$\begin{aligned}
0\leq|f(x)|&<|f^*(x)| &&\text{при } \operatorname{Re}x<0,\\
0\leq|f(x)|&>|f^*(x)| &&\text{при } \operatorname{Re}x>0,\\
0<|f(x)|&=|f^*(x)| &&\text{при } \operatorname{Re}x=0.
\end{aligned}$$

Решение. Нека x_j са нулите на полинома $f(x)$. Имаме

$$f(x)=a_n\prod_{j=1}^{n}(x-x_j),\quad f^*(x)=(-1)^n\overline{a}_n\prod_{j=1}^{n}(x+x_j).$$

Да положим $x=u+vi$, $x_j=u_j+iv_j$. Тогава от равенството

$$|x+x_j|^2-|x-x_j|^2=4uu_j$$

следва, че при $u\gtreqless 0$, $|x-x_j|\gtreqless|x+x_j|$, откъдето се получават желаните равенства.

62. Нека α и β са произволни числа, за които $|\alpha|>|\beta|$. Покажете, че полиномът $f(x)$ е хурвицов тогава и само тогава, когато полиномът

$$g(x)=\alpha f(x)-\beta f^*(x)$$

е хурвицов.

Решение. От предната задача и от неравенството $|\alpha|>|\beta|$ следва, че ако $f(x)$ е хурвицов, то и $g(x)$ е хурвицов. Имаме

$$g^*(x)=\overline{\alpha}f^*(x)-\overline{\beta}f(x),$$

откъдето

$$f(x)=\alpha_1 g(x)-\beta_1 g^*(x)$$

с

$$\alpha_1=\frac{\overline{\alpha}}{|\alpha|^2-|\beta|^2},\quad \beta_1=-\frac{\beta}{|\alpha|^2-|\beta|^2}.$$

Очевидно $|\alpha_1|>|\beta_1|$, следователно $f(x)$ е хурвицов.

63. Нека ξ е комплексно число с отрицателна реална част. Докажете, че полиномът $f(x)$ от степен $n>1$ е хурвицов тогава и само тогава, когато

$$|f(\xi)|<|f^*(\xi)|$$

и полиномът

$$f_1(x)=\frac{f^*(\xi)f(x)-f(\xi)f^*(x)}{x-\xi}$$

от степен $n-1$ е хурвицов.

Решение. Ако $f(x)$ е хурвицов, от $\operatorname{Re}\xi<0$ и зад. 61 следва

$$|f(\xi)|<|f^*(\xi)|$$

и съгласно предната задача полиномът

$$g(x)=f^*(\xi)f(x)-f(\xi)f^*(x)$$

е хурвицов, откъдето и полиномът $f_1(x)=\dfrac{g(x)}{x-\xi}$ е хурвицов.

Обратното се доказва по подобен начин.

64. Нека ξ е комплексно число с отрицателна реална част и $f(x)=\sum_{\nu=0}^{n} a_\nu x^\nu$ е полином от степен $n>1$. Да положим

$$F(x,\xi)=\frac{f^*(\xi)f(x)-f(\xi)f^*(x)}{x-\xi}=$$

$$=F_0(x)+F_1(x)\xi+F_2(x)\xi^2+\ldots+F_{n-1}(x)\xi^{n-1}.$$

Докажете, че полиномът $f(x)$ е хурвицов тогава и само тогава, когато

$$a_0 \neq 0, \quad \operatorname{Re}\frac{a_1}{a_0}>0$$

и полиномът

$$F_0(x)+\xi F_1(x)=H(x)$$

от степен $n-1$ е хурвицов.

Решение. Непосредствено се проверяват следните равенства:

(1) $$\bar{a}_0 f(x)-a_0 f^*(x)=x\,F_0(x),$$

$$-\bar{a}_1 f(x)-a_1 f^*(x)=-F_0(x)+xF_1(x),$$

(2) $$x^2(F_0(x)+\xi F_1(x))=f(x)\varphi(x)-f^*(x)\psi(x),$$

където

$$\varphi(x)=\bar{a}_0 x-\bar{a}_1\xi x+\bar{a}_0\xi, \quad \psi(x)=a_0x+a_1\xi x+a_0\xi.$$

Нека сега $f(x)$ е хурвицов полином. Тогава $a_0 \neq 0$, защото $f(x)$ не може да има нулата за корен. По-нататък, понеже всички корени на $f(x)$ имат отрицателни реални части, реципрочните им стойности също ще имат отрицателни реални части. Но сборът на тези реципрочни стойности е $-\frac{a_1}{a_0}$, следователно $\operatorname{Re}\frac{a_1}{a_0}>$ >0.

За да покажем, че $H(x)$ е хурвицов, ще докажем, че ако $\operatorname{Re}\alpha \geq 0$, то $H(\alpha) \neq 0$.

Действително, ако числото σ е такова, че $\operatorname{Re}\sigma<0$, то, както следва от предната задача, полиномът $f_1(x)=F(x,\sigma)$ ще бъде хурвицов и следователно $F(\alpha,\sigma)\neq$ $\neq 0$. Да положим $\sigma=-\frac{1}{\tau}$, откъдето следва $\operatorname{Re}\tau<0$. Получаваме

(3) $$\tau^{n-1}F\left(\alpha,-\frac{1}{\tau}\right)=\Phi(\alpha,\tau)=F_0(\alpha)\tau^{n-1}+F_1(\alpha)\tau^{n-2}+\ldots+F_{n-1}(\alpha)\neq 0.$$

Ще разгледаме отделно случаите $F_0(\alpha)\neq 0$ и $F_0(\alpha)=0$. Ако $F_0(\alpha)\neq 0$, $\Phi(\alpha,x$ ще бъде полином от степен $n-1$, всичките корени на който имат неотрицателни реални части, както това следва от (3). Тогава и сумата на тези корени която съгласно формулите на Виет е равна на $-\frac{F_1(\alpha)}{F_0(\alpha)}$, ще притежава това свойство, т. е.

$$\operatorname{Re}\left(-\frac{F_1(\alpha)}{F_0(\alpha)}\right)\geq 0.$$

Ако α беше корен на $H(x)$, т. е. ако

$$H(\alpha)=F_0(\alpha)+\xi F_1(\alpha)=0,$$

ще получим

$$-\frac{F_1(\alpha)}{F_0(\alpha)}=\frac{1}{\xi},$$

което е невъзможно, защото

$$\operatorname{Re}\frac{1}{\xi}<0.$$

Нека сега $F_0(\alpha)=0$. Тогава от $H(\alpha)=0$ ще последва $F_1(\alpha)=0$ и при $x=\alpha$ равенствата (1) ще приемат вида

$$\bar{a}_0 f(\alpha)-a_0 f^*(\alpha)=0, \quad \bar{a}_1 f(\alpha)+a_1 f^*(\alpha)=0,$$

откъдето

$$(\bar{a}_0 a_1+a_0\bar{a}_1)\,f(\alpha)=0.$$

Но $\operatorname{Re}\alpha\geqq 0$, следователно $f(\alpha)\neq 0$ и получаваме $\bar{a}_0 a_1+\bar{a}_1 a_0=0$, т. е.

$$\frac{a_0}{a_1}=-\frac{\bar{a}_0}{\bar{a}_1}=-\left(\frac{\bar{a}_1}{\bar{a}_0}\right),$$

откъдето следва

$$\operatorname{Re}\frac{a_1}{a_0}=0,$$

което противоречи на доказаното вече неравенство $\operatorname{Re}\dfrac{a_1}{a_0}>0$.

Сега, обратно, нека полиномът $H(x)$ е хурвицов и нека $a_0\neq 0$, $\operatorname{Re}\dfrac{a_1}{a_0}>0$; ще покажем, че и полиномът $f(x)$ е хурвицов. Равенството (2) можем да запишем във вида

(4) $$x^2 H(x)=f(x)\,\varphi(x)-f^*(x)\,\psi(x).$$

Тъй като $(x^2)^*=x^2$, оттук следва

$$(x^2 H(x))^*=f^*(x)\,\varphi^*(x)-f(x)\,\psi^*(x).$$

От последните две равенства получаваме

(5) $$[\varphi^*(x)\,\varphi(x)-\psi^*(x)\,\psi(x)]\,f(x)=x^2\,[H(x)\,\varphi^*(x)+H^*(x)\,\psi(x)].$$

Нека сега α е такова, че $\operatorname{Re}\alpha\geqq 0$. Тъй като $H(x)$ е хурвицов, от зад. 61 следва, че

(6) $$|H(\alpha)|>|H^*(\alpha)| \text{ или } |H(\alpha)|=|H^*(\alpha)|>0.$$

Да допуснем, че α е корен на $f(x)$. Тъй като $\alpha\neq 0$, като вземем пред вид че $a_0\neq 0$ от (5) получаваме

$$H(\alpha)\,\varphi^*(\alpha)+H^*(\alpha)\,\psi(\alpha)=0.$$

Това равенство ще противоречи на (6), стига да покажем, че

(7) $$|\varphi^*(\alpha)|>|\psi(\alpha)|.$$

При $\operatorname{Re}b<0$ полиномът $u(x)=x-b$ е хурвицов, откъдето според зад. 61 при $\operatorname{Re}x<0$ ще имаме $|u^*(x)|>|u(x)|$, т. е.

$$|-x-\bar{b}|>|x-b|.$$

Ако положим $b=\frac{1}{\xi}$, $x=-\frac{a_1}{a_0}-\frac{1}{\alpha}$, условията $\operatorname{Re} b<0$ и $\operatorname{Re} x<0$ ще бъдат изпълнени, т. е.

$$\left|\frac{a_1}{a_0}+\frac{1}{\alpha}-\frac{1}{\overline{\xi}}\right|>\left|\frac{a_1}{a_0}+\frac{1}{\alpha}+\frac{1}{\xi}\right|.$$

Умножавайки лявата част с $|a_0\alpha\overline{\xi}|$, дясната с $|a_0\alpha\xi|$ и взимайки пред вид, че $|\overline{\xi}|=|\xi|$, получаваме неравенството

(8) $$|a_1\alpha\overline{\xi}+a_0\overline{\xi}-\alpha a_1|>|a_1\alpha\xi+a_0\alpha|.$$

Обаче

$$\varphi^*(x)=-a_0x+a_1\overline{\xi}x+a_0\overline{\xi},$$

откъдето лявата част на (8) е равна на $|\varphi^*(\alpha)|$, а дясната — на $|\varphi(\alpha)|$. С това неравенството (7) е доказано.

Накрая ще отбележим, че полиномът $H(x)$ действително е от степен $n-1$. Наистина очевидно е, че степента му не надминава $n-1$. Ако тя е строго по-малка, коефициентът пред x^{n+1} в дясната част на (4) трябва да бъде нула, т. е.

$$a_n(\overline{a}_0-\overline{a}_1\xi)-(-1)^n\overline{a}_n(a_0+a_1\xi)=0$$

или

$$\left|\frac{1}{\xi}-\frac{\overline{a}_1}{\overline{a}_0}\right|=\left|\frac{1}{\xi}+\frac{a_1}{a_0}\right|.$$

Но при $\operatorname{Re} c>0$ полиномът $v(x)=x+c$ е хурвицов, следователно при $\operatorname{Re} x<0$ имаме

$$|x+c|<|-x+\overline{c}|=|x-\overline{c}|.$$

В частност при $c=\frac{a_1}{a_0}$, $x=\frac{1}{\xi}$ получаваме

$$\left|\frac{1}{\xi}+\frac{a_1}{a_0}\right|<\left|\frac{1}{\xi}-\frac{\overline{a}_1}{\overline{a}_0}\right|,$$

което противоречи на по-горното равенство.

65. Теорема на Хурвиц. Полиномът

$$f(x)=a_0+a_1x+\ldots+a_nx^n,\quad a_n\neq 0,$$

с реални коефициенти и $a_0>0$ е хурвицов тогава и само тогава, когато детерминантите

$$D_1=a_1,\ D_2=\begin{vmatrix} a_1 & a_0\\ a_3 & a_2\end{vmatrix},\quad D_3=\begin{vmatrix} a_1 & a_0 & 0\\ a_3 & a_2 & a_1\\ a_5 & a_4 & a_3\end{vmatrix},$$

$$D_4=\begin{vmatrix} a_1 & a_0 & 0 & 0\\ a_3 & a_2 & a_1 & a_0\\ a_5 & a_4 & a_3 & a_2\\ a_7 & a_6 & a_5 & a_3\end{vmatrix},\ldots,D_n=\begin{vmatrix} a_1 & a_0 & 0 & \ldots & 0\\ a_3 & a_2 & a_1 & \ldots & 0\\ \\ a_{2n-1} & a_{2n-2} & a_{2n-3} & \ldots & a_n\end{vmatrix}$$

са положителни (тук при $j>n$ под a_j разбираме 0).

Доказателство. Нека

$$g(x)=a_0+a_2x^2+a_4x^4+\dots,$$
$$h(x)=a_1x+a_3x^3+a_5x^5+\dots$$

Тогава $f(x)=g(x)+h(x)$ и очевидно $f^*(x)=g(x)-h(x)$. Като заместим тези равенства (4) от предната задача и вземем пред вид дефинициите на $\varphi(x)$ и $\psi(x)$, получаваме

$$x^2H(x)=2(a_0x+a_0\xi)h(x)-2a_1\xi\,xg(x)$$

или

$$K(x)=a_0a_1-\xi(a_1a_2-a_0a_3)x+a_0a_3x^2-\xi(a_1a_4-a_0a_5)x^3+a_0a_5x^4-\dots,$$

където с $K(x)$ сме означили полинома $\frac{1}{2}H(x)$. Въз основа на предната задача, като вземем пред вид, че по предложение $a_0>0$, можем да твърдим, че при $\operatorname{Re}\xi<0$ полиномът $f(x)$ е хурвицов тогава и само тогава, когато $a_1>0$ и полиномът $H(x)$ е хурвицов. Да вземем $\xi=-1$. Тогава $K(x)$ добива вида

$$K(x)=a_0a_1+(a_1a_2-a_0a_3)x+a_0a_3x^2+(a_1a_4-a_0a_5)x^3+\dots$$

и тъй като неговата степен е $n-1$, той е хурвицов тогава и само тогава, когато детерминантите

$$\Delta_1=a_1a_2-a_0a_3,\quad \Delta_2=\begin{vmatrix} a_1a_2-a_0a_3 & a_0a_1\\ a_1a_4-a_0a_5 & a_0a_3\end{vmatrix},\dots$$

$$\Delta_{n-1}=\begin{vmatrix} a_1a_2-a_0a_3 & a_0a_1 & 0 & \dots & 0\\ a_1a_4-a_0a_5 & a_0a_3 & a_1a_2-a_0a_3 & \dots & 0\\ \dots & \dots & \dots & \dots & \dots\\ \dots & \dots & \dots & \dots & \dots\end{vmatrix}$$

са положителни. По такъв начин $f(x)$ е хурвицов тогава и само тогава, когато са положителни всички числа $D_1=a_1, \Delta_1, \Delta_2, \dots, \Delta_{n-1}$. Но, както се вижда непосредствено, имаме равенствата

$$a_0a_1\Delta_j=a_0(a_0a_1)^{\frac{j}{2}}D_{j+1} \quad \text{или} \quad a_0a_1\Delta_j=(a_0a_1)^{\frac{j+1}{2}}D_{j+1}$$

в зависимост от това, дали j е четно или нечетно, следователно, като вземем пред вид, че $a_0>0$, $a_1>0$, получаваме, че Δ_j и D_{j+1} имат еднакви знаци при $j=1, 2, \dots, n-1$.

С това доказателството е завършено.

66. Намерете необходими и достатъчни условия реалният полином

$$x^3+ax^2+bx+c$$

да е хурвицов.

Отг. $a>0$, $c>0$, $ab-c>0$.

67. Намерете необходими и достатъчни условия реалният полином

$$x^4+ax^3+bx^2+cx+d$$

да е хурвицов.

Отг. $a>0$, $c>0$, $d>0$, $abc-c^2-a^2d>0$.

68. Намерете необходими и достатъчни условия всички нули на реалния полином

$$x^3+ax^2+bx+c$$
да лежат в единичния кръг $|x|<1$.

Упътване. Чрез трансформацията
$$x=\frac{1+y}{1-y}$$
въпросът се свежда до зад. 66.

Отг. $1-a+b-c>0$, $1+a+b+c>0$, $3-a-b+3c>0$

69. Докажете, че коефициентите на всеки реален хурвицов полином
$$f(x)=x^n+a_1x^{n-1}+\ldots+a_n$$
са положителни

Упътване. Докажете най-напред твърдението за полиноми от първа и втора степен и използувайте това, че произведение на полиноми с положителни коефициенти е също полином с положителни коефициенти.

70. Докажете, че ако полиномът $f(x)$ от степен n е хурвицов и γ е произволно отрицателно число, полиномът
$$f_1(x)=-\gamma f(x)+xf'(x)$$
е също хурвицов.

Решение. Ще използуваме теоремата на Лагер. Нека ξ е произволна нула на $f_1(x)$, т. е. $\gamma f(\xi)=\xi f'(\xi)$. За съответната точка
$$\xi'=\xi-\frac{nf(\xi)}{f'(\xi)},$$
имаме $\xi'=\left(1-\frac{n}{\gamma}\right)\xi$. Да допусием, че ξ не лежи в лявата полуравнина $\operatorname{Re} x<0$, т. е. $\operatorname{Re}\xi\geq 0$. Тогава за ξ' също ще имаме $\operatorname{Re}\xi'\geq 0$. През ξ и ξ' можем да прекараме окръжност K, която лежи извън полуравнина $\operatorname{Re} x<0$. По теоремата на Лагер полиномът $f(x)$ трябва да има нула вътре в K или върху K. Това обаче противоречи на условието, че всички нули на $f(x)$ лежат в лявата полуравнина.

71. Докажете, че ако полиномът $F(x)$ има само реални и отрицателни нули и
$$f(x)=a_0+a_1x+\ldots+a_nx^n$$
е хурвицов полином, полиномът
$$\varphi(x)=a_0F(0)+a_1F(1)x+\ldots+a_nF(n)x^n$$
е също хурвицов.

Упътване. Приложете неколкократно резултата от предната задача, като на γ давате последователно стойности, равни на нулите на $F(x)$.

72. Обобщете резултата от предната задача, като условието $F(x)$ да има само реални и отрицателни нули замените с условието реалните нули на реалния полином $F(x)$, които са от нечетна кратност, да са отрицателни, а останалите — да лежат в множеството, ограничено от левия клон на хиперболата

$$\left(x-\frac{n}{2}\right)^2-(n-1)y^2=\frac{1}{4}n(n-1).$$

Упътване. Като се вземе пред вид зад. 70, достатъчно е да се установи твърдението за случая, когато $F(x)$ е полином от втора степен. За целта използувайте метода на решение на зад. 52.

73. Покажете, че твърденията от предните три задачи остават в сила, ако навсякъде „хурвицов полином" се замени с условието съответният полином да има само реални нули.

Следващите задачи са посветени на един числен метод за определяне броя на нулите на даден полином вляво и вдясно от имагинерната ос.

74. Нека $f(x)$ е полином от степен n със старши коефициент $a_0=1$ и $f(0)\neq 0$. Ако $x_1, x_2,\ldots,x_n$ са нулите на $f(x)$, да се намери полином $f_1(x)$ с нули $\frac{1}{2}\left(x_i+\frac{1}{x_i}\right)$, $i=1, 2,\ldots, n$.

Решение. Полагаме $y=\frac{1}{2}\left(x+\frac{1}{x}\right)$, т.е. $x^2-2yx+1$, откъдето $x=y\pm\sqrt{y^2-1}$. Ще покажем, че

$$f_1(y)=\frac{f(y+\sqrt{y^2-1})\,f(y-\sqrt{y^2-1})}{2^n f(0)}$$

е полином от n-та степен, който удовлетворява условието на задачата и има старши коефициент 1. Наистина, като вземем пред вид тъждеството

$$(y+\sqrt{y^2-1}-x_\nu)\,(y-\sqrt{y^2-1}-x_\nu)=-2x_\nu\left[y-\frac{1}{2}\left(x_\nu+\frac{1}{x_\nu}\right)\right],$$

получаваме

$$\begin{aligned}f(y+\sqrt{y^2-1})\,f(y-\sqrt{y^2-1})&=\\&=\prod_{\nu=1}^{n}(y+\sqrt{y^2-1}-x_\nu)\,(y-\sqrt{y^2-1}-x_\nu)=\\&=(-2)^n\left(\prod_{\nu=1}^{n}x_\nu\right)\prod_{\nu=1}^{n}\left[y-\frac{1}{2}\left(x_\nu+\frac{1}{x_\nu}\right)\right]=\\&=2^n f(0)\prod_{\nu=1}^{n}\left[y-\frac{1}{2}\left(x_\nu+\frac{1}{x_\nu}\right)\right],\end{aligned}$$

откъдето лесно следва твърдението на задачата.

75. Като разделим полинома $f(x)$ на $x^2-2yx+1$, ще получим остатък от вида

$$\psi(y)x+\varphi(y),$$

където $\varphi(y)$ и $\psi(y)$ са полиноми на y. Покажете, че

$$f_1(x)=\frac{1}{2^n f(0)}\left[(\varphi(x)+x\psi(x))^2-(x^2-1)\psi^2(x)\right].$$

76. В означенията на предните две задачи да предположим, че полиномът $f(x)$ не се анулира върху имагинерната ос, и да разгледаме редицата от полиноми

$$f_0(x)=f(x),\ f_1(x),\ f_2(x),\ldots,f_k(x),\ldots,$$

където $f_k(x)$ се получава по същия начин, както $f_1(x)$ от $f(x)$. Докажете, че така построената редица от полиноми е сходяща и клони към полинома

$$(x-1)^p\ (x+1)^q,$$

където q е броят на нулите на $f(x)$ в лявата полуравнина и p е броят на нулите на $f(x)$ в дясната полуравнина $\mathrm{Re}\,x>0$.

Твърдението на тази задача ни дава един числен метод (метод на Загускин) за намиране на p и q, тъй като при достатъчно голямо k разликата $p-q$ ще бъде приблизително равна на сбора от нулите на $f(x)$ (който лесно се определя от първата формула на Виет). От $p-q=s$ и $p+q=n$ получаваме

$$p=\frac{1}{2}(n+s),\qquad q=\frac{1}{2}(n-s).$$

Решение. Достатъчно е да отбележим, че редицата a_n, дефинирана чрез рекурентната връзка

$$a_{n+1}=\frac{1}{2}\left(a_n+\frac{1}{a_n}\right),\ n=0,\ 1,\ 2,\ldots$$

при $\mathrm{Re}\,a_0\pm 0$ е сходяща и клони към $+1$ при $\mathrm{Re}\,a_0>0$ и към -1 при $\mathrm{Re}\,a_0<0$. Наистина, като решим рекурентните уравнения спрямо a_k, лесно получаваме по индукция, че

$$a_k=\frac{(a_0+1)^{2^k}+(a_0-1)^{2^k}}{(a_0+1)^{2^k}-(a_0-1)^{2^k}},$$

т. е.

$$a_k=\left[\left(\frac{a_0+1}{a_0-1}\right)^{2^k}+1\right]:\left[\left(\frac{a_0+1}{a_0-1}\right)^{2^k}-1\right]$$

и остава да отбележим, че при $\mathrm{Re}\,a_0<0$ имаме $\left|\frac{a_0+1}{a_0-1}\right|<1$ и следователно $\lim\limits_{k\to\infty}a_k=-1$, а при $\mathrm{Re}\,a_0>0$ — аналогично $\lim\limits_{k\to\infty}a_k=1$. (Итерационната редица a_k не е нищо друго освен редицата от приближения, получени по известния метод на Нютон за пресмятане на квадратен корен от 1.)

Да илюстрираме изложения метод с един прост **пример**. Нека $f(x)=x^3-1$. Разделяме $f(x)$ на $x^2-2yx+1$:

$$\begin{array}{l|l} x^3-1 & x^2-2yx+1 \\ \hline & x+2y \end{array}$$

$$-\frac{x^3-2yx^2+x}{2yx^2-x-1}$$

$$-\frac{2yx^2-4y^2x+2y}{(4y^2-1)x-2y-1}$$

и получаваме

$$\varphi(y)=-2y-1,\ \psi(y)=4y^2-1.$$

За трансформираното уравнение

$$[\varphi(y)+y\psi(y)]^2-(y^2-1)\psi^2(y)=0$$

получаваме

$$4y^3-3y-1=0.$$

И така

$$f_1(x)=x^3-\frac{3}{4}x-\frac{1}{4}.$$

Аналогично намираме

$$f_2(x)=x^3+\frac{3}{2}x^2-\frac{15}{16}x-\frac{25}{16},\ f_3(x)=x^3+\frac{21}{20}x^2-\frac{41}{20}x-\frac{1681}{1600}.$$

От приближеното равенство $p-q=s\approx-\frac{21}{20}$ намираме $s=-1$, откъдето

$$p=\frac{1}{2}(n+s)=+1, q=\frac{1}{2}(n-s)=2.$$

И така даденият полином (както в разглеждания прост пример се проверява и непосредствено) има две нули вляво от имагинерната ос и една нула вдясно от нея.

§ 6. РАЗПРЕДЕЛЕНИЕ НА РЕАЛНИТЕ КОРЕНИ НА АЛГЕБРИЧНИТЕ УРАВНЕНИЯ

Горни граници за положителните корени на уравненията

Метод на Лагранж. Нека

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

е полином с реални коефициенти. Да означим с M най-голямата от абсолютните стойности на отрицателните коефициенти на $f(x)$

и с k — разликата между n и степента на първия член в $f(x)$ с отрицателен коефициент. Числото

$$L=1+\sqrt[k]{M}$$

е горна граница за положителните корени на уравнението $f(x)=0$.

Пример. За уравнението

$$x^5-10x^4+15x^3+4x^2-16x+390=0$$

имаме $M=16$, $k=1$, $L=1+16=17$. И така положителните корени на даденото уравнение лежат в интервала $(0,17)$.

Метод на Нютон. Нека $f(x)$ е полином от n-та степен с реални коефициенти и с положителен старши коефициент. Ако за числото L имаме

$$f(L)>0,\ f'(L)>0,\ f''(L)>0, \ldots,\ f^{(n)}(L)>0,$$

то L е горна граница за положителните корени на уравнението $f(x)=0$.

Пример. Да приложим метода на Нютон за намиране горна граница на корените на разгледаното по-горе уравнение. За производните на полинома $f(x)=x^5-10x^4+15x^3+4x^2-16x+390$ имаме

$$\frac{f'(x)}{1!}=5x^4-40x^3+45x^2+8x-16,$$

$$\frac{f''(x)}{2!}=10x^3-60x^2+45x+4,$$

$$\frac{1}{3!}f'''(x)=10x^2-40x+15,$$

$$\frac{1}{4!}f^{IV}(x)=5x-10,$$

$$\frac{1}{5!}f^{V}(x)=1.$$

Удобно е да търсим числото L, започвайки от $(n-1)$-вата производна (в случая от четвъртата производна). При $x=2$ имаме $f^{IV}(2)=0$; понеже $f'''(2)<0$, увеличаваме числото, докато получим положителна стойност за $f'''(x)$, и така достигаме до $f'''(4)>0$; при $x=4$ имаме $f''(4)<0$, но $f''(6)>0$, по-нататък получаваме $f'(6)<0$, но $f'(7)>0$ и окончателно, понеже $f(7)<0$, но $f(8)>0$, и така достигаме до горната граница $L=8$.

Този начин за намиране на L, започвайки от производната от най-висок ред, може лесно да се обоснове, като се използува фактът, че ако производната на дадена функция е положителна в някакъв интервал, функцията е растяща в същия интервал.

Забележка. Въпросът за намиране на долна граница за отрицателните корени на уравнението $f(x)=0$ се свежда към въпроса за намиране на горна граница на корените на уравнението $f(-x)=0$. По-точно, ако L е горна граница за корените на уравнението $f(-x)=0$, то $-L$ е долна граница за корените на уравнението $f(x)=0$. Също така ясно е, че ако $L>0$ е горна граница за положителните корени на уравнението $x^n f\left(\frac{1}{x}\right)=0$, то $\frac{1}{L}$ е долна граница за положителните корени на уравнението $f(x)=0$.

Теорема на субституциите. Нека $f(x)$ е полином с реални коефициенти и в краищата на интервала (a, b) да приема стойности с обратни знаци, т. е. $f(a)\,f(b)<0$; тогава уравнението $f(x)=0$ има нечетен брой корени в интервала (a, b). Ако $f(a)\,f(b)>0$, уравнението $f(x)=0$ или няма корени в (a, b), или четен брой корени в този интервал.

Забележка. Тук, както и в следващите теореми, корените на уравнението се броят съобразно техните кратности. Например за полинома $f(x)=x^3-x^2$ имаме $f(-2)\,f(2)<0$ и в интервала $(-2, 2)$ уравнението $f(x)=0$ има три корена $x_1=x_2=0$ (двоен корен) и $x_3=1$ (прост корен).

Теорема на Рол. Между два последователни корена на уравнението $f(x)=0$, производното уравнение $f'(x)=0$ има нечетен брой корени.

Следствие 1. Ако m означава броят на реалните корени на уравнението $f(x)=0$, уравнението $f'(x)=0$ ще има най-малко $m-1$ реални корена. В частност, ако всички корени на уравнението $f(x)=0$ са реални, производното уравнение $f'(x)=0$ също ще има само реални корени.

Следствие 2. Между два последователни реални корена на уравнението $f'(x)=0$ уравнението $f'(x)=0$ не може да има повече от един корен.

Пример. Да намерим броя на реалните корени на уравнението $f(x)=0$, където

$$f(x)=x^5-2x^4+2x^3+4x^2-11x+3.$$

Производното уравнение $f'(x)=0$, т. е. $5x^4-8x^3+6x^2+8x-11=0$ има корени $x_1=1$, $x_2=-1$ и може да се запише във вида

$$(x^2-1)\,(5x^2-8x+11)=0.$$

Тъй като тричленът $5x^2-8x+11$ не се анулира за реални стойности на x, ясно е, че производното уравнение $f'(x)=0$ има точно два реални корена. Съгласно следствие 1 даденото уравнение $f(x)=0$ има най-много 3 реални корена. От неравенствата

$$f(-\infty)<0,\ f(-1)>0,\ f(1)<0,\ f(+\infty)>0$$

и от теоремата за субституциите заключаваме, че даденото уравнение има три реални корена, по един във всеки от интервалите $(-\infty,-1)$, $(-1,1)$, $(1,+\infty)$. Можем да намерим и по-малки интервали, като вземем пред вид, че $f(-2)<0$, $f(0)>0$, $f(2)>0$. Така се убеждаваме, че във всеки от интервалите $(-2,-1)$, $(0,1)$, $(1,2)$ уравнението $f(x)=0$ има точно по един корен и няма други реални корени.

Нека $f(x)=0$ е алгебрично уравнение с реални коефициенти, като предполагаме, че полиномът $f(x)$ е нареден по намаляващи (или по растящи) степени на x и членовете с коефициенти 0 са изпуснати. Казваме, че между два последователни члена на $f(x)$ има една *вариация*, когато коефициентите на тези членове са с обратни знаци. Изобщо, ако $a_0, a_1, \ldots, a_n$ е редица от реални числа, под *брой на вариациите* на тази редица ще разбираме броя на последователните смени на знаците на нейните членове, като се абстрахираме от равните на нула членове на редицата. Например броят на вариациите на редицата $2,-1,0,-2,3,-4$ е равен на 3. Ясно е, че броят на всички вариации в даден полином е равен на броя на вариациите в редицата от неговите коефициенти.

Теорема на Декарт. Броят на положителните корени на алгебричното уравнение $f(x)=0$ с реални коефициенти не надминава броя на вариациите в редицата от коефициентите му. Ако този брой m е по-малък от броя v на вариациите, разликата $v-m$ е четно число.

Пример. Уравнението

$$f(x)=x^6-23x^4+7x^2-8x+1=0$$

има $v=4$ вариации и следователно броят на положителните му корени е равен на 4 или на 2, или на 0.

Ако искаме да намерим горна граница за броя на отрицателните корени на уравнението $f(x)=0$, можем да приложим теоремата на Декарт за уравнението $f(-x)=0$. В случая уравнението $f(-x)=0$ има вида

$$x^6-23x^4+7x^2+8x+1=0$$

и броят на вариациите е равен на 2. Следователно последното уравнение има два, или нула на брой положителни корена, така че броят на отрицателните корени на даденото уравнение е равен на 2 или на 0. Пресмятането показва, че $f(-1)\,f(0)<0$, откъдето съгласно теоремата за субституциите следва, че в интервала $(-1,0)$ уравнението $f(x)=0$ има поне един корен. Ясно е тогава, че уравнението $f(x)=0$ ще има точно два отрицателни корена. Като вземем пред вид още, че $f(0)>0$ и $f(1)<0$, се убеждаваме, че даденото уравнение има или два, или четири положителни корена.

Следствие от теоремата на Декарт. Ако уравнението $f(x)=0$ има само реални корени, броят на положителните корени е равен на броя на вариациите в редицата от коефициентите на $f(x)$.

Теорема на Бюдан — Фурие. Нека $f(x)$ е полином от n-та степен с реални коефициенти. С v (c) да означим броя на вариациите в редицата от стойностите на полиномите.

$$f(x),\ f'(x),\ f''(x), \dots, f^{(n)}(x) \tag{1}$$

при $x=c$ (c произволно реално число). Нека в краищата на интервала (a, b) нито един от полиномите (1) да не се анулира. Броят на корените на уравнението $f(x)=0$ в интервала (a, b) не надминава разликата $v(a)-v(b)$ от вариациите на редицата (1) при $x=a$ и $x=b$. Ако този брой m е по-малък от $v(a)-v(b)$, разликата $v(a)-v(b)-m$ е четно число.

Забележка. Можем да се освободим от ограничението числата a и b да не анулират полиномите от редицата на Фурие (1), като вместо интервала (a, b) разглеждаме интервала $(a+\varepsilon, b-\varepsilon)$ при достатъчно малко $\varepsilon>0$.

Пример. Да определим броя на корените на уравнението за полинома $f(x)=x^6-3x^5-3x^4+11x^3-3x^2-3x+1$ във всеки един от интервалите $(-2, -1)$, $(-1,0)$, $(0,1)$, $(1,2)$, $(2,3)$.

Намираме производните на $f(x)$ и съответните им знаци за $x=-2, -1, 0, 1, 2, 3$, като за прегледност подреждаме резултатите в следната таблица:

	-2	-1	0	1	2	3
$f(x)=x^6-3x^5-3x^4+11x^3-3x^2-3x+1$	+	−	+	+	−	+
$\frac{1}{1!}f'(x)=6x^5-15x^4-12x^3+33x^2-6x-3$	−	+	−	+	−	+
$\frac{1}{2!}f''(x)=15x^4-30x^3-18x^2+33x-3$	+	+	−	−	−	+
$\frac{1}{3!}f'''(x)=20x^3-30x^2-12x+11$	−	−	+	−	+	+
$\frac{1}{4!}f^{IV}(x)=15x^2-15x-3$	+	+	−	−	+	+
$\frac{1}{5!}f^{V}(x)=6x-3$	−	−	−	−	+	+
$\frac{1}{6!}f^{VI}(x)=1$	+	+	+	+	+	+
$v=$	6	5	4	2	1	0

Съгласно теоремата на Бюдан — Фурие полиномът $f(x)$ има точно по един корен в интервалите $(-2, -1)$, $(-1, 0)$, $(1,2)$, $(2,3)$ и два или нула корена в интервала $(0,1)$. С непосредствена проверка се убеждаваме, че $f\left(\frac{1}{2}\right)<0$ и понеже $f(0)>0$ и $f(1)>0$, заключаваме, че уравнението $f(x)=0$ има два корена в интервала $(0,1)$.

За да определим точния брой на корените в даден интервал, можем да си послужим с една основна теорема на Щурм. Преди да формулираме тази теорема, ще дефинираме понятието *щурмова редица*. Нека $f(x)$ е полином с реални коефициенти и без кратни корени. Редицата от нулеви полиноми с реални коефициенти

$$f(x)=f_0(x),\ f_1(x),\ f_2(x), \ldots, f_s(x) \tag{2}$$

се нарича щурмова редица за полинома $f(x)$, когато са изпълнени следните условия:

1. Всеки два съседни полинома от редицата (2) нямат общи корени.

2. Последният полином $f_s(x)$ не се анулира за реални стойности на x.

3. Ако α е реален корен на полинома $f_k(x)$, $1 \leq k \leq s-1$, то $f_{k-1}(\alpha)\, f_{k+1}(\alpha)<0$.

4. Ако α е корен на $f(x)$, произведението $f(x)\, f_1(x)$ си сменя знака от — към +, когато x преминава през корена α отляво надясно.

Теорема на Щурм. Броят на реалните корени на уравнението $f(x)=0$ в интервала (a, b), където $f(a)\, f(b)<0$, е точно равен на разликата $v(a)-v(b)$ от броя на вариациите на щурмовата редица (2) при $x=a$ и $x=b$.

За да прилагаме теоремата на Щурм, е необходимо да разполагаме с щурмова редица. Такава редица можем да построим, като си послужим с алгоритъма на Евклид за намиране на най-голям общ делител на полиномите $f(x)$ и $f'(x)$. Полагаме $f_1(x)=f'(x)$. Ако $r_1(x)$ е остатъкът при делението на $f(x)$ с $f'(x)$, полагаме $f_2(x)=-r_1(x)$; ако $r_2(x)$ е остатъкът при делението на $f_1(x)$ с $f_2(x)$, полагаме $f_3(x)=-r_2(x)$ и т. н. Понеже полиномът $f(x)$ по предположение няма кратни корени, най-големият общ делител на $f(x)$ и $f'(x)$ е равен на 1, то най-накрая ще достигнем до полином $f_n(x)$, който е равен на отлична от 0 константа.

Така построената редица

$$f(x),\ f_1(x),\ f_2(x), \ldots, f_n(x)$$

удовлетворява всички условия от определението за щурмова редица.

Пример. Да намерим броя на реалните корени на уравнението

$$f(x)=x^5-5x^3-10x^2+2=0$$

в интервала $(-1,3)$.

Следвайки указания начин за построяване на щурмова редица намираме (абстрахирайки се от несъществените положителни числови множители):

$$f(x)=x^6-5x^3-10x^2+2, f_1(x)=x^4-3x^2-4x,$$
$$f_2(x)=x^3+3x^2-1, f_3(x)=-2x^2+x+1,$$
$$f_4(x)=-3x-1, f_5(x)=-1.$$

Между другото виждаме, че полиномите $f(x)$ и $f'(x)$ са взаимно прости и следователно уравнението $f(x)=0$ няма кратни корени. За знаците на членовете на така построената щурмова редица при $x=-1$ и $x=3$ получаваме съответно $-,+,-,-,+,$ и $+,+,+$ $-,-,-$. Имаме $v(-1)=4$, $v(3)=1$, $v(-1)-v(3)=3$. Съгласно теоремата на Щурм получаваме, че броят на корените на уравнението $f(x)=0$ в интервала $(-1,3)$ е равен на 3. Да отбележим, че даденото уравнение има най-много два положителни корена и един отрицателен (както лесно се вижда от теоремата на Декарт). Ясно е тогава, че уравнението $f(x)=0$ няма други реални корени, освен тези 3 корена от интервала $(-1,3)$. Разбира се, броят на реалните корени може да се намери и по теоремата на Щурм, приложена за интервала $(-\infty,+\infty)$. В случая имаме $v(-\infty)=4$, $v(\infty)=1$, $v(-\infty)-v(+\infty)=3$, откъдето също заключаваме, че уравнението $f(x)=0$ има точно 3 реални корена.

1. Намерете горна и долна граница за реалните корени на уравнението $f(x)=0$, където:

а) $f(x)=x^4+4x^3-8x^2-10x+14$;
б) $f(x)=x^5-56x^4+34x^2+31x-67$;
в) $f(x)=2x^5+3x^4-7x^2-36x+11$;
г) $f(x)=x^6+10x^5+25x^4-24x^3-136x^2-64x+80$.

2. Правило на Лагер за намиране горна граница на положителните корени. Нека

$$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n,\quad a_0>0,$$

е полином с реални коефициенти и да положим

$$f_0(x)=a_0,\ f_1(x)=a_0x+a_1,\ f_2(x)=a_0x^2+a_1x+a_2,\ldots,$$
$$f_{n-1}(x)=a_0x^{n-1}+a_1x^{n-2}+\ldots+a_{n-2}x+a_{n-1},\ f_n(x)=f(x).$$

Ако за положителното число L имаме

$$f_0(L)>0,\ f_1(L)>0,\ f_2(L)>0,\ldots,f_n(L)>0,$$

то L е горна граница за положителните корени на уравнението $f(x)=0$.

Упътване. Използувайте тъждеството

$$q(x)=f_0(L)x^{n-1}+f_1(L)x^{n-2}+\ldots+f_{n-1}(L),$$

където $q(x)$ е частното при делението на $f(x)$ с $x-L$ и $r=f_n(L)$ е съответният остатък.

3. Нека N да означава абсолютната стойност на най-големия по модул отрицателен коефициент на полинома $f(x)$ и $A_0, A_1, A_2, \ldots, A_{p-1}$ са положителните коефициенти, които предшествуват първия отрицателен коефициент. Докажете, че числото

$$1+\frac{N}{A_0+A_1+A_2+\ldots+A_{p-1}}$$

е горна граница за положителните корени на уравнението $f(x)=0$.

Решение. Съгласно условието на задачата при $x>0$ ще имаме

$$f(x)>A_0x^n+A_1x^{n-1}+\ldots+A_{p-1}x^{n-p+1}-N(x^{n-p}+x^{n-p-1}+\ldots+1).$$

Ако положим

$$\alpha=A_0+A_1+\ldots+A_{p-1},$$

от неравенството $x>1+\frac{N}{\alpha}$ получаваме последователно

$$\alpha x>\alpha+N,$$
$$\alpha x^2>\alpha x+Nx,$$
$$\ldots\ldots\ldots$$
$$\alpha x^{n-p-1}>\alpha x^{n-p-2}+Nx^{n-p-2},$$
$$\alpha x^{n-p}>\alpha x^{n-p-1}+Nx^{n-p-1},$$
$$\alpha x^{n-p+1}>\alpha x^{n-p}+Nx^{n-p},$$

откъдето след почленно събиране ще имаме

$$N(x^{n-p}+x^{n-p-1}+\ldots+1)<\alpha x^{n-p+1}-\alpha.$$

Но тогава

$$f(x)>A_0 . x^n+A_1x^{n-1}+\ldots+A_{p-1}x^{n-p+1}-\alpha x^{n-p+1}+\alpha,$$

откъдето

$$f(x)>(A_0+A_1+\ldots+A_{p-1}-\alpha)x^{n-p+1}+\alpha=\alpha>0.$$

4. Намерете горна граница за положителните корени на уравнението $2x^6+5x^4-3x^3+13x^2-39x+72=0$ по всеки един от известните ви методи.

5. Като използувате теоремата на Рол и теоремата за субституциите, намерете броя на реалните корени на уравнението $f(x)=0$ и отделете тези корени в интервали с дължина 1, където

а) $f(x)=x^5+2x^4+x^3-4x^2-8x+3$;

б) $f(x)=x^4-12x^3+43x^2-42x-12$;

в) $f(x)=3x^4-4x^3-36x^2+5$;

г) $f(x)=x^6-2x^5-x^4-12x^3+17x^2+82x+50$.

Отг. а) три реални корена, по един във всеки от интервалите $(-2, -1)$, $(0,1)$ $(1, 2)$; б) два реални корена, по един във всеки от интервалите $(-1{,}0)$, $(6, 7)$; в) четири реални корена, по един във всеки от интервалите $(-3, -2)$, $(-1, 0)$, $(0, 1)$, $(4, 5)$.

6. Намерете броя на реалните корени на уравнението $f(x)=$ $=0$, където:

а) $f(x)=\frac{x^n}{n}+\frac{x^{n-1}}{n-1}+\ldots+\frac{x^2}{2}+\frac{x}{1}+1$;

б) $f(x)=\frac{x^n}{n!}+\frac{x^{n-1}}{(n-1)!}+\ldots+\frac{x^2}{2!}+\frac{x}{1!}+1$;

в) $f(x)=nx^n-x^{n-1}-\ldots-x-1$.

Отг. а) при четно n — няма реални корени, при нечетно n — един реален корен; б) също както в случая а); в) при нечетно n числото 1 е единственият реален корен, при четно n — два реални корена, от които единият е равен на 1, а другият е отрицателен.

7. Като използувате теоремата на Рол и теоремата за субституциите, намерете броя на реалните корени на уравнението $f(x)=0$ в зависимост от стойностите на реалния параметър λ:

а) $f(x)=x^5-20x+\lambda$;

б) $f(x)=3x^4-4x^3+6x^2-12x+\lambda$;

в) $f(x)=3x^4-16x^3-6x^2+48x+\lambda$;

г) $f(x)=nx^{n+1}-(n+1)x^n+\lambda$.

Отг. а) при $|\lambda|>16\sqrt{2}$ — един реален корен, а при $|\lambda|\leq 16\sqrt{2}$ — три реални корена;
б) при $\lambda>7$ — няма реални корени, а при $\lambda\leq 7$ — два реални корена;
в) при $\lambda<-29$ или $35<\lambda\leq 40$ — два реални корена; при $-29\leq\lambda\leq$ ≤ 35 — четири реални корена; при $\lambda>40$ — няма реални корени;
г) при нечетно n и $\lambda<0$ или $0<\lambda\leq 1$ — два реални корена; при четно n и $\lambda<0$ или $\lambda>1$ — един реален корен; при $\lambda=0$ всичките корени са реални; при четно n и $0<\lambda\leq 1$ — три реални корена; при нечетно n и $\lambda>1$ — няма реални корени.

8. Намерете условието, което трябва да удовлетворяват отличните от нула реални числа p и q, така че уравнението x^5+ $px+q=0$ да има възможно най-много реални корени.

Отг. $3125q^4-256p^5<0$ (тогава уравнението има три реални корена).

9. Като използувате теоремата на Декарт, намерете горна граница за броя на положителните и отрицателните корени на уравнението:

а) $x^4+3x^3-2x^2-x-1=0$;

б) $2x^5+4x^3+2x^2-x+1=0$;

в) $4x^6-x^5+x^2-7x-5=0$;

г) $x^6-2x^5+3x^4-10x^2-35x-10=0$.

10. С помощта на теоремата на Бюдан — Фурие намерете броя на реалните корени на уравнението $f(x)=0$ в интервала (a, b), където:

а) $f(x)=3x^4-6x^3-2x^2+5x+1,\ a=-1,\ b=2;$
б) $f(x)=2x^4-2x^3+4x^2-6x-5,\ a=-2,\ b=3;$
в) $f(x)=12x^5-15x^4+30x^2-60x+8,\ a=-2,\ b=2;$
г) $f(x)=16x^5-10x^4+20x^2-80x+99,\ a=-3,\ b=0;$
д) $f(x)=2x^5-10x^4-20x^2-10x+7,\ a=0,\ b=6.$

Отг. а) 4; б) 2; в) 3; г) 1; д) 2.

11. С помощта на теоремата на Щурм намерете броя на реалните корени на уравнението $f(x)=0$ и ги отделете в интервали с дължина 1, където:

а) $f(x)=x^4-x^2-3x-1;$
б) $f(x)=x^4-2x^3-7x^2+8x+1;$
в) $f(x)=x^4-4x^3+8x^2-12x+8;$
г) $f(x)=x^4-2x^3+2x^2-6x+1;$
д) $f(x)=x^5+5x^4+10x^2-5x-3.$

Отг. а) два корена: $(-1,0)$, $(1,\ 2)$;
б) четири корена: $(-3,\ -2)$, $(-1,0)$, $(1,2)$;
в) два корена: $x_1=2,\ 1<x_2<2$;
г) два корена: $(0,\ 1)$, $(2,\ 3)$;
д) три корена: $(-6,\ -5)$, $(-1,0)$, $(0,1)$.

12. Докажете, че уравнението $f(x)=0$, където $f(x)=x^n+(a+b)x^{n-1}+(a^2+ab+b^2)x^{n-2}+\ldots+(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1})x+(a^n+a^{n-1}b+\ldots+ab^{n-1}+b^n)$
и a, b са произволни реални числа, има най-много един реален корен.

Упътване. Приложете теоремата на Рол за полинома

$$g(x)=(x-a)(x-b)f(x).$$

13. Покажете, че ако всички корени на уравнението $f(x)=0$ са реални, уравнението $[f'(x)]^2-f(x)\,f''(x)=0$ няма реални корени.

Упътване. Диференцирайте тъждеството $\dfrac{f'(x)}{f(x)}=\sum\limits_{k=1}^{n}\dfrac{1}{x-x_k}$, където x_k са корените на уравнението $f(x)=0$.

14. Покажете, че ако всички корени на уравненията $f(x)-a=0$ и $f(x)-b=0$ са реални и λ е число, заключено между a и b, уравнението $f(x)-\lambda=0$ също има само реални корени.

Решение. Съгласно теоремата на Рол всички корени на уравнението $f'(x)=0$ са реални. Да ги означим с $\xi_1\leq\xi_2\leq\ldots\leq\xi_{n-1}$. Нека още $x_1\leq x_2\leq\ldots\leq x_n$ означават корените на уравнението $f(x)-a=0$, а $y_1\leq y_2\leq\ldots\leq y_n$ — корените на $f(x)-b=0$. Ще имаме

$$y_1\leq\xi_1\leq y_2\leq\xi_2\leq\ldots\leq y_{n-1}\leq\xi_{n-1}\leq y_n,$$
$$x_1\leq\xi_1\leq x_2\leq\xi_2\leq\ldots\leq x_{n-1}\leq\xi_{n-1}\leq x_n.$$

Оттук следва, че интервалите $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ нямат общи точки. Тъй като $f(x_i)-\lambda=a-\lambda$ и $f(y_i)-\lambda=b-\lambda$, то $[f(x_i)-\lambda][f(y_i)-\lambda<0$ и следователно във всеки от интервалите (x_i, y_i), $i=1, 2, \ldots, n$, уравнението $f(x)-\lambda=0$ има по един корен. Разбира се, в случай на кратни корени, при броенето им трябва да се съобразяваме с техните кратности.

16. Нека $f(x)$ е полиномът с реални коефицинти и $\lambda\neq0$ е произволно реално число. Покажете, че $f'(x)+\lambda f(x)=0$ има поне толкова реални корени, колкото и $f(x)=0$.

Решение Нека a и b са два последователни корена на уравнението $f(x)=0$ съответно от кратности k и l. Ще имаме

$$f(x)=(x-a)^k(x-b)^l g(x),\ g(a)\neq0,\ g(b)\neq0,$$

където полиномът $g(x)$ не си променя знака в интервала (a, b) За полинома $h(x)=f'(x)+\lambda f(x)$ получаваме

$$h(x)=(x-a)^{k-1}(x-b)^{l-1}\varphi(x),$$

където

$$\varphi(x)=k(x-b)\,g(x)+l\,(x-a)\,g(x)+(x-a)(x-b)\,g'(x)+\lambda(x-a)(x-b)\,g(x$$

Корените на $h(x)=0$, които лежат в интервала (a, b) съвпадат с тези на уравнението $\varphi(x)=0$ от същия интервал. Поеже

$$\varphi(a)=k(a-b)\,g(a),\ \varphi(b)=l(b-a)\,g(b),$$

то числата $\varphi(a)$ и $\varphi(b)$ са с противоположни знаци и следователно уравнението $h(x)=0$ има нечетен брой корени в интервала (a, b). Нека сега $x_1<x_2<\ldots<<x_p$ са реалните корени на уравнението $f(x)=0$ и $k_1, k_2, \ldots, k_p$ са техните кратности, $k_1+k_2+\ldots+k_p=s$. Тук s означава броя на всичките реални корени на уравнението $f(x)=0$. Същите числа $x_1, x_2, \ldots, x_p$ са корени на уравнението $h(x)=0$ от кратности $k_1-1, k_2-1, \ldots, k_p-1$. Съгласно доказаното по-горе във всеки от интервалите $(x_1, x_2), (x_2, x_3), \ldots, (x_{p-1}, x_p)$, уравнението $h(x)=0$ ще има поне по един корен, така че $h(x)=0$ ще има най-малко

$$(k_1-1)+(k_2-1)+\ldots+(k_p-1)+p-1=s-1$$

реални корена. Като вземем пред вид още, че разглежданите полиноми $f(x)$ и $h(x)$ са от една и съща степен и с реални коефициенти и следователно нереалните корени са два по два комплексно спрегнати, заключаваме, че уравнението $h(x)=0$ ще има поне s на брой реални корени.

16. В означенията на предната задача покажете, че ако уравнението $f(x)=0$ има само реални корени, всичките корени на уравнението $f'(x)+\lambda f(x)=0$ също са реални.

17. Теорема на Пулен — Ермит. Нека $f(x)$ е полином с реални коефициенти и $g(x)=a_0x^k+a_1x^{k-1}+\ldots+a_{k-1}x+a_k$, $a_k\neq0$ е полином, всичките нули на който са реални. Тогава уравнението

$$a_0f(x)+a_1f'(x)+\ldots+a_kf^{(k)}(x)=0$$

има поне толкова реални корена, колкото уравнението $f(x)=0$

Упътване. Приложете неколкократно резултата от зад. 15, като стойности на $-\lambda$ вземете нулите на $g(x)$.

§ 7. СПЕЦИАЛНИ ПОЛИНОМИ

Ортогонални полиноми. Нека $p(x)$ е неотрицателна функция в интервала (a, b) (краен или безкраен), за която съществуват интегралите

$$\mu_n=\int_a^b x^n p(x)\, dx,\ n=0, 1, 2,\dots$$

и $\mu_0>0$. Ще казваме, че две функции $g(x)$ и $h(x)$ са ортогонални в интервала (a, b) относно теглото $p(x)$, когато

$$\int_a^b p(x)\, g(x)\, h(x)\, dx=0.$$

Една редица от полиноми $P_0(x), P_1(x),\dots,P_n(x),\dots$, от степени съответно $0, 1, 2,\dots, n,\dots$, се нарича ортогонална в интервала (a, b) спрямо теглото $p(x)$, когато всеки два различни полинома от редицата са ортогонални, т. е.:

$$\int_a^b p(x)\, P_i(x)\, P_j(x)\, dx=0 \text{ при } i\neq j,\ i, j=0, 1, 2,\dots$$

1. Докажете, че за всяко тегло $p(x)$ в интервала (a, b) съществува еднозначно определена ортогонална редица от полиноми с положителни старши коефициенти

$$P_0(x),\ P_1(x),\dots,P_n(x),\dots$$

и нормирана с условието $\int_a^b p(x)\, P_k^2(x)\, dx=1,\ k=0, 1, 2,\dots$

Упътване. За краткост положете

$$\int_a^b p(x)\, g(x)\, h(x)\, dx=(g, h),$$

където g и h са полиноми с произволни реални коефициенти. Така дефинираното число (g, h) притежава свойствата на скаларно произведение в линейното пространство от всички полиноми с реални коефициенти. Като вземете пред вид това, използувайте метода на Грам и Шмид за ортогонализиране.

2. Покажете, че за полиномите $P_n(x)$ от предната задача, които образуват ортогонална и нормирана система в интервала (a, b) спрямо теглото $p(x)$, са в сила равенствата

$$P_n(x)=\frac{1}{\sqrt{\Delta_{n-1}\Delta_n}}\begin{vmatrix} \mu_0 & \mu_1 & \dots & \mu_{n-1} & 1 \\ \mu_1 & \mu_2 & \dots & \mu_n & x \\ \dots & \dots & \dots & \dots & \dots \\ \mu_n & \mu_{n+1} & \dots & \mu_{2n-1} & x^n \end{vmatrix},\ n\geq 1,$$

където

$$\mu_l=\int_a^b x^l p(x)\,dx,\ l=0, 1, 2, \ldots,$$

е l-тият момент на функцията $p(x)$ и

$$\Delta_n=\begin{vmatrix} \mu_0 & \mu_1 & \cdot & \cdot & \cdot & \mu_n \\ \mu_1 & \mu_2 & \cdot & \cdot & \cdot & \mu_{n+1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \mu_n & \mu_{n+1} & \cdot & \cdot & \cdot & \mu_{2n} \end{vmatrix}$$

е съответната детерминанта на Грам.

3. Докажете, че всеки полином $f(x)$ от степен $\leq n$ може да се представи еднозначно във вида

$$f(x)=a_0P_0(x)+a_1P_1(x)+\ldots+a_nP_n(x),$$

където $P_0(x)$, $P_1(x), \ldots$ е ортогонална в (a, b) система от полиноми и за коефициентите (на Фурие) a_k са в сила равенствата

$$a_k=\frac{1}{A_k}\int_a^b P_k(x)f(x)p(x)\,dx,\ k=0, 1, 2, \ldots, n,$$

$$A_k=\int_a^b p(x)P_k^2(x)dx.$$

4. В означенията от предната задача покажете, че е в сила следното равенство (*на Парсифал*)

$$\int_a^b p(x)\,f^2(x)\,dx=\sum_{\nu=0}^{\infty}A_\nu a_\nu^2.$$

5. Нека $P_0(x)$, $P_1(x), \ldots, P_n(x), \ldots$ е ортогонална редица от полиноми спрямо теглото $p(x)$ в интервала (a, b) и k_n, k_n' да са съответно коефициентите пред x^n и x^{n-1} в полинома $P_n(x)$. Покажете, че

$$P_{n+1}(x)=(\alpha_nx+\beta_n)P_n(x)-\gamma_nP_{n-1}(x),\ n=1, 2, \ldots,$$

където

$$\alpha_n=\frac{k_{n+1}}{k_n},\quad \beta_n=\alpha_n\left(\frac{k_{n+1}'}{k_{n+1}}-\frac{k_n'}{k_n}\right),\quad \gamma_n=\frac{\alpha_nA_n}{\alpha_{n-1}A_{n-1}}.$$

Решение. Полиномът $P_{n+1}(x)-\alpha_nx\,P_n(x)$ е степен $\leq n$ и следователно при подходящи $\delta_0, \delta_1, \ldots, \delta_n$ ще имаме

$$P_{n+1}(x)-\alpha_nxP_n(x)=\delta_0\,P_0(x)+\delta_1P_1(x)+\ldots+\delta_n\,P_n(x).$$

Като умножим почленно последното равенство с $p(x)P_\nu(x)$, $\nu=0, 1,\dots, n-2$, и интегрираме, ще получим

$$\delta_\nu\int_a^b p(x)P_\nu^2(x)\,dx=0\,,$$

откъдето следва, че $\delta_\nu=0$ за $\nu=0, 1, 2,\dots, n-2$. И така

$$P_{n+1}(x)=(\alpha_n x+\beta_n)P_n(x)+\delta_{n-1}P_{n-1}(x).$$

Оттук, по подобен начин получаваме

$$\alpha_n\int_a^b xp(x)P_n(x)P_{n-1}(x)\,dx+\delta_{n-1}\int_a^b p(x)P_{n-1}^2(x)dx=0,$$

$$\int_a^b xp(x)P_n(x)P_{n-1}(x)dx=\int_a^b p(x)P_n(x)(k_{n-1}x^n+c_1'x^{n-1}+\dots)\,dx=$$

$$=\frac{k_{n-1}}{k_n}\int_a^b p(x)P_n^2(x)\,dx=\frac{k_{n-1}}{k_n}A_n\,.$$

Намираме

$$\delta_{n-1}=-\alpha_n\frac{k_{n-1}}{k_n}\cdot\frac{A_n}{A_{n-1}}=-\gamma_n.$$

Чрез сравняване на коефициентите пред x^n от двете страни на (1), получаваме

$$k'_{n+1}=\alpha_n k'_n+\delta_n k_n$$

или

$$\delta_n=\frac{1}{k_n}(k'_{n+1}-\alpha_n k'_n)=\beta_n\,.$$

Формулата (1) остава в сила и при $n=0$, ако положим $P_{-1}(x)=0$.

6. Докажете следното тъждество (*Кристофел—Дарбу*)

$$\sum_{\nu=0}^{n}\frac{1}{A_\nu}P_\nu(x)P_\nu(y)=\frac{1}{A_n\alpha_n}\,\frac{P_{n+1}(x)P_n(y)-P_{n+1}(y)P_n(x)}{x-y}\,.$$

Решение. Съгласно предната задача имаме

$$P_{\nu+1}(x)=(\alpha_\nu x+\beta_\nu)P_\nu(x)-\gamma_\nu P_{\nu-1}(x),$$
$$P_{\nu+1}(y)=(\alpha_\nu y+\beta_\nu)P_\nu(y)-\gamma_\nu P_{\nu-1}(y).$$

Първото умножаваме с $P_\nu(y)$, а второто — с $P_\nu(x)$ и изваждаме почленно

$$P_{\nu+1}(x)P_\nu(y)-P_{\nu+1}(y)P_\nu(x)=\alpha_\nu(x-y)P_\nu(x)P_\nu(y)+$$
$$+\gamma_\nu[P_\nu(x)P_{\nu-1}(y)-P_\nu(y)P_{\nu-1}(x)].$$

Оттук, като използуваме още веднаж тъждеството от предната задача, получаваме

$$\frac{1}{A_\nu}(x-y)P_\nu(x)P_\nu(y)=\frac{1}{A_\nu\alpha_\nu}[P_{\nu+1}(x)P_\nu(y)-P_{\nu+1}(y)P_\nu(x)]+$$

$$+\frac{1}{A_{\nu-1}\alpha_{\nu-1}}[P_\nu(x)P_{\nu-1}(y)-P_\nu(y)P_{\nu-1}(x)].$$

Последното равенство е вярно и за $\nu=0$, стига да положим $P_{-1}(x)=P_{-1}(y)=0$. Давайки на ν стойности $\nu=0, 1, 2,\dots, n$, чрез почленно събиране получаваме

$$\sum_{\nu=0}^{n}\frac{1}{A_\nu}P_\nu(x)P_\nu(y)=\frac{1}{A_n\alpha_n}\cdot\frac{P_{n+1}(x)P_n(y)-P_{n+1}(y)P_n(x)}{x-y}.$$

7. В означенията от предните задачи покажете, че за всяко реално x е в сила неравенството

$$\frac{k_n}{k_{n+1}}[P'_{n+1}(x)P_n(x)-P'_n(x)P_{n+1}(x)]>0.$$

Решение. В тъждеството на Кристофел—Дарбу (зад. 6) полагаме $y=x$, откъдето получаваме

$$\frac{k_n}{A_n k_{n+1}}[P'_{n+1}(x)P_n(x)-P'_n(x)P_{n+1}(x)]=\sum_{\nu=0}^{n}\frac{1}{A_\nu}P_\nu^2(x)>0.$$

8. Докажете, че нулите на ортогоналните в интервала (a, b) полиноми $P_n(x)$ са реални и прости и лежат в същия интервал.

Решение. Да означим с $x_1, x_2, \ldots, x_k$ нулите на $P_n(x)$, които са от нечетна кратност и лежат в интервала (a, b). Очевидно $0\leq k\leq n$. Да положим

$$R(x)=(x-x_1)(x-x_2)\ldots(x-x_k)$$

при $k\geq 1$ и $R(x)=1$ при $k=0$. Полиномът $R(x)$ променя своя знак в (a, b) само в точките, където $P_n(x)$ си сменя знака. Следователно произведението $p(x)P_n(x)R(x)$ не си мени знака в (a, b). Ако $k<n$, ще имаме

$$\int_a^b p(x)P_n(x)R(x)\,dx=0,$$

което води до противоречие. И така трябва да имаме $k=n$.

9. Докажете, че нулите на ортогоналните полиноми $P_n(x)$ и $P_{n-1}(x)$ се взаимно разделят, т. е. между две последователни нули на $P_n(x)$ има точно една нула на $P_{n-1}(x)$.

Решение. Ще предполагаме, че коефициентите пред най-високите степени на x в полиномите $P_n(x)$ и $P_{n-1}(x)$ са положителни, т. е. $k_n>0$ и $k_{n-1}>0$. Съгласно зад. 7 ще имаме

$$P'_n(x)P_{n-1}(x)-P'_{n-1}(x)P_n(x)>0$$

при всяко реално x. Нека α и β са две последователни нули на $P_n(x)$; тогава

$$P'_n(\alpha)P_{n-1}(\alpha)>0,\quad P'_n(\beta)P_{n-1}(\beta)>0.$$

Тъй като $P'_n(\alpha)$ и $P'_n(\beta)$ са с противоположни знаци, то $P_{n-1}(\alpha)$ и $P_{n-1}(\beta)$ са също с противоположни знаци. Следователно между α и β има поне една нула на $P_{n-1}(x)$. Като вземем пред вид, че $P_{n-1}(x)$ е от степен $n-1$ и че нулите на $P_n(x)$ са реални и прости, се убеждаваме, че между всеки две последователни нули на $P_n(x)$ има точно една нула на $P_{n-1}(x)$.

10. Нека $x_1, x_2, \ldots, x_n$ да означават нулите на ортогоналния полином $P_n(x)$ и $F(x)$ да е произволен полином с реални коефициенти от степен $\leq 2n-1$. Докажете следната *квадратурна формула на Гаус*

$$\int_a^b p(x)F(x)\,dx=\sum_{\nu=1}^{n}H_\nu F(x_\nu),$$

където числата H_ν (коефициенти на Кристофел) са положителни и се определят от равенствата

$$H_\nu=\frac{1}{[P_n'(x_\nu)]^2}\int_a^b p(x)\left[\frac{P_n(x)}{x-x_\nu}\right]^2 dx,\quad \nu=1,\ 2,\dots,n.$$

Решение. Разделяме $F(x)$ на $P_n(x)$ и получаваме

$$F(x)=P_n(x)\,Q(x)+R(x),$$

където $R(x)$ е полином от степен $\leq n-1$. Имаме

$$F(x_\nu)=R(x_\nu)\ \text{при}\ \nu=1,\ 2,\dots,\ n.$$

Съгласно интерполационната формула на Лагранж, можем да представим полинома $R(x)$ във вида

$$R(x)=\sum_{\nu=1}^{n}R(x_\nu)\frac{P_n(x)}{(x-x_\nu)P'_n(x_\nu)},$$

или все едно

$$R(x)=\sum_{\nu=1}^{n}F(x_\nu)\frac{P_n(x)}{(x-x_\nu)\,P'_n(x_\nu)}.$$

По-нататък получаваме

$$\int_a^b p(x)\,F(x)\,dx=\int_a^b p(x)\,R(x)\,dx=\sum_{\nu=1}^{n}F(x_\nu)\int_a^b\frac{p(x)\,P_n(x)\,dx}{(x-x_\nu)\,P'_n(x_\nu)}\,dx=$$

$$=\sum_{\nu=1}^{n}H_\nu\,F(x_\nu),$$

където числата

$$H_\nu=\frac{1}{P'_n(x_\nu)}\int_a^b\frac{P_n(x)}{x-x_\nu}\,dx$$

не зависят от полинома $F(x)$. В частност при $F(x)=\left[\frac{P_n(x)}{x-x_\nu}\right]$ ще имаме

$$\int_a^b p(x)\left[\frac{P_n(x)}{x-x_\nu}\right]dx=H_\nu\,[P'_n(x_\nu)]^2,$$

откъдето следва, че числата H_ν, $\nu=1,\ 2,\dots,\ n$, са положителни.

11. Покажете, че

$$\int_a^b p(x)\,dx=H_1+H_2+\dots+H_n.$$

Определение. Полиномите $P_n^{(\alpha,\beta)}(x)$, дефинирани чрез равенствата

$$P_n^{(\alpha,\beta)}(x)=\frac{(-1)^n}{2^n n!}(1-x)^{-\alpha}(1+x)^{-\beta}\frac{d^n}{dx^n}[(1-x)^{\alpha+n}(1+x)^{\beta+n}],$$

$$\alpha>-1,\ \beta>-1,\ n=0,\ 1,\ 2,\dots,$$

се наричат *полиноми на Якоби.*

12. Докажете, че

а) $P_0^{(\alpha,\beta)}(x)=1$, $P_1^{(\alpha,\beta)}(x)=\frac{1}{2}[(\alpha+\beta+2)x+(\alpha-\beta)]$.

$$P_2^{(\alpha,\beta)}(x)=\frac{1}{8}\{[(\alpha+\beta)^2+7(\alpha+\beta)+12]x^2+2(\alpha-\beta)(\alpha+\beta+3)x+$$
$$+(\alpha-\beta)^2-(\alpha+\beta)-4\};$$

б) $P_n^{(\alpha,\beta)}(x)=\sum_{\nu=0}^{n}\binom{n+\alpha}{n-\nu}\binom{n+\beta}{\nu}\left(\frac{x-1}{2}\right)^{\nu}\left(\frac{x+1}{2}\right)^{n-\nu}$;

в) $P_n^{(\alpha,\beta)}(1)=\binom{n+\alpha}{n}$.

Тук, както и по-горе, за всяко x имаме по дефиниция

$$\binom{x}{n}=\frac{x(x-1)(x-2)\ldots(x-n+1)}{1.2.3\ldots n};$$

г) $P_n^{(\alpha,\beta)}(-x)=(-1)^nP_n^{(\beta,\alpha)}(x)$.

Упътване. За да докажете б), използвайте формулата на Лайбниц

$$(uv)^{(n)}=\sum_{\nu=0}^{n}\binom{n}{\nu}u^{(\nu)}v^{(n-\nu)}.$$

Следващите твърдения се получават лесно от б).

13. Докажете, че полиномите на Якоби $P_n^{(\alpha,\beta)}(x)$ са ортогонални в интервала $(-1,1)$ спрямо теглото $p(x)=(1-x)^{\alpha}(1+x)^{\beta}$, т. е.

$$\int_{-1}^{1}(1-x)^{\alpha}(1+x)^{\beta}P_n^{(\alpha,\beta)}(x)P_m^{(\alpha,\beta)}(x)dx=0,\ n\neq m.$$

Решение. Достатъчно е да докажем, че за всеки полином $f(x)$ от степен $\leq n-1$ е в сила равенството

$$\int_{-1}^{1}(1-x)^{\alpha}(1+x)^{\beta}f(x)P_n^{(\alpha,\beta)}(x)\,dx=0.$$

За краткост да положим $u=(1-x)^{n+\alpha}(1+x)^{n+\beta}$. Тогава горното равенство приема вида

$$\int_{-1}^{1}f(x)u^{(n)}(x)\,dx=0.$$

Като интегрираме по части, преобразуваме лявата страна на равенството във вида

$$[u^{(n-1)}f-u^{(n-2)}f'+\ldots+(-1)^{n-1}uf^{(n-1)}]_{-1}^{+1}+(-1)^n\int_{-1}^{1}u(x)f^{(n)}(x).$$

От формулата на Лайбниц се вижда, че k-тата производна на u при $0\leq k\leq n-1$ съдържа като множител $1+x$ в степен $\geq\alpha+n-k$ и $1-x$ — в степени $\geq\beta+n-k$.

Следователно тази производна се анулира в точките $x=-1$ и $x=1$. Тъй като и $f^{(n)}(x)=0$, твърдението е доказано.

14. Покажете, че за коефициентите k_n и k_n' пред x^n и x^{n-1} в n-тия полином $P_n^{(\alpha,\beta)}(x)$ на Якоби и за нормиращия множител

$$A_n=\int_{-1}^{1}(1-x)^{\alpha}(1+x)^{\beta}[P_n^{(\alpha,\beta)}(x)]^2\,dx,$$

са в сила равенствата

$$k_n=\frac{1}{2^n}\binom{2n+\alpha+\beta}{n},\quad k_n'=\frac{\alpha-\beta}{2^n}\binom{2n+\alpha+\beta-1}{n-1},$$

$$A_n=\frac{2^{\alpha+\beta+1}}{2n+\alpha+\beta+1}\cdot\frac{\Gamma(n+\alpha+1)\,\Gamma(n+\beta+1)}{n!\,\Gamma(n+\alpha+\beta+1)}.$$

Тук $\Gamma(x)$ означава известната от анализа гама-функция на Ойлер. $\Gamma(x)=\int_0^{\infty}e^{-y}y^{x-1}\,dy$; в частност $\Gamma(n)=(n-1)!$ при всяко естествено число n.)

Решение. Като вземем пред вид равенството

$$(x-1)^{n-\nu}(x+1)^{\nu}=x^{n-\nu}-(n-\nu)x^{n-\nu-1}+\ldots](x^{\nu}+\nu x^{\nu-1}+\ldots)=$$
$$=x^n+(2\nu-n)x^{n-1}+\ldots$$

и тъждеството б) от зад. 12, за коефициентите k_n и k_n' получаваме

$$k_n=\frac{1}{2^n}\sum_{\nu=0}^{n}\binom{n+\alpha}{\nu}\binom{n+\beta}{n-\nu},\quad k_n'=\frac{1}{2^n}\sum_{\nu=0}^{n}\binom{n+\alpha}{\nu}\binom{n+\beta}{n-\nu}(2\nu-n).$$

За да опростим горните изрази, умножаваме безкрайните редове

$$(1+x)^p=\sum_{\mu=0}^{\infty}\binom{p}{\mu}x^{\mu},\quad (1+x)^q=\sum_{\nu=0}^{\infty}\binom{q}{\nu}x^{\nu},$$

откъдето получаваме

$$(1+x)^{p+q}=\sum_{\mu=0}^{\infty}\binom{p}{\mu}x^{\mu}\sum_{\nu=0}^{\infty}\binom{q}{\nu}x^{\nu}=\sum_{\tau=0}^{\infty}\binom{p+q}{\tau}x^{\tau}$$

и чрез сравняване на коефициентите пред x^n достигаме до формулата

$$\sum_{\mu=0}^{n}\binom{p}{\mu}\binom{q}{n-\mu}=\binom{p+q}{n}.$$

По-нататък, като диференцираме реда за $(1+x)^p$ и умножим с

$(1+x)^q=\sum_{\nu=0}^{\infty}\binom{q}{\nu}x^\nu$, получаваме

$$p(1+x)^{p+q-1}=\sum_{\mu=1}^{\infty}\mu\binom{p}{\mu}x^\mu\sum_{\nu=0}^{\infty}\binom{q}{\nu}x^\nu=p\sum_{\tau=0}^{\infty}\binom{p+q-1}{\tau}x^\tau,$$

откъдето чрез сравняване на коефициентите пред x^{n-1} намираме

$$\sum_{\mu=1}^{n}\mu\binom{p}{\mu}\binom{q}{n-\mu}=p\binom{p+q-1}{n-1}.$$

С помощта на доказаните формули лесно получаваме равенствата

$$k_n=\frac{1}{2^n}\binom{2n+\alpha+\beta}{n} \text{ и } k_n'=\frac{\alpha-\beta}{2^n}\binom{2n+\alpha+\beta-1}{n-1}.$$

За нормиращия множител A_n имаме

$$A_n=k_n\int_{-1}^{1}x^n(1-x)^\alpha(1+x)^\beta P_n^{(\alpha,\beta)}(x)\,dx=\frac{k_n}{2^n n!}\int_{-1}^{1}x^n u^{(n)}\,dx,$$

откъдето с интегриране по части получаваме

$$A_n=\frac{k_n}{2^n}\int_{-1}^{1}(1-x)^{\alpha+n}(1+x)^{\beta+n}dx.$$

Като извършим трансформацията $x=2t-1$, интегралът се свежда до $2^{\alpha+\beta+2n-}$ $B(\alpha+n,\ \beta+n)$, където $B(p;q)$ е интегралът на Ойлер

$$B(p,q)=\int_0^1 t^q(1-t)^p dt=\frac{\Gamma(p+1)\Gamma(q+1)}{\Gamma(p+q+2)},\quad p,\ q>1.$$

Следователно

$$A_n=\frac{2^{\alpha+\beta+1}}{2n+\alpha+\beta+1}\cdot\frac{\Gamma(n+\alpha+1)\Gamma(n+\beta+1)}{n!\,\Gamma(n+\alpha+\beta+1)}.$$

15. Докажете, че всеки три последователни полинома на Якоби са свързани с рекурентната зависимост

$$\begin{aligned}2(n+1)(n+\alpha+\beta+1)(2n+\alpha+\beta)P_{n+1}^{(\alpha,\beta)}(x)=\\ =(2n+\alpha+\beta+1)[(2n+\alpha+\beta+2)(2n+\alpha+\beta)x+\alpha^2-\beta^2]P_n^{(\alpha,\beta)}(x)-\\ -2(n+\alpha)(n+\beta)(2n+\alpha+\beta+2)P_{n-1}^{(\alpha,\beta)}(x).\end{aligned}$$

Упътване. Използувайте резултатите от зад. 5 и зад. 14.

16. Докажете, че полиномът на Якоби $P_n^{(\alpha,\beta)}(x)$ удовлетворява диференциалното уравнение

$$(1-x^2)y''+[\beta-\alpha-(\alpha+\beta+2)x]y'+n(\alpha+\beta+n+1)y=0.$$

Решение. За функцията $u=(1-x)^{\alpha+n}(1+x)^{\beta+n}$ чрез диференциране получаваме

$$(1-x^2)u'+[(\alpha+\beta+2n)x+(\beta-\alpha)]u=0.$$

Като приложим формулата на Лайбниц за $(n+1)$-вата производна, от последното равенство получаваме

$$(1-x^2)v''+[(\alpha+\beta-2)x+\beta-\alpha]v'+(n+1)(\alpha+\beta+2n)v=0,$$

където $v=v(x)=u^{(n)}(x)$. Като положим $v=(1-x)^{\alpha}(1+x)^{\beta}$, горното уравнение приема вида

$$(1-x^2)y''+[\beta-\alpha-(\alpha+\beta+2)x]y'+n(\alpha+\beta+n+1)y=0.$$

С това твърдението е доказано.

17. Покажете, че

$$T_n(x)=\cos n\theta \text{ и } U_n(x)=\frac{\sin(n+1)\theta}{\sin\theta},$$

където $\theta=\arccos x$ са полиноми на x от степен n. Полиномите $T_n(x)$ и $U_n(x)$ се наричат *полиноми на Чебишев* съответно от първи и втори вид.

Докажете, че полиномите на Чебишев $T_n(x)$ са ортогонални в $(-1, 1)$ спрямо теглото $(1-x^2)^{-\frac{1}{2}}$, а полиномите на Чебишев $U_n(x)$ са ортогонални в същия интервал $(-1, 1)$ спрямо теглото $(1-x^2)^{\frac{1}{2}}$, т. е.

$$\int_{-1}^{1}(1-x^2)^{-\frac{1}{2}}T_n(x)\,T_m(x)\,dx=0,\quad n\neq m,$$

$$\int_{-1}^{1}(1-x^2)^{\frac{1}{2}}U_n(x)\,U_m(x)\,dx=0,\quad n\neq m.$$

Упътване. В горните два интеграла положете $x=\cos\theta$.

18. Докажете, че полиномите на Чебишев се изразяват чрез полиномите на Якоби по следния начин:

$$T_n(x)=\frac{(2n)!!}{(2n-1)!!}P_n^{\left(-\frac{1}{2},-\frac{1}{2}\right)}(x),$$

$$U_n(x)=\frac{(2n+2)!!}{2(2n+1)!!}P_n^{\left(\frac{1}{2},\frac{1}{2}\right)}(x).$$

Упътване. Използвайте ортогоналността на $T_n(x)$ и $U_n(x)$, определението за полиномите на Якоби и резултата от зад. 1. След като установите, че $T_n(x)=\lambda_n P_n^{\left(-\frac{1}{2},-\frac{1}{2}\right)}(x)$ и $U_n(x)=\mu_n P_n^{\left(\frac{1}{2},\frac{1}{2}\right)}(x)$, определете нормиращите числови множители λ_n и μ_n, като положите например $x=1$. Използвайте още тъждеството в) от зад. 12.

19. Покажете, че:

а) $\int_{-1}^{1} T_n^2(x)(1-x^2)^{-\frac{1}{2}}\,dx = \int_{-1}^{1} U_n^2(x)(1-x^2)^{\frac{1}{2}} = \frac{\pi}{2}$;

б) $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$;

в) $U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$;

г) $T_n(x) = \frac{(-1)^n\sqrt{1-x^2}}{(2n-1)!!}\frac{d^n}{dx^n}[(1-x^2)^{n-\frac{1}{2}}]$;

д) $U_n(x) = \frac{(-1)^n(n+1)}{(2n+1)!!\sqrt{1-x^2}}\frac{d^n}{dx^n}[(1-x^2)^{n+\frac{1}{2}}]$;

е) $(1-x^2)T_n''(x) - xT_n'(x) + n^2T_n(x) = 0$;

ж) $(1-x^2)U_n''(x) - 3xU_n'(x) + n(n+2)U_n(x) = 0$.

20. *Полиномите на Лежандър* $P_n(x)$ се дефинират чрез

$$P_n(x) = \frac{1}{2^n n!}\frac{d^n}{dx^n}[(x^2-1)^n],\ n=0,\ 1,\ 2, \ldots$$

Докажете, че:

а) $P_n(x) = P_n^{(0,0)}(x)$ и $\int_{-1}^{1} P_n(x)P_m(x)\,dx = \begin{cases} 0, & \text{при } m \neq n, \\ \frac{2}{2n-1}, & \text{при } m = n; \end{cases}$

б) $(n+1)P_{n+1}(x) = (2n+1)xP_n(x) - nP_{n-1}(x)$;

в) $(1-x^2)P_n''(x) - 2xP_n'(x) + n(n+1)P_n(x) = 0$;

г) $P_n(-x) = (-1)^n P_n(x)$;

д) $P_{n+1}'(x) - P_{n-1}'(x) = (2n+1)P_n(x)$;

е) $(1-x^2)P_n'(x) = nP_{n-1}(x) - nxP_n(x)$;

ж) $(1-x)^n P_n\left(\frac{1+x}{1-x}\right) = 1 + \binom{n}{1}^2 x + \binom{n}{2}^2 x^2 + \ldots + \binom{n}{n-1}^2 x^{n-1} + x^n$.

21. *Полиномите на Лагер* $L_n^{(\alpha)}(x)$ се дефинират чрез формулата

$$L_n^{(\alpha)}(x) = \frac{1}{n!}e^x x^{-\alpha}\frac{d^n}{dx^n}(x^{n+\alpha}e^{-x}),\ \alpha > -1,\ n=0,\ 1,\ 2, \ldots$$

Докажете, че полиномите на Лагер са ортогонални в интервала $(0,\infty)$ спрямо теглото $p(x) = x^\alpha e^{-x}$, т. е.

$$\int_0^\infty x^\alpha e^{-x} L_n^{(\alpha)}(x)\, L_m^{(\alpha)}(x)\,dx = 0, \text{ при } n \neq m.$$

22. Докажете следните свойства на полиномите на Лагер $L_n^{(\alpha)}(x)$:

а) $L_n^{(\alpha)}(x) = \sum_{\nu=0}^{n} \frac{(-1)^\nu}{\nu!}\binom{n+\alpha}{n-\nu}x^\nu$;

б) $k_n = \frac{(-1)^n}{n!}$, $k_n' = \frac{(-1)^{n-1}}{(n-1)!}(n+\alpha)$, където k_n и k_n' са коефициентите пред x^n и x^{n-1} в $L_n^{(\alpha)}(x)$;

в) $\int_0^\infty x^\alpha e^{-x}[L_n^{(\alpha)}(x)]^2\, dx = \binom{n+\alpha}{n}\Gamma(\alpha+1)$;

г) $(n+1)L_{n+1}^{(\alpha)}(x) = (-x+2n+\alpha+1)L_n^{(\alpha)}(x) - (n+\alpha)\, L_{n-1}^{(\alpha)}(x)$;

д) $x\frac{d^2}{dx^2}L_n^{(\alpha)}(x) + (\alpha+1-x)\,\frac{d}{dx}L_n^{(\alpha)}(x) + n\, L_n^{(\alpha)}(x) = 0$.

23. *Полиномите на Ермит* $H_n(x)$ се дефинират чрез формулата

$$H_n(x) = (-1)^n e^{x^2}\frac{d^n}{dx^n}(e^{-x^2}),\quad n=0,\ 1,\ 2,\dots$$

Докажете, че полиномите $H_n(x)$ са ортогонални в $(-\infty,\infty)$ спрямо теглото e^{-x^2}, т. е.

$$\int_{-\infty}^{+\infty} e^{-x^2}H_n(x)H_m(x)dx = 0,\ \text{при}\ n \neq m.$$

24. Докажете следните свойства на полиномите $H_n(x)$:

а) $H_n(x) = \sum_{\nu=0}^{[n:2]} \frac{(-1)^\nu}{\nu!}\frac{(2x)^{n-2\nu}}{(n-2\nu)!}$;

б) $A_n = \int_{-\infty}^{\infty} e^{-x^2}H_n^2(x)dx = 2^n n!\int_{-\infty}^{\infty} e^{-x^2}\, dx = 2^n n!\sqrt{\pi}$;

в) $H_{n+1}(x) = 2\, xH_n(x) - 2nH_{n-1}(x)$;

г) $H_n'(x) = 2nH_{n-1}(x)$;

д) $H_n''(x) - 2xH_n'(x) + 2(2n+1)\, H_n(x) = 0$.

25. Покажете, че полиномите на Чебишев, Лежандър, Лагер и Ермит могат съответно да се дефинират чрез следните производящи функции:

$$\frac{1-z^2}{1-2xz+z^2}=1+2\sum_{n=1}^{\infty}T_n(x)z^n,\quad \frac{1}{1-2xz+z^2}=\sum_{n=0}^{\infty}U_n(x)z^n,$$

$$\frac{1}{\sqrt{1-2xz+z^2}}=\sum_{n=0}^{\infty}P_n(x)z^n,\quad \frac{e^{-\frac{xz}{1-z}}}{(1-z)^{\alpha+1}}=\sum_{n=0}^{\infty}L_n^{(\alpha)}(x)z^n.$$

$$e^{-z^2+2zx}=\sum_{n=0}^{\infty}\frac{1}{n!}H_n(x)z^n.$$

26. Покажете, че за полиномите на Чебишев $T_n(x)$ и $U_n(x)$ са в сила неравенствата

$$|T_n(x)|\leq 1,\quad |U_n(x)|\leq n+1$$

при произволно x от интервала $[-1, 1]$. При първото неравенство се достига знакът за равенство само за нулите на $U_{n-1}(x)$ и за $x=\pm 1$. При второто неравенство знакът за равенство се достига само при $x=\pm 1$.

Решение. Като положим $x=\cos\theta$, се убеждаваме, че първото неравенство се свежда до очевидното неравенство $|\cos n\theta|\leq 1$. Знакът за равенството се достига само когато $n\theta$ е кратно на π. Второто неравенство следва директно от

$$U_n(x)=\frac{\sin(n+1)\theta}{\sin\theta}=\cos n\theta+\cos\theta\frac{\sin n\theta}{\sin\theta}$$

и от неравенствата

$$|\cos n\theta|\leq 1,\quad \left|\frac{\sin n\theta}{\sin\theta}\right|\leq n.$$

Знакът за равенство ще се достига само когато $|\cos\theta|=1$, т. е. $\theta=0$ или $\theta=\pi$.

27. Нека $P(x)$ е полином от степен $\leq n-1$ и $x_1, x_2,\dots, x_n$ да означават нулите на чебишевия полином $T_n(x)$. Докажете, че

$$P(x)=\frac{1}{n}\sum_{i=1}^{n}(-1)^{i-1}\sqrt{1-x_i^2}\,P(x_i)\,\frac{T_n(x)}{x-x_i}.$$

Упътване. Използувайте интерполационната формула на Лагранж

$$P(x)=\sum_{\nu=1}^{n}\frac{P(x_\nu)f(x)}{f'(x_\nu)(x-x_\nu)},\quad f(x)=(x-x_1)(x-x_2)\dots(x-x_n)$$

и че за нулите x_i на $T_n(x)$ имаме

$$x_i=\cos(2i-1),\ T_n'(x_i)=(-1)^{i-1}\frac{n}{\sqrt{1-x_i^2}},\quad i=1, 2,\dots, n.$$

28. Нека $P(x)$ е полином от степен $\leq n-1$. Докажете, че

$$P(x)=\frac{1}{n+1}\sum_{\nu=1}^{n}(-1)^{\nu-1}(1-x_\nu^2)P(x_\nu)\frac{U_n(x)}{x-x_\nu},$$

където $x_1, x_2, \ldots, x_n$ са нулите на чебишевия полином от втори вид $U_n(x)$.

Упътване. Както и в предната задача, използувайте интерполационната формула на Лагранж и че за нулите x_ν на $U_n(x)$ имаме

$$x_\nu=\cos\frac{\nu\pi}{n+1},\quad U_n'(x_\nu)=(-1)^{\nu-1}\frac{n+1}{1-x_\nu^2},\quad \nu=1, 2, \ldots, n.$$

29. Нека $P(x)$ е полином от степен $\leq n$. Докажете, че

$$P(x)=\frac{1}{2n}U_{n-1}(x)[P(1)(x+1)+(-1)^nP(-1)(x-1)]+$$

$$+\frac{1}{n}\sum_{\nu=1}^{n-1}(-1)^\nu P(x_\nu)\frac{U_{n-1}(x)(x^2-1)}{x-x_\nu},$$

където $x_1, x_2, \ldots, x_{n-1}$ са нулите на $U_{n-1}(x)$.

Упътване. Използувайте интерполационната формула на Лагранж

$$P(x)=\sum_{\nu=0}^{n}\frac{P(x_\nu)f(x)}{f'(x_\nu)(x-x_\nu)},\quad f(x)=(x-x_0)(x-x_1)\ldots(x-x_n),$$

където $x_\nu=\cos\nu\frac{\pi}{n}$, $\nu=1, 2, \ldots, n-1$, $x_0=+1$, $x_n=-1$. Като положите $f(x)=(x^2-1)U_{n-1}(x)$, използувайте още равенствата

$$f'(x_\nu)=(x_\nu^2-1)U_{n-1}'(x_\nu)=(-1)^\nu n,\quad \nu=1, 2, \ldots, n-1,$$

$$f'(1)=2U_{n-1}(1)=2n,\quad f'(-1)=-2U_{n-1}(-1)=(-1)^n 2n.$$

30. Нека $P(x)=a_0x^{n-1}+\ldots+a_{n-1}$ е полином от степен $n-1$ и да е в сила неравенството

$$\sqrt{1-x^2}\,|P(x)|\leq 1,$$

за всяко x от интервала $[-1, 1]$. Докажете, че $|a_0|\leq 2^{n-1}$. Знакът за равенство се достига само когато $P(x)=\gamma\, U_{n-1}(x)$, $|\gamma|=1$.

Решение. Съгласно тъждеството от зад. 27 ще имаме

$$a_0=\frac{1}{n}2^{n-1}\sum_{k=1}^{n}(-1)^{k-1}\sqrt{1-x_k^2}\;P(x_k),$$

откъдето непосредствено следва, че $|a_0|\leq\frac{1}{n}\cdot 2^{n-1}\cdot n=2^{n-1}$. Равенството е възможно само тогава, когато

$$\sqrt{1-x_k^2}\,P(x_k)=(-1)^{k-1}\gamma,\ |\gamma|=1,\ k=1,\ 2,\ldots,n.$$

При горните условия полиномът $P(x)$ е еднозначно определен, но на същите условия отговаря и полиномът $\gamma\,U_{n-1}(x)$. Ясно е тогава, че ще имаме $P(x)=\gamma U_{n-1}(x)$.

31. Нека $P(x)$ е полином от n-та степен със старши коефициент единица. Докажете, че максимумът на $|P(x)|$ в интервала $[-1,1]$ не е по-малък от 2^{1-n}. Ако $|P(x)|=2^{1-n}$ за всяко x от интервала $[-1,1]$, то $P(x)=\gamma 2^{1-n}T_n(x)$, където числото γ удовлетворява условието $|\gamma|=1$.

Решение. Съгласно тъждеството от зад. 29 ще имаме

$$1=a_0=\frac{2^{n-1}}{n}\sum_{\nu=1}^{n}(-1)^{\nu}P(x_\nu)+\frac{2^{n-2}}{n}[P(1)+(-1)^nP(-1)].$$

Тогава, като положим $M=\max|P(x)|$, $-1\leq x\leq 1$, ще получим

$$1\leq M\left[\frac{2^{n-2}}{n}\cdot 2+\frac{2^{n-1}}{n}\cdot(n-1)\right]=M\cdot 2^{n-1},$$

откъдето

$$M\geq 2^{1-n}.$$

Равенство ще имаме само когато

$$P(1)=2^{1-n}\gamma,\ P(-1)=(-1)^n2^{1-n}\gamma,$$

$$P(x_\nu)=(-1)^\nu 2^{1-n}\gamma,\ \nu=1,\ 2,\ldots,n-1,\ |\gamma|=1.$$

При горните условия полиномът $P(x)$ е определен еднозначно. Понеже на същите условия отговаря и полиномът $2^{1-n}\gamma T_n(x)$, то

$$P(x)=\gamma\,2^{1-n}T_n(x).$$

И така от всички полиноми от степен n и със старши коефициент единица, най-малко се отклонява от нулата в интервала $[-1,1]$ полиномът на Чебишев $2^{1-n}T_n(x)$ и това е свойство, което напълно характеризира чебишевите полиноми.

32. Нека $P(x)$ е полином от степен $\leq n-1$, такъв че в интервала $-1\leq x\leq 1$ да е изпълнено неравенството

$$\sqrt{1-x^2}\,|P(x)|\leq 1.$$

Докажете, че за всяко x от същия интервал $[-1,1]$ имаме

$$|P(x)|\leq n.$$

При някое $x\in[-1,1]$ може да се достигне знак за равенство само когато

$$P(x)=\gamma U_{n-1}(x),\ |\gamma|=1$$

и $x=1$ или $x=-1$.

Упътване. Използувайте резултатите от зад. 26 и зад. 27.

33. Нека

$$S(\theta)=b_1 \sin\theta+b_2 \sin 2\theta+\ldots+b_n \sin n\theta$$

е произволен синусов полином от n-ти ред, за който $|S(\theta)|\leq 1$ при всяко реално θ. Докажете, че

$$\left|\frac{S(\theta)}{\sin n\theta}\right|\leq n.$$

Знакът за равенство се достига само когато

$$S(\theta)=\gamma \sin n\theta,\ |\gamma|=1$$

и $\theta=0$.

Упътване. Приложете резултата от зад. 30 за полинома

$$P(x)=P(\cos\theta)=\frac{S(\theta)}{\sin\theta}.$$

34. Нека тригонометричният полином $g(\theta)=\lambda_0+\lambda_1 \cos\theta+\mu_1 \sin\theta+\lambda_2 \cos 2\theta+\mu_2 \sin 2\theta+\ldots+\lambda_n \cos n\theta+\mu_n \sin n\theta$ удовлетворява неравенството $|g(\theta)|\leq 1$ за всяко реално θ. Докажете, че

$$|g'(\theta)|\leq n.$$

(*Неравенство на Н. С. Бернщайн.*)

Упътване. Приложете резултата от предната задача за синусовия полином

$$S(\theta)=\frac{1}{2}[g(\theta_0+\theta)-g(\theta_0-\theta)],$$

където θ_0 е произволно фиксирано реално число, като положите $\theta=0$.

35. Нека $P_1(x)$ е полином от степен n, такъв че за всяко x от интервала $[-1, 1]$ да е в сила неравенството

$$|P_1(x)|\leq 1.$$

Докажете, че

$$|P_1'(x)|\leq n^2.$$

Знакът за равенство може да се достига само при

$$|P_1'(x)|\leq n^2.$$

(*Неравенство на А. Марков.*)

Упътване. Приложете резултата от предната задача за полинома $g(\theta)=P_1(\cos\theta)$ и зад. 32, при което вместо $P(x)$ (в означенията на зад. 32) разгледате полинома $\frac{1}{n}P_1(\cos\theta)$.

36. Нека $P_n(x)$ е n-тият полином на Лежандър. Докажете, че $P_n(\cos\theta)$ е косинусов полином с неотрицателни коефициенти.

Решение. Съгласно зад. 25 имаме

$$\frac{1}{\sqrt{1-2xz+z^2}}=\sum_{n=0}^{\infty}P_n(x)z^n.$$

Като положим

$$a=\cos\theta+i\sin\theta,$$

ще можем да пишем

$$\frac{1}{\sqrt{1-2\cos\theta z+z^2}}=\frac{1}{\sqrt{1-az}}\cdot\frac{1}{\sqrt{1-a^{-1}z}}=$$

$$=\left(\sum_{k=0}^{\infty}\frac{1.3\ldots(2k-1)}{2.4\ldots2k}a^kz^k\right)\left(\sum_{l=0}^{\infty}\frac{1.3\ldots(2l-1)}{2.4\ldots2l}a^{-l}z^l\right).$$

Коефициентът пред z^n дава $P_n(x)$, $x=\cos\theta$:

$P_n(\cos\theta)=g_0g_n\cos n\theta+g_1g_{n-1}\cos(n-2)\theta+g_2g_{n-2}\cos(n-4)\theta+\ldots+g_ng_0\cos n\theta$,

където

$$g_0=1,\ g_n=\frac{1.3\ldots(2n-1)}{2.4\ldots2n}>0,\ n=1,2,3,\ldots$$

37. Докажете, че за n-тия полином на Лежандър $P_n(x)$ е в сила неравенството

$$|P_n(x)|\leqq 1$$

за всяко $x\in[-1,1]$, като знакът за равенство се достига при $n>0$. само за $x=-1$ и $x=1$.

Упътване. Използувайте резултата от предната задача и равенството $P_n(1)=1$.

38. Нека $P(x)$ е произволен полином от степен n с реални коефициенти, така че

$$\int_{-1}^{1}P^2(x)\,dx=1.$$

Докажете, че че всяко $x\in[-1,1]$ е в сила неравенството

$$P(x)\leqq\frac{n+1}{\sqrt{2}}.$$

Изследвайте кога се достига знакът за равенство.

Решение. Като развием полинома $P(x)$ по полиномите $P_n(x)$ на Лежандър, ще имаме

$$P(x)=\sum_{\nu=0}^{n}t_\nu\sqrt{\frac{2\nu+1}{2}}P_\nu(x),\quad\int_{-1}^{1}P^2(x)dx=\sum_{\nu=0}^{n}t_\nu^2=1.$$

От неравенството на Коши—Буняковски следва:

$$P^2(x) \leq \sum_{\nu=0}^{n} t_\nu^2 \sum_{\nu=0}^{n} \frac{2\nu+1}{2} P_\nu^2(x) = \sum_{\nu=0}^{n} \frac{2\nu+1}{2} P_\nu^2(x),$$

като равенство при дадено $x=x_0$ се достига само когато

$$t_\nu = t\sqrt{\frac{2\nu+1}{2}} P_\nu(x_0), \quad \nu=0, 1, 2, \ldots, n,$$

където t се определя с условието $\sum_{\nu=0}^{n} t_\nu^2 = 1$. Като вземем пред вид неравенството $|P_\nu(x)| \leq 1$ (вж. зад. 37), получаваме

$$P^2(x) \leq \sum_{\nu=0}^{n} \frac{2\nu+1}{2} = \frac{(n+1)^2}{2}.$$

Ясно е, че равенството се достига само при $x = \pm 1$ и тогава $t = \pm \frac{\sqrt{2}}{n+1}$.

39. Нека $F(x)$ е реален полином от степен $2n-1>1$ или $2n-2>0$, такъв че

$$\int_a^b F(x)\, p(x)\, dx = 0, \tag{1}$$

където $p(x)$ е дадена функция на тегло в интервала (a, b) и $P_n(x)$ са съответните ортогонални полиноми спрямо теглото $p(x)$. Докажете, че полиномът $F(x)$ има поне една нечетнократна нула в интервала между най-малката и най-голямата нула на $P_n(x)$, като при това този интервал е минимален (*теорема на Л. Чакалов*).

Решение. Нека $x_1 < x_2 < \ldots < x_n$ да означават нулите на полинома $P_n(x)$. Съгласно квадратурната формула на Гаус (вж. зад. 10), равенството (1) може да се запише във вида

$$\int_a^b (F(x)\, p(x)\, dx = H_1 F(x_1) + H_2 F(x_2) + \ldots + H_n F(x_n) = 0. \tag{2}$$

Тук $H_1, H_2, \ldots, H_n$ са положителни числа (коефициенти на Кристофел), независещи от полинома $F(x)$. Ясно е тогава, че поне две числа $F(x_k)$ и $F(x_{k+1})$ $(1 \leq k \leq n-1)$ са с противоположни знаци или всичките са равни на нула. С това първата част на теоремата е доказана.

Ще докажем минималността на интервала (x_1, x_n) най-напред за полиномите $F(x)$ от степен $2n-1$. За целта да разгледаме полинома

$$F_1(x) = (x-\xi)\left[\frac{P_n(x)}{(x-x_1)^2} + \lambda\right], \tag{3}$$

където ξ е произволно число, подчинено на условието $x_1<\xi<\alpha$, $\alpha=\frac{g_1}{g_0}$ е нулата на ортогоналния полином $P_1(x)=g_0x-g_1$ и λ е константа, определена от условието

$$\int_a^b p(x)F_1(x)\,dx=0. \tag{4}$$

Като запишем разликата $x-\xi$ във вида $x-\xi=(x-x_1)+(x_1-\xi)$ и вземем пред вид, че

$$\int_a^b (x-x_1)\frac{P_n^2(x)}{(x-x_1)^2}p(x)dx=\int_a^b P_n(x)\frac{P_n(x)}{x-x_1}p(x)\,dx=0\,,$$

се убеждаваме, че равенството (4) е равносилно на

$$A+\lambda B=0.$$

където

$$A=\int_a^b (x_1-\xi)\frac{P_n^2(x)}{(x-x_1)^2}p(x)\,dx,\quad B=\int_a^b (x-\xi)\,p(x)dx=g_1-\xi g_0=g_0(\alpha-\xi);$$

Оттук, понеже $A<0$ и $B>0$, за λ получаваме положителна стойност. Следователно полиномът (3) има само един корен $x=\xi$ в интервала (x_1, x_n), който е еднократен. Понеже ξ може да се вземе произволно близко до x_1, то следва, че в интервала (x_1, x_n) долната граница x_1 не може да се увеличи. Аналогично се доказва, че горната граница x_n не може да се намали. Случаят на полиноми $F(x)$ от степен $2n-2$ е по-сложен. Да предположим отначало, че $n>2$ и с x_1', x_2' да означим нулите на ортогоналния полином $P_2(x)$, а с ξ, η и λ — три реални числа, като числото ξ е подчинено на условието $x_1<\xi<x_1'$. При тези означения да разгледаме полинома

$$F_2(x)=(x-\xi)\,(x-\eta)\left[\frac{P_n^2(x)}{(x-x_1)^2\,(x-x_n)^2}+\lambda\right], \tag{5}$$

за който предполагаме, че

$$\int_a^b F_2(x)\,p(x)\,dx=0,$$

Последното равенство, което налага известна връзка между въведените параметри може да се запише още така:

$$C(\eta)-\lambda D(\eta)=0, \tag{6}$$

където

$$C(\eta)=\int_a^b (x-\xi)\,(x-\eta)\,\frac{P_n^2(x)}{(x-x_1)^2\,(x-x_n^2)}\,p(x)\,dx,$$

$$D(\eta)=\int_a^b (x-\xi)\,(x-\eta)\,p(x)\,dx=\xi\,c_1-c_2+\eta\,(c_1-\xi\,c_0).$$

Тук коефициентът $c_1-\xi c_0$ на η е положителен, понеже $c_1-\xi c_0=c_0(\alpha-\xi)$ и $\xi<x_1'<\alpha$. Изразът $C(\eta)$ е непрекъсната функция на η. Съгласно квадратурната формула на Гаус при $\eta=x_n$ получаваме

$$C(x_n)=A_1(x_1-\xi)(x_1-x_n)\frac{P'^2_n(x)}{(x_1-x_n)^2}$$

и следователно $C(x_n)>0$. Ясно е тогава, че за достатъчно близки до x_n стойности на η също ще имаме $C(\eta)>0$. По подобен начин се убеждаваме, че $D(\eta)>0$ при $\eta>x_2'$, като за целта вземем пред вид, че полиномът $h(x)=(x-\xi)(\eta-x)$ е положителен в (x_1', x_2') и приложим за този полином квадратурната формула на Гаус. При такъв избор на η от (6) получаваме за λ положителна стойност. Тогава полиномът $F_2(x)$ от (5) ще има само една нула $x=\xi$, която е проста и може да бъде избрана произволно близко до x_1. С това е доказано, че долната граница x_1 не може да се увеличи. Аналогично се доказва, че горната граница x_n не може да се намали. По такъв начин е доказана минималността на интервала (x_1, x_n) и за полиномите $F(x)$ от степен $2n-2$ при $n>2$. Случаят $n=2$ се разглежда непосредствено. Тогава полиномът $F(x)$ е от втора степен и като удовлетворяващ условието (I) ще има реални нули, т. е.

$$F(x)=a(x-\alpha)(x-\beta),$$

където α, β са реални числа и поне едно от тях, например α, лежи в интервала, определен от нулите x_1', x_2' на $P_2(x)$. От квадратурната формула на Гаус получаваме

$$A_1'\frac{x_1'-\alpha}{x_2'-\alpha}+A_2'\frac{x_2'-\beta}{x_1'-\beta}=0,$$

където A_1' и A_2' са положителни числа. Оттук следва, че $\frac{x_2'-\beta}{x_1'-\beta}<0$, т. е. числото β лежи извън интервала $[x_1', x_2']$. При това очевидно е, че α може да се избере произволно близко както до x_1', така и до x_2'.

40. Теоремата за крайните нараствания може да се прецизира за полиноми по следния начин. Нека $f(x)$ е реален полином от степен $2n>2$ и α е най-голямата нула на полинома на Лежандър $P_n(x)$; тогава ще съществува число ξ в интервала

$$\left[\frac{1}{2}(a+b)-\frac{1}{2}(b-a)\alpha, \frac{1}{2}(a+b)+\frac{1}{2}(b-a)\alpha\right], a<b,$$

така че да бъде в сила равенството

$$f(b)-f(a)=(b-a)f'(\xi).$$

Числото α не може да се замени с по-малко. Същото твърдение остава в сила и за реалните полиноми от степен $2n-1>0$ (*Л. Чакалов*).

Упътване. Без ограничение на общността може да се предполага, че $f(a)=f(b)$ и $a=-1$, $b=1$. Приложете резултата от предната теорема на Л. Чакалов (вж. зад. 39) за $F(x)=f'(x)$ и $p(x)=1$.

ГЛАВА IX

ПОЛИНОМИ НА НЯКОЛКО ПРОМЕНЛИВИ. СИМЕТРИЧНИ ПОЛИНОМИ

§ 1. ПРЪСТЕН ОТ ПОЛИНОМИ НА n ПРОМЕНЛИВИ. СИМЕТРИЧНИ ПОЛИНОМИ

Нека P е дадено поле. Символ от вида

$$(1)\qquad ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n},$$

където $a\in P$ и $\alpha_1, \alpha_2, \dots, \alpha_n$ са цели неотрицателни числа, се нарича *едночлен* на променливите $x_1, x_2, \dots, x_n$. Елементът $a\in P$ се нарича *коефициент* на едночлена (1). Два едночлена $u=ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ и $v=bx_1^{\beta_1}x_2^{\beta_2}\dots x_n^{\beta_n}$ се умножават по правилото

$$uv=(ab)x_1^{\alpha_1+\beta_1}x_2^{\alpha_2+\beta_2}\dots x_n^{\alpha_n+\beta_n}.$$

Два едночлена $ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ и $a'x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$, които могат да се различават само по коефициентите си, се наричат *подобни* и под сбор на тези едночлени се разбира подобният на всеки един от тях едночлен:

$$ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}+a'x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}=(a+a')x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}.$$

При това казваме, че сме извършили *приведение* при събирането на двата едночлена. По анологичен начин извършваме приведение и при събиране на повече подобни едночлени.

Определение. Под *полином на променливите* $x_1, x_2, \dots, x_n$ *над полето* P разбираме крайна сума на едночлени от вида (1).

След извършване на приведения полиномът еднозначно (с точност до реда на събираемите) се представя като сбор от неподобни едночлени. В такъв случай казваме, че полиномът е представен в *каноничен вид (канонична форма)*. Коефициентите на едночлените от каноничната форма на полинома се наричат *коефициенти* на дадения полином.

Под *степен на едночлена* (1) при $a\neq 0$ се разбира сборът $\alpha_1+\alpha_2+\dots+\alpha_n$ на показателите, с които участват променливите $x_1, x_2, \dots, x_n$ в дадения едночлен. Под *степен на полином* се разбира най-голямата от степените на едночлените от каноничната форма на полинома.

Два полинома наричаме *равни*, когато имат една и съща канонична форма. Очевидно равните полиноми имат равни степени.

Различните от нула елементи на полето P могат да се разглеждат като полиноми от нулева степен.

Всеки полином на n променливи може да се разглежда като полином на всяка една от променливите с коефициенти полиноми на останалите $n-1$ променливи. Като вземем пред вид това обстоятелство, можем да говорим за *степен на полинома спрямо всяка една от променливите*. Например полиномът

$$f(x_1, x_2, x_3)=2x_1\, x_2\, x_3^5+x_1^6\, x_2^2-3x_1^3\, x_2^4\, x_3^3+4x_3^2-5$$

е от 10-а степен, като спрямо отделните променливи x_1, x_2, x_3 е съответно от степен 6, 4, 5.

Определение. Под *сбор* на два полинома $f=f(x_1, x_2, \ldots, x_n)$ и $g=g(x_1, x_2, \ldots, x_n)$ разбираме полинома $f+g$, коефициентите на който са равни на сбора от съответните коефициенти на полиномите f и g. (Разбира се, че ако даден едночлен участвува в каноничната форма на един от полиномите f и g, в другия полином ще считаме, че се съдържа едночлен, подобен на дадения, но с коефициент 0.)

Определение. Под *произведение* на два полинома $f=f(x_1, x_2, \ldots$ $\ldots, x_n)$ и $g=g(x_1, x_2, \ldots, x_n)$ разбираме полинома fg, който се получава, като умножим всеки едночлен на f с всеки едночлен на g, съберем получените произведения и извършим приведение на подобните събираеми.

При така дадените определения за сбор и произведение множеството от всички полиноми на променливите $x_1, x_2, \ldots, x_n$ с коефициенти от полето P представлява комутативен пръстен. Този пръстен ще означаваме с $P[x_1, x_2, \ldots, x_n]$.

Полиномите, на които всичките коефициенти са равни на нула, се отъждествяват с нулевия елемент на полето P, който същевременно представлява нулевият елемент на пръстена $P[x_1, x_2, \ldots$ $\ldots, x_n)$ и се нарича нулев полином. Ако f е произволен полином, противоположният му $-f$ е с коефициенти, съответно противоположни на коефициентите на f. Имаме $-f=(-1)\, f$ и $f+(-f)=0$.

Нулевият полином е единственият полином, на който не се приписва определена степен.

Единицата $1 \in P$ на полето P играе ролята на единичен елемент и в пръстена от полиноми над P.

Лексикографска наредба в пръстена на полиноми на n променливи. Нека $u=ax_1^{\alpha_1}\, x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ и $v=bx_1^{\beta_1}\, x_2^{\beta_2} \ldots x_n^{\beta_n}$ са два неподобни едночлена от пръстена $P[x_1, x_2, \ldots, x_n]$. Ще считаме, че u предхожда v, когато

$$\alpha_1=\beta_1,\ \alpha_2=\beta_2, \ldots,\ \alpha_{s-1}=\beta_{s-1},\ \alpha_s>\beta_s$$

при някое $1 \leq s \leq n$.

Например едночленът $u=3x_1^2\, x_2^3\, x_3^2\, x_4^4$ предхожда едночлена $v=4x_1^2\, x_2^3\, x_3\, x_4^7$.

Така в множеството на едночлените можем да дефинираме наредба, която се нарича *лексикографска*.

Лесно се вижда, че всеки полином може да се нареди еднозначно лексикографски, като се спазва принципът, от два едночлена да се записва вляво онзи, който предхожда другия. Едночленът, който при лексикографския запис на полинома е на първо място, се нарича *главен (най-висок, най-виси)* член на дадения полином.

Да подредим лексикографски например членовете на полинома

$$f=3x_1^2x_2x_4+7x_1^2x_2x_3x_4-2x_1^2x_3x_4+x_1^3x_2x_3^3+$$
$$+x_1^3x_2^2x_3+x_1x_2^2x_3x_4.$$

Имаме

$$f=x_1^3x_2^2x_3+x_1^3x_2x_3^3+7x_1^2x_2x_3x_4+3x_1^2x_2x_4-2x_1^2x_3x_4+x_1x_2^2x_3x_4.$$

Главният член на този полином е $x_1^3x_2^2x_3$.

Главният член на произведението от два или повече полиноми е произведение от главните членове на отделните множители.

Един полином $f=f(x_1, x_2, \dots, x_n)$ на променливите $x_1, x_2, \dots, x_n$ се нарича *симетричен*, когато не се променя при произволна пермутация на променливите. Най-прости примери за симетрични полиноми ни дават полиномите, които познаваме от формулите на Виет:

$$\sigma_1=x_1+x_2+\dots+x_n,$$
$$\sigma_2=x_1x_2+x_1x_3+\dots+x_{n-1}x_n,$$
$$\sigma_3=x_1x_2x_3+\dots+x_{n-2}x_{n-1}x_n,$$
$$\dots\dots\dots\dots\dots\dots$$
$$\sigma_n=x_1x_2x_3\dots x_n.$$

Тези полиноми се наричат *елементарни симетрични полиноми*. Очевидно всеки полином на елементарните симетрични полиноми е симетричен полином на $x_1, x_2, \dots, x_n$. Твърде важно е, че е вярно и обратното твърдение. По-точно в сила е следната

Основна теорема за симетричните полиноми. Всеки симетричен полином $f=f(x_1, x_2, \dots, x_n)$ на променливите $x_1, x_2, \dots, x_n$ се представя като полином $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ на елементарните симетрични полиноми $\sigma_1, \sigma_2, \dots, \sigma_n$, като при това полиномът $\varphi(t_1, t_2, \dots, t_n)$ е определен еднозначно чрез $f(x_1, x_2, \dots, x_n)$ и коефициентите му се изразяват рационално чрез тези на $f(x_1, x_2, \dots, x_n)$.

За да получим представянето

$$f(x_1, x_2, \dots, x_n)=\varphi(\sigma_1, \sigma_2, \dots, \sigma_n),$$

можем да постъпим по следния начин. Най-напред намираме главния член

$$ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$$

на симетричния полином $f=f(x_1, x_2, \ldots, x_n)$ (лесно се доказва, че $k_1 \geq k_2 \geq \ldots \geq k_n$); след това съставяме разликата

$$f_1=f-a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\ldots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n},$$

която представлява симетричен полином на $x_1, x_2, \ldots, x_n$ с по-нисък главен член от този на f; с полинома f_1 постъпваме по същия начин, както с f, и след краен брой аналогични операции изразяваме накрая полинома f като полином $\varphi(\sigma_1 \sigma_2, \ldots, \sigma_n)$ на $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Пример. Да представим симетричния полином

$$f=x_1^4x_2^2+x_1^4x_3^2+x_1^2x_2^4+x_1^2x_3^4+x_2^4x_3^2+x_2^2x_3^4$$

като полином на елементарните симетрични полиноми $\sigma_1, \sigma_2, \sigma_3$. Ще използуваме указания по-горе начин, като освен това за удобство ще си послужим и с метода на неопределените коефициенти. Знаем, че членовете на полинома $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ се определят чрез главните членове на $f, f_1, f_2, \ldots$. При последователно определяне на главните членове на тези полиноми, както посочихме по-горе, тези главни членове следват в строго низходящ ред по отношение на лексикографската наредба, т. е. главният член на f_1 е по-нисък от главния член $x_1^4 x_2^2$ на f, главния член на f_2 е по-нисък от този на f_1 и т. н. Задачата се свежда до намиране на всички едночлени от вида $Ax_1^{l_1} x_2^{l_2} x_3^{l_3}$, удовлетворяващи следните условия: а) да са по-ниски от главния член $x_1^4 x_2^2$ на дадения полином f; б) за показателите l_1, l_2, l_3 да са в сила неравенствата $l_1 \geq l_2 \geq l_3$; в) понеже даденият полином е хомогенен от 6-а степен, да бъде изпълнено винаги равенството $l_1+l_2+l_3=6$. Записваме само съответните показатели на търсените едночлени и срещу тях — отговарящите им едночлени $\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\sigma_3^{l_3}$:

4 2 0	$\sigma_1^2\sigma_2^2$
4 1 1	$\sigma_1^3\sigma_3$
3 3 0	σ_2^3
3 2 1	$\sigma_1\sigma_2\sigma_3$
2 2 2	σ_3^2.

Оттук виждаме, че полиномът f трябва да се представи във вида

$$f=\sigma_1^2\sigma_2^2+A\sigma_1^3\sigma_3+B\sigma_2^3+C\sigma_1\sigma_2\sigma_3+D\sigma_3^2.$$

Коефициентът пред първия едночлен е равен на коефициента на главния член на дадения полином f, т. е. в случая е 1, а останалите коефициенти A, B, C, D ще намерим чрез заместване на променливите с подходящи стойности. При $x_1=x_2=1$, $x_3=0$ получаваме съответните стойности $f=2$, $\sigma_1=2$, $\sigma_2=1$, $\sigma_3=0$, откъдето намираме $B=-2$. По-нататък да положим например $x_1=x_2=1, x_3=-2$; намираме съответните стойности $f=42$, $\sigma_1=0$, $\sigma_2=-3$, $\sigma_3=-2$, откъдето $D=-3$. След това е удобно да положим например $x_1=x_2=2$, $x_3=-1$, защото тогава за σ_2 ще се получи стойност $\sigma_2=0$ и като заместим в представянето на f чрез $\sigma_1, \sigma_2, \sigma_3$ съответните стойности $f=168$, $\sigma_1=+3$, $\sigma_2=0$, $\sigma_3=-4$, както попреди, получаваме следващия коефициент $A=-2$. Остана да пресметнем коефициента C. Да положим например $x_1=x_2=x_3=1$. За тези стойности на променливите намираме $f=6$, $\sigma_1=3$, $\sigma_2=3$, $\sigma_3=1$, откъдето $6=81+27A+9C+27B+D$, и като вземем пред вид пресметнатите стойности на A, B, D, получаваме окончателно $C=4$. И така:

$$f=\Sigma x_1^4x_2^2=\sigma_1^2\sigma_2^2-2\sigma_1^3\sigma_3-2\sigma_2^3+4\sigma_1\sigma_2\sigma_3-3\sigma_3^2.$$

Тук със $\Sigma x_1^4x_2^2$ сме означили за краткост дадения полином

$$f=x_1^4x_2^2+x_1^4x_3^2+x_1^2x_2^4+x_1^2x_3^4+x_2^4x_3^2+x_2^2x_3^4.$$

(Аналогични кратки означения за хомогенните симетрични полиноми ще използуваме и в някои от следващите примери и задачи. Например основните елементарни симетрични полиноми $\sigma_1, \sigma_2, \ldots$ ще записваме накратко така: $\sigma_1=\Sigma x_1$, $\sigma_2=\Sigma x_1x_2, \ldots$)

Пръстенът $P[x_1, x_2, \ldots, x_n]$ от полиноми на n променливи над полето P е област на цялостност (т. е. комутативен пръстен, без делители на нулата) и следователно може да се разшири до поле от частни. Полето от частни на $P[x_1, x_2, \ldots, x_n]$ ще означаваме с $P(x_1, x_2, \ldots, x_n)$. Неговите елементи се представят като отношения на полиноми от $P[x_1, x_2, \ldots, x_n]$ и затова ще ги наричаме *рационални функции* на променливите $x_1, x_2, \ldots, x_n$ над полето P.

Една рационална функция от полето $P(x_1, x_2, \ldots, x_n)$ ще наричаме *симетрична*, когато не се променя при произволна пермутация на $x_1, x_2, \ldots, x_n$.

Лесно се доказва, че рационалните симетрични функции се представят като частни на симетрични полиноми. От основната теорема за симетричните полиноми следва, че *всяка рационална симетрична функция на променливите $x_1, x_2, \ldots, x_n$ може да се представи като рационална функция на елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$.*

Като следствие от основната теорема за симетричните полиноми и от формулите на Виет се получава следното важно твърдение:

Всяка цяла рационална симетрична функция от корените $\alpha_1, \alpha_2, \ldots, \alpha_n$ на уравнението $x^n+a_1x^{n-1}+\ldots+a_n$ се изразява като цяла рационална функция на коефициентите му $a_1, a_2, \ldots, a_n$.

Като вземем пред вид казаното по-горе за рационалните симетрични функции, можем да изкажем още следното твърдение:

всяка рационална симетрична функция на корените на дадено алгебрично уравнение се изразява рационално чрез коефициентите му.

Формули на Нютон. За симетричните полиноми

$$S_k = x_1^k + x_2^k + \ldots + x_n^k,$$

които се наричат *степенни сборове*, са в сила равенствата

$$(1)\qquad \begin{aligned} &S_1 - \sigma_1 = 0,\\ &S_2 - \sigma_1 S_1 + 2\sigma_2 = 0,\\ &S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 = 0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - \ldots + (-1)^{k-1}\sigma_{k-1} S_1 + (-1)^k k\sigma_k = 0. \end{aligned}$$

В горните формули полагаме $\sigma_k = 0$ при $k > n$.

Ако $x_1, x_2, \ldots, x_n$ са корените на уравнението

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0,$$

формулите (1) на Нютон могат да се запишат във вида

$$\begin{aligned} &S_1 + a_1 = 0,\\ &S_2 + a_1 S_1 + 2a_2 = 0,\\ &S_3 + a_1 S_2 + a_2 S_1 + 3a_3 = 0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &S_k + a_1 S_{k-1} + a_2 S_{k-2} + \ldots + a_{k-1} S_1 + k a_k = 0. \end{aligned}$$

И тук правим аналогична уговорка, че при $k > n$ трябва да считаме $a_k = 0$.

Пример 1. Да пресметнем степенния сбор

$$S_4 = x_1^4 + x_2^4 + x_3^4 + x_4^4,$$

където x_1, x_2, x_3, x_4 са корените на уравнението

$$x^4 + x^3 + 2x^2 - 3x + 4 = 0.$$

По формулите (2) на Нютон получаваме

$$\begin{aligned} &S_1 + a_1 = 0,\\ &S_2 + a_1 S_1 + 2a_2 = 0,\\ &S_3 + a_1 S_2 + a_2 S_1 + 3a_3 = 0,\\ &S_4 + a_1 S_3 + a_2 S_2 + a_3 S_1 + 4a_4 = 0, \end{aligned}$$

т. е.

$$\begin{aligned} &S_1 + 1 = 0.\\ &S_2 + S_1 + 2.2 = 0,\\ &S_3 + S_2 + 2S_1 + 3.(-3) = 0,\\ &S_4 + S_3 + 2S_2 - 3S_1 + 4.4 = 0, \end{aligned}$$

откъдето намираме последователно: $S_1=-1$, $S_2=-3$, $S_3=14$, $S_4=$ $=-27$. И така

$$S_4=x_1^4+x_2^4+x_3^4+x_4^4=-27.$$

Пример 2. Да пресметнем $S_{-3}=x_1^{-3}+x_2^{-3}+x_3^{-3}+x_4^{-3}$, където x_1, x_2, x_3, x_4 са корените на уравнението

$$x^4-3x^2+4x+2=0.$$

Очевидно степенният сбор $S_{-k}=x_1^{-k}+x_2^{-k}+\ldots+x_n^{-k}$ от корените на уравнението $f(x)=0$ съвпада със степенния сбор S_k от корените на реципрочното уравнение $x^n f\left(\frac{1}{x}\right)=0$. В случая реципрочното уравнение е

$$2x^4+4x^3-3x^2+1=0$$

и за съответния степенен сбор S_3 намираме по формулите на Нютон:

$$S_1+2=0,$$
$$S_2+2S_1+2\left(-\frac{3}{2}\right)=0,$$
$$S_3+2S_2-\frac{3}{2}S_1+3.0=0,$$

откъдето $S_3=17$. И така, ако x_1, x_2, x_3, x_4 са корените на даденото уравнение $x^4-3x^2+4x+2=0$, то

$$S_{-3}=x_1^{-3}+x_2^{-3}+x_3^{-3}+x_4^{-3}=17.$$

1. Подредете лексикографски следните полиноми:

а) $F=2x_1x_2^3-3x_1^2x_2+7x_3^4-3x_1^5+4x_2x_3^3+x_2^2-x_1+x_3+2$;

б) $F=x_1+x_2^2+x_3^3-2x_1x_2x_3+4x_2^2x_3^2-5x_2^3+8x_1^2+3$;

в) $F=x_1x_2x_3-3x_1^2x_4-3x_3^2+4x_2x_4+7x_1x_5-12x_6$;

г) $F=x_1^5-5x_1^3x_2+5x_2+5x_1x_2^2+3x_1^2x_3-5x_2x_3+x_1x_4-x_5$;

д) $F=3x_6-5x_1x_5+3x_2x_4-3x_3^2+2x_1^2x_4-x_1x_2x_3+x_2^3$.

Отг. а) $F=-3x_1^5-x_1^2x_2+2x_1x_2^3-x_1+x_2^2+4x_2x_3^3+7x_3^4+x_3+2$;

б) $F=8x_1^2-2x_1x_2x_3+x_1-5x_2^3+4x_2^2x_3^2+x_2^2+x_3^3+3$;

в) $F=-3x_1^2x_4+x_1x_2x_3+7x_1x_5+4x_2x_4-3x_3^2-12x_6$;

г) $F=x_1^5-5x_1^3x_2+3x_1^2x_3+5x_1x_2^2+x_1x_4-5x_2x_3+5x_2-x_5$;

д) $F=2x_1^2x_4-x_1x_2x_3-5x_1x_5+x_2^3+3x_2x_4-3x_3^2+3x_6$.

2. Изразете чрез елементарните симетрични полиноми σ_1, σ_2, σ_3 следните симетрични полиноми:

а) $F=x_1^3+x_2^3+x_3^3-3x_1x_2x_3$;
б) $F=x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_1x_3^2+x_2x_3^2$;
в) $F=x_1^4+x_2^4+x_3^4-2x_1^2x_2^2-2x_1^2x_3^2-2x_2^2x_3^2$;
г) $F=x_1^5x_2^2+x_1^5x_3^2+x_1^2x_2^5+x_2^5x_3^2+x_1^2x_3^5=x_2^2x_3^5$;
д) $F=(x_1+x_2)(x_2+x_3)(x_3+x_1)$;
е) $F=(x_1^2+x_2^2)(x_2^2+x_3^2)(x_3^2+x_1^2)$;
ж) $F=(2x_1-x_2-x_3)(2x_2-x_3-x_1)(2x_3-x_1-x_2)$;
з) $F=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$;
и) $F=(x_1+x_2+1)(x_2+x_3+1)(x_3+x_1+1)$;
к) $F=(x_1+\varepsilon x_2)(x_2+\varepsilon x_1)(x_2+\varepsilon x_3)(x_3+\varepsilon x_2)(x_1+\varepsilon x_3)(x_3+\varepsilon x_1)$, $\varepsilon^3=1$, $\varepsilon\neq 1$.

Отг. а) $\sigma_1^3-3\sigma_1\sigma_2$
б) $\sigma_1\sigma_2-3\sigma_3$;
в) $\sigma_1^4-4\sigma_1\sigma_2+8\sigma_1\sigma_3$;
г) $\sigma_1^3\sigma_2^2-2\sigma_1^4\sigma_3-3\sigma_1\sigma_2^3+6\sigma_1^2\sigma_2\sigma_3+$
$+\sigma_2^2\sigma_3-7\sigma_1\sigma_3^2$;
д) $\sigma_1\sigma_2-\sigma_3$;
е) $\sigma_1^2\sigma_2^2-2\sigma_1^3\sigma_3-2\sigma_2^3+4\sigma_1\sigma_2\sigma_3-\sigma_3^2$;
ж) $27\sigma_1-9\sigma_1\sigma_2+2\sigma_1^3$;
з) $\sigma_1^2\sigma_2^2-4\sigma_1^3\sigma_3-4\sigma_2^3+18\sigma_1\sigma_2\sigma_3-27\sigma_3^2$;
и) $\sigma_1\sigma_2+\sigma_1^2+2\sigma_1+\sigma_2-\sigma_3+1$
к) $\sigma_1^2\sigma_2^2-3\sigma_1^3\sigma_3-3\sigma_2^3+10\sigma_1\sigma_2\sigma_3-8\sigma_3^2$.

3. Изразете чрез елементарните симетричните полиноми σ_1, σ_2, σ_3, σ_4 следните симетрични полиноми;

а) $F=(x_1+x_2)(x_1+x_3)(x_1+x_4)(x_2+x_3)(x_2+x_4)(x_3+x_4)$;
б) $F=(x_1x_2+x_3x_4)(x_1x_3+x_2x_4)(x_1x_4+x_2x_3)$;
в) $F=(x_1+x_2-x_3-x_4)(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4)$.

Отг. а) $\sigma_1\sigma_2\sigma_3-\sigma_1^2\sigma_4-\sigma_3^2$;
б) $\sigma_1^2\sigma_4+\sigma_3^2-4\sigma_2\sigma_4$;
в) $\sigma_1^3-4\sigma_1\sigma_2+8\sigma_3$.

4. Изразете чрез елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ следните симетрични полиноми:

а) $F=\sum x_1^2$;
б) $F=\sum x_1^3$;
в) $F=\sum x_1^2x_2x_3$;
г) $F=\sum x_1^2x_2^2$;
д) $F=\sum x_1^2x_2^2x_3$;
е) $F=\sum x_1^3x_2^2$;
ж) $F=\sum x_1^5$;
з) $F=\sum x_1^3x_2x_3x_4$
и) $F=\sum x_1^4x_2x_3$;
к) $F=\sum x_1^6$.

Отг. а) $F=\sigma_1^2-2\sigma_2$;
б) $F=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$;
в) $F=\sigma_1\sigma_3-4\sigma_4$;
г) $F=\sigma_2^2-2\sigma_1\sigma_3+2\sigma_4$;

д) $F=\sigma_2\sigma_3-3\sigma_1\sigma_4+5\sigma_5$;

е) $F=\sigma_1\sigma_2^2-2\sigma_1^2\sigma_3-\sigma_2\sigma_3+5\sigma_1\sigma_4-5\sigma_5$;

ж) $F=\sigma_1^5-5\sigma_1^3\sigma_2+5\sigma_1\sigma_2^2+5\sigma_1^2\sigma_3-5\sigma_2\sigma_3-$
$-5\sigma_1\sigma_4+5\sigma_5$;

з) $F=\sigma_1^2\sigma_4-2\sigma_2\sigma_4-\sigma_1\sigma_5+6\sigma_6$;

и) $F=\sigma_1^3\sigma_3-3\sigma_1\sigma_2\sigma_3-\sigma_1^2\sigma_4+3\sigma_3^2+2\sigma_2\sigma_4+$
$+\sigma_1\sigma_5-6\sigma_3$;

к) $F=\sigma_1^6-6\sigma_1^4\sigma_2+9\sigma_1^2\sigma_2^2+6\sigma_1^3\sigma_3-2\sigma_2^3-$
$-12\sigma_1\sigma_2\sigma_3-6\sigma_1^2\sigma_4+3\sigma_3^2+6\sigma_2\sigma_4+6\sigma_1\sigma_5-$
$-6\sigma_6$.

5. Изразете чрез елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ следните симетрични полиноми:

а) $F=(-x_1+x_2+\ldots+x_n)^2+(x_1-x_2+x_3+\ldots+x_n)^2+\ldots+(x_1+x_2+x_3+\ldots-x_n)^2$;

б) $F=(-x_1+x_2+x_3+\ldots+x_n)(x_1-x_2+x_3+\ldots+x_n)\ldots(x_1+x_2+x_3+\ldots-x_n)$; в) $F=\sum\limits_{i>k}(x_i-x_k)^2$; г) $F=\sum\limits_{i>k}(x_i+x_k)^3$; д) $F=\sum\limits_{i>k}(x_i-x_k)^4$; е) $F=\sum\limits_{\substack{i>k\\ i\neq j\ j\neq k}}(x_i+x_k-x_j)^2$.

Отг. а) $F=n\sigma_1^2-8\sigma_2$; б) $F=-\sigma_1^n+4\sigma_1^{n-2}\sigma_2-8\sigma_1^{n-3}\sigma_3+\ldots+(-2)^n\sigma_n$;
в) $F=(n-1)\sigma_1^2-2n\sigma_2$; г) $F=(n-1)\sigma_1^3-3(n-2)\sigma_1\sigma_2+3(n-4)\sigma_3$;
д) $F=(n-1)\sigma_1^4-4n\sigma_1^2\sigma_2+2(n+6)\sigma_2^2-4(n-3)\sigma_1\sigma_3-4n\sigma_4$; е) $F=$
$=\frac{3(n-1)(n-2)}{2}\sigma_1^2-(3n-2)(n-2)\sigma_2$.

6. Изразете чрез елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ симетричния полином

$$F=\sum x_1^2x_2^2\ldots x_k^2.$$

Отг. $F=\sigma_k^2-2\sigma_{k-1}\sigma_{k+1}+2\sigma_{k-2}\sigma_{k+2}-2\sigma_{k-3}\sigma_{k+3}+\ldots$

7. Изразете чрез елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ симетричния полином

$$F=\sum(a_1x_1+a_2x_2+\ldots+a_nx_n)^2,\ a_i\neq a_j \text{ при } i\neq j.$$

Отг. $F=(n-1)!\sum\limits_{i=1}^{n}a_i^2\sigma_i^2-2(n-2)!\left[n\sum\limits_{i=1}^{n}a_i^2-\left(\sum\limits_{i=1}^{n}a_i\right)^2\right]\sigma_2$.

8. Изразете чрез елементарните симетрични полиноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ следните симетрични дроби:

а) $F=\frac{x_1}{x_2}+\frac{x_2}{x_3}+\frac{x_3}{x_1}+\frac{x_2}{x_1}+\frac{x_3}{x_2}+\frac{x_1}{x_3}$;

б) $F=\frac{(x_1-x_2)^2}{x_1+x_2}+\frac{(x_2-x_3)^2}{x_2+x_3}+\frac{(x_3-x_1)^2}{x_3+x_1}$;

в) $F=\left(\frac{x_1}{x_3}+\frac{x_3}{x_2}+\frac{x_2}{x_1}\right)\left(\frac{x_1}{x_2}+\frac{x_2}{x_3}+\frac{x_3}{x_1}\right)$;

г) $F=\frac{(x_1-x_2)^2}{x_1x_2}+\frac{(x_2-x_3)^2}{x_2x_3}+\frac{(x_3-x_1)^2}{x_1x_3}$;

д) $F=\frac{x_1^2}{(1+x_1)}+\frac{x_2^2}{(1+x_2)}+\frac{x_3^2}{(1+x_3)}$;

Отг. а) $F=\frac{\sigma_1\sigma_2-3\sigma_3}{\sigma_3}$; б) $F=\frac{2(\sigma_1^2\sigma_2-3\sigma_1\sigma_3-\sigma_2^2)}{\sigma_1\sigma_2-\sigma_3}$;

в) $F=\frac{\sigma_2^3+\sigma_1^3\sigma_3-6\sigma_1\sigma_2\sigma_3+9\sigma_3^2}{\sigma_3^2}$; г) $F=\frac{\sigma_1\sigma_2}{\sigma_3}-9$;

д) $F=\frac{\sigma_1^2+\sigma_1\sigma_2+\sigma_1\sigma_3-2\sigma_2-3\sigma_3}{1+\sigma_1+\sigma_2+\sigma_3}$.

9. Изразете чрез елементарните симетрични полиноми σ_1, σ_2 σ_3, σ_4 следните симетрични дроби:

а) $F=\frac{x_1x_2}{x_3x_4}+\frac{x_1x_3}{x_2x_4}+\frac{x_1x_4}{x_2x_3}+\frac{x_2x_3}{x_1x_4}+\frac{x_2x_4}{x_1x_3}+\frac{x_3x_4}{x_1x_2}$;

б) $F=\frac{x_1+x_2}{x_3+x_4}+\frac{x_1+x_3}{x_2+x_4}+\frac{x_1+x_4}{x_2+x_3}+\frac{x_2+x_3}{x_1+x_4}+\frac{x_2+x_4}{x_1+x_3}+\frac{x_3+x_4}{x_1+x_2}$.

Отг. а) $E=\frac{\sigma_2^2-2\sigma_1\sigma_3+2\sigma_4}{\sigma_4}$;

б) $F=\frac{\sigma_1^2\sigma_2^2+\sigma_1^3\sigma_3-6\sigma_1\sigma_2\sigma_3+6\sigma_3^2+2\sigma_1^2\sigma_4}{\sigma_1\sigma_2\sigma_3-\sigma_1^2\sigma_4-\sigma_3^2}$.

10. Изразете чрез елементарните симетрични полиноми σ_1, σ_2 $\sigma_3,\ldots,\sigma_n$ следните симетрични дроби:

а) $F=\sum\frac{1}{x_i}$;

б) $F=\sum\frac{1}{x_i^2}$;

в) $F=\sum\limits_{i\neq j}\frac{x_i}{x_j}$;

г) $F=\sum\limits_{i\neq j}\frac{x_i^2}{x_j^2}$;

д) $F=\sum\limits_{i\neq j}\frac{x_i^2}{x_j}$;

е) $F=\sum\limits_{\substack{i\neq j\\ i\neq k\\ j>k}}\frac{x_jx_k}{x_i}$.

Отг. а) $\frac{\sigma_{n-1}}{\sigma_n}$; б) $\frac{\sigma_{n-1}^2-2\sigma_{n-2}\sigma_n}{\sigma_n^2}$; в) $\frac{\sigma_1\sigma_{n-1}-n\sigma_n}{\sigma_n}$;

г) $\frac{\sigma_1^2\sigma_{n-1}^2-2\sigma_2\sigma_{n-1}^2-2\sigma_1^2\sigma_{n-2}\sigma_n+4\sigma_2\sigma_{n-2}\sigma_n-n\sigma_n^2}{\sigma_n^2}$;

д) $\frac{1}{\sigma_n}\left(\sigma_1^2\sigma_{n-1}-2\sigma_2\sigma_{n-1}-\sigma_1\sigma_n\right)$; е) $\frac{1}{\sigma_n}\left[\sigma_2\sigma_{n-1}-(n-1)\sigma_1\sigma_n\right]$.

11. Като използувате формулите на Нютон, изразете чрез елементарните симетрични полиноми следните степенни сборове:

а) $S_2=x_1^2+x_2^2+\ldots+x_n^2$; б) $S_3=x_1^3+x_2^3+\ldots+x_n^3$;

в) $S_4=x_1^4+x_2^4+\ldots+x_n^4$; г) $S_{-2}=\frac{1}{x_1^2}+\frac{1}{x_2^2}+\ldots+\frac{1}{x_n^2}$;

д) $S_{-4}=\frac{1}{x_1^4}+\frac{1}{x_2^4}+\ldots+\frac{1}{x_n^4}$; е) $S_5=x_1^5+x_2^5+\ldots+x_n^5$.

Отг. а) $S_2=\sigma_1^2-2\sigma_2$;

б) $S_3=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$;

в) $S_4=\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2+4\sigma_1\sigma_3-4\sigma_4$;

г) $S_{-2}=\frac{1}{\sigma_n^2}\left(\sigma_{n-1}^2-2\sigma_{n-2}\sigma_n\right)$;

д) $S_{-4}=\frac{1}{\sigma_n^4}\left(\sigma_{n-1}^4-4\sigma_{n-2}\sigma_{n-1}^2\sigma_n+4\sigma_{n-3}\sigma_{n-1}\sigma_n^2+2\sigma_{n-2}^2\sigma_n^2-4\sigma_{n-4}\sigma_n^3\right)$;

е) $S_5=\sigma_1^5-5\sigma_1^3\sigma_2+5\sigma_1\sigma_2^2+5\sigma_1^2\sigma_3-5\sigma_2\sigma_3-5\sigma_1\sigma_4+5\sigma_5$.

12. Като използувате формулите на Нютон, изразете елементарните симетрични полиноми σ_1, σ_2, σ_3, σ_4, σ_5, σ_6 чрез степенните сборове S_1, S_2, S_3, S_4, S_5, S_6.

Отг. $2\sigma_2=S_1^2-S_2$;

$6\sigma_3=S_1^3-3S_1S_2+S_3$;

$24\sigma_4=S_1^4-6S_1^2S_2+8S_1S_3+3S_2^2-6S_4$;

$120\sigma_5=S_1^5-10S_1^3S_2+20S_1^2S_3+15S_1S_2^2-20S_2S_3-30S_1S_4+24S_5$;

$720\sigma_6=S_1^6-15S_1^4S_2+40S_1^3S_3+45S_1^2S_2^2-120S_1S_2S_3-15S_2^3-90S_1^2S_4+40S_3^2+$
$+90S_2S_4+144S_1S_5-120S_6$.

13. Нека $\sigma_1, \sigma_2, \ldots, \sigma_n$ са елементарните симетрични полиноми на променливите $x_1, x_2, \ldots, x_n$. Докажете, че за степенния сбор S_k, $k=1, 2, 3, \ldots$, е в сила равенството

$$S_k=\begin{vmatrix} \sigma_1 & 1 & 0 & \ldots 0 \\ 2\sigma_2 & \sigma_1 & 1 & \ldots 0 \\ \cdot & \cdot & \cdot & \cdot\ \cdot\ \cdot \\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \ldots \sigma_1 \end{vmatrix}.$$

Решение. Към първия стълб на детерминантата в дясната страна на равенството прибавяме всички останали, умножени съответно с $-S_1, S_2, -S_3, \ldots, (-1)^{k-1} S_{k-1}$. Като вземем пред вид формулите на Нютон, получаваме

$$\begin{vmatrix} \sigma_1 & 1 & 0 \ldots 0 \\ 2\sigma_2 & \sigma_1 & 1 \ldots 0 \\ \cdot & \cdot & \cdot \\ (k-1)\,\sigma_{k-1} & \sigma_{k-2} & \ldots 1 \\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} \ldots \sigma_1 \end{vmatrix} = \begin{vmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & \sigma_1 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & & \cdot \\ 0 & \sigma_{k-2} & \sigma_{k-3} & \ldots, & 1 \\ (-1)^{k-1}S_k & \sigma_{k-1} & \sigma_{k-2} & \ldots & \sigma_1 \end{vmatrix} = S_k$$

14. Нека $S_1, S_2, \ldots, S_n$ са степенните сборове на променливите $x_1, x_2, \ldots, x_n$. Докажете, че

$$\sigma_k = \frac{1}{k!}\begin{vmatrix} S_1 & 1 & 0 & 0 & \ldots 0 \\ S_2 & S_1 & 2 & 0 & \ldots 0 \\ S_3 & S_2 & S_1 & 3 & \ldots 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ S_k & S_{k-1} & S_{k-2} & S_{k-3} & \ldots S_1 \end{vmatrix}.$$

Упътване. Към първия стълб на детерминантата прибавете всички останали, умножени съответно с $-\sigma_1, \sigma_2, -\sigma_3, \ldots, (-1)^{k-1}\sigma_{k-1}$, и използувайте формулите на Нютон.

15. Пресметнете степенните сборове S_k за корените на уравнението $f(x)=0$, където:

а) $f(x)=x^4-x^3-19x^2+49x-30$, $k=1, 2, 3, 4$;
б) $f(x)=x^5-x^4-x^3-1$, $k=-3, -2, -1, 5, 6$;
в) $f(x)=x^6-2x^3-2x^2-2x-2$, $k=5, 6$.

Отг. а) $S_1=1$, $S_2=39$, $S_3=-89$, $S_4=723$;
б) $S_{-1}=0$, $S_{-2}=0$, $S_{-3}=-3$, $S_5=16$, $S_6=24$;
в) $S_5=10$, $S_6=24$.

16. Намерете уравнение $f(x)=0$ от трета степен, степенните сборове S_1, S_2, S_3 от корените на което са: $S_1=0, S_2=6, S_3=-3$.

Отг. $f(x)=x^3-3x+1=0$.

17. Намерете уравнение $f(x)=0$ от четвърта степен, за което $S_1=-1$, $S_2=-5$, $S_3=16$, $S_4=-25$.

Отг. $f(x)=x^4+x^3+2x^2-3x+4=0$.

18. Нека S_1, S_3, S_5 означават степенните сборове на променливите x_1, x_2, x_3. Докажете, че

$$\frac{S_1^5-S_5}{S_1^3-S_3}=\frac{5}{3}(\sigma_1^2-\sigma_2).$$

19. Пресметнете степенните сборове $S_1, S_2, \ldots, S_n$ от корените на уравнението $f(x)=0$, където

а) $f(x)=x^n+\frac{x^{n-1}}{1!}+\frac{x^{n-2}}{2!}+\ldots+\frac{x}{(n-1)!}+\frac{1}{n!}$;

б) $f(x)=x^n+x^{n-1}+\ldots+\ x+1;$
в) $f(x)=x^n+2x^{n-1}+3x^{n-2}+\ldots+(n-1)x^2+nx+n+1;$

г) $f(x)=x^n+\frac{a}{1!}x^{n-1}+\frac{a(a+1)}{2!}x^{n-2}+\ldots+\frac{a(a+1)\ldots(a+n-1)}{n!}.$

Отг. а) $S_1=-1,\ S_2=S_3=\ldots=S_n=0;$
б) $S_1=S_2=\ldots=S_n=-1;$
в) $S_1=S_2=\ldots=S_n=-2;$
г) $S_1=S_2=\ldots=S_n=-a;$

20. Пресметнете степенните сборове $S_1, S_2, \ldots, S_n$ от корените на уравнението

$$f(x)=x^n+(a+b)x^{n-1}+(a^2+ab+b^2)x^{n-2}+\ldots+(a^n+a^{n-1}b+\ldots+ab^{n-1}+b^n)=0.$$

Упътване. Пресметнете степенните сборове $S_1', S_2', \ldots, S_n'$ от корените на полинома $\varphi(x)=(x-a)(x-b)f(x)$.

Отг. $S_k=-(a^k+b^k),\ k=1, 2, \ldots, n.$

21. Пресметнете степенните сборове $S_1, S_2, \ldots, S_n$ от корените на уравнението

$$f(x)=x^n+(a+b)x^{n-1}+(a^2+b^2)x^{n-2}+\ldots+(a^n+b^n)=0.$$

Отг. $S_k=\begin{cases}-a^k-b^k, & \text{при } k \text{ — нечетно;}\\ -(a^{\frac{k}{2}}-b^{\frac{k}{2}})^2 & \text{при } k \text{ — четно,}\end{cases}$

22. Намерете уравнение $f(x)=0$ от степен n, за което:

а) $S_1=S_2=\ldots=S_{n-1}=0;$
б) $S_1=-1,\ S_2=S_3=\ldots=S_n=0;$
в) $S_2=S_3=\ldots=S_n=0.$

Отг. а) $f(x)=x-a;$

б) $f(x)=x^n+\frac{x^{n-1}}{1!}+\frac{x^{n-2}}{2!}+\ldots+\frac{x}{(n-1)!}+\frac{1}{n!};$

в) $f(x)=x^n-\frac{a}{1!}x^{n-1}+\frac{a}{2!}x^{n-2}+\ldots+(-1)^n\frac{a^n}{n!}.$

23. Намерете уравнение от n-та степен, за което

$$S_2=1,\ S_3=S_4=\ldots=S_n=S_{n+1}=0.$$

Решение. Нека

$$f(x)=x^n+\alpha x^{n-1}+a_2x^{n-2}+a_3x^{n-3}+\ldots+a_{n-1}x+a_n=0$$

е търсеното уравнение. Съгласно формулите на Нютон имаме

$$\begin{aligned}&a_1=\alpha,\\ &2a_2=\alpha a_1-1,\\ &3a_3=\alpha a_2-a_1,\\ &\ldots\ldots\\ &ka_k=\alpha a_{k-1}-a_{k-2},\\ &\ldots\ldots\ldots\ldots\\ &na_n=\alpha a_{n-1}-a_{n-2},\\ &0=\alpha a_n-a_{n-1}.\end{aligned}$$

От тези равенства непосредствено следва, че $k!\,a_k$ е полином на α от степен k. Като положим $k!a_k=P_k(\alpha)$, $P_0=1$, получаваме

$$P_1(\alpha)=\alpha,\ P_k(\alpha)-\alpha P_{k-1}(\alpha)+(k-1)P_{k-2}(\alpha)=0,\ -\alpha P_n(\alpha)+nP_{n-1}(\alpha)=0.$$

Първите две равенства показват, че $P_k(\alpha)$ е полином на Ермит, а от последното равенство следва, че α е корен на $P_{n+1}(x)$.

И така търсеното уравнение е

$$P_0(\alpha)x^n+\frac{P_1(\alpha)}{1!}x^{n-1}+\frac{P_2(\alpha)}{2!}+\ldots+\frac{P_n(\alpha)}{n!}=0,$$

където $P_0(x)$, $P_1(x),\ldots,P_n(x)$ са полиномите на Ермит:

$$P_k(x)=(-1)^k e^{\frac{x^2}{2}}\frac{d^k e^{-\frac{x^2}{2}}}{dx^k},\ k=0,1,2,\ldots,n,$$

а α е корен на полинома $P_{n+1}(x)$.

24. Решете системата уравнения

$$\begin{cases} x_1+x_2+\ldots+x_n=a, \\ x_1^2+x_2^2+\ldots+x_n^2=a, \\ \ldots\ldots\ldots\ldots\ldots \\ x_1^n+x_2^n+\ldots+x_n^n=a \end{cases}$$

и пресметнете $x_1^{n+1}+x_2^{n+1}+\ldots+x_n^{n+1}$.

Отг. Неизвестните $x_1, x_2,\ldots,x_n$ са корените на уравнението

$$x^n-\frac{a}{1!}x^{n-1}+\frac{a(a-1)}{2!}x^{n-2}-\ldots+(-1)^n\frac{a(a-1)\ldots(a-n+1)}{n!}=0,$$

$$x_1^{n+1}+x_2^{n+1}+\ldots+x_n^{n+1}=a+\frac{1}{n!}a(a-1)(2-a)\ldots(n-a).$$

25. Покажете, че ако

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

е полином с реални коефициенти и за някое ν, $1\leq\nu\leq n$, е изпълнено неравенството $a_\nu^2<a_{\nu-1}\,a_{\nu+1}$ $(a_0=1)$, то не всички корени на полинома $f(x)$ са реални.

Упътване. Използувайте равенството

$$\Sigma(x_1x_2\ldots x_\nu)^2=a_\nu^2-2a_{\nu-1}\,a_{\nu+1}.$$

26. Докажете, че за всяко нечетно просто число p е в сила сравнението

$$1^{p-1}+2^{p-1}+3^{p-1}+\ldots+(p-1)^{p-1}-(p-1)\equiv1+(p-1)!\,(\mathrm{mod}\,p^2).$$

Решение. Разглеждаме полинома

$$f(x)=(x-1)(x-2)\ldots[x-(p-1)]=x^{p-1}+a_1x^{p-2}+\ldots+a_{p-2}x+a_{p-1}.$$

Очевидно

$$a_{p-1}=(-1)^{p-1}(p-1)!=(p-1)!$$

По модул p имаме $f(x)\equiv x^{p-1}-1$, откъдето получаваме

$$a_1\equiv 0 \pmod p,\ a_2\equiv 0 \pmod p, \dots, a_{p-2}\equiv 0 \pmod p.$$

За степенните сборове ще имаме

$$S_1\equiv 0 \pmod p,\ S_2\equiv 0 \pmod p, \dots, S_{p-2}\equiv 0 \pmod p,$$

$$S_{p-1}=-a_1S_{p-2}-a_2S_{p-3}-\dots-a_{p-2}S_1-(p-1)a_{p-1}\equiv-(p-1)(p-1)! \pmod{p^2}.$$

Следователно

$$S_{p-1}-(p-1)\equiv-(p-1)(p-1)!-(p-1) \pmod{p^2}.$$

Но $-(p-1)(p-1)!-(p-1)=-p[(p-1)!+1]+(p-1)!+1\equiv(p-1)!+1 \pmod{p^2}$

27. Изразете чрез степенните сборове симетричните функции

а) $\sum x_1^\alpha x_2^\beta$;   б) $\sum x_1^\alpha x_2^\beta x_3^\gamma$.

Решение. а) За да пресметнем симетричната функция $\sum x_1^\alpha x_2^\beta$, умножаваме степенните сборове S_α и S_β. Ясно е, че в развитието на произведението $\sum x_1^\alpha \sum x_2^\beta$ ще се съдържат събираеми от вида $x_1^{\alpha+\beta}$ и $x_1^\alpha x_2^\beta$. Следователно ще имаме

$$\sum x_1^\alpha \sum x_2^\beta=\sum x_1^{\alpha+\beta}+\sum x_1^\alpha x_2^\beta.$$

От последното равенство получаваме

(1) $$\sum x_1^\alpha x_2^\beta=S_\alpha S_\beta-S_{\alpha+\beta} \text{ при } \alpha\neq\beta.$$

Ако $\alpha=\beta$, в сумата $\sum x_1^\alpha x_2^\alpha$ събираемите ще бъдат две по две равни, така че ще имаме:

(2) $$\sum x_1^\alpha x_2^\alpha=\frac{1}{2}\left(S_\alpha^2-S_{2\alpha}\right).$$

б) За да пресметнем симетричната функция $\sum x_1^\alpha x_2^\beta x_3^\gamma$, умножаваме $\sum x_1^\alpha x_2^\beta$ със степенния сбор $\sum x_1^\gamma$. В развитието на полученото произведение ще се съдържат събираеми от вида

$$x_1^\alpha x_2^\beta x_3^\gamma,\quad x_1^{\alpha+\gamma}x_2^\beta,\quad x_1^{\beta+\gamma}x_2^\beta.$$

Следователно ще имаме

$$\sum x_1^\alpha x_2^\beta \sum x_1^\gamma=\sum x_1^\alpha x_2^\beta x_3^\gamma+\sum x_1^{\alpha+\gamma}x_2^\beta+\sum x_1^\alpha x_2^{\beta+\gamma}.$$

Като вземем пред вид (1), последното равенство приема вида

$$(S_\alpha S_\beta-S_{\alpha+\beta})S_\gamma=\sum x_1^\alpha x_2^\beta x_3^\gamma+S_{\alpha+\gamma}S_\beta-S_{\alpha+\beta+\gamma}+S_\alpha S_{\beta+\gamma}-S_{\alpha+\beta+\gamma},$$

откъдето получаваме

(3) $$\sum x_1^\alpha x_2^\beta x_3^\gamma=S_\alpha S_\beta S_\gamma-S_{\alpha+\gamma}S_\beta-S_{\alpha+\beta}S_\gamma-S_{\beta+\gamma}S_\alpha+2S_{\alpha+\beta+\gamma}$$

при $\alpha\neq\beta$, $\beta\neq\gamma$, $\alpha\neq\gamma$. Ако два от показателите са равни, например $\alpha=\beta\neq\gamma$, ще имаме

(4) $$\sum x_1^\alpha x_2^\alpha x_3^\gamma=\frac{1}{2}\left(S_\alpha^2S_\gamma-2S_{\alpha+\gamma}S_\alpha-S_{2\alpha}S_\gamma+2S_{2\alpha+\gamma}\right),$$

а при $\alpha=\beta=\gamma$ за симетричната функция $\sum x_1^\alpha x_2^\alpha x_3^\alpha$ ще получим

(5) $$\sum x_1^\alpha x_2^\alpha x_3^\alpha=\frac{1}{6}\left(S_\alpha^3-3S_\alpha S_{2\alpha}+2S_{3\alpha}\right).$$

28. Като използувате предната задача, изразете чрез елементарните симетрични полиноми σ_1, σ_2, σ_3 на променливите x_1, x_2, x_3 следните симетрични полиноми:

а) $F=x_1^3x_2^2+x_1^3x_3^2+x_1^2x_2^3+x_1^2x_3^3+x_2^3x_3^2+x_2^2x_3^3$;

б) $F=x_1^2x_2^2+x_1^2x_2^2+x_2^2x_3^2$.

Отг. а) $F=-2\sigma_1^3\sigma_3+\sigma_1\sigma_2^2-\sigma_2\sigma_3$; б) $F=\sigma_2^2-2\sigma_1\sigma_3$.

29. Като използувате зад. 27, изразете чрез елементарните симетрични полиноми σ_1, σ_2, σ_3, σ_4 на променливите x_1, x_2, x_3, x_4 следните симетрични полиноми:

а) $F=\sum x_1^3x_2^2x_3$;

б) $F=\sum x_1^2x_2^2x_3$;

в) $F=\sum x_1^2x_2^2x_3^2$.

Отг. а) $F=\sigma_1\sigma_2\sigma_3-3\sigma_1^2\sigma_4-3\sigma_3^2+4\sigma_2\sigma_4$; б) $F=\sigma_2\sigma_3-\sigma_1\sigma_4$;
в) $F=\sigma_3^2-\sigma_2\sigma_4$.

30. Като използувате зад. 27, изразете чрез елементарните симетрични полиноми симетричната дроб F на променливите x_1, $x_2,\dots,x_n$, където:

а) $F=\sum\frac{x_1^2}{x_2}$, $n=4$;

б) $F=\sum\frac{x_1^2x_2}{x_3}$, $n=4$.

Отг. а) $F=\frac{1}{\sigma_4}\left(\sigma_1^2\sigma_3-\sigma_1\sigma_4-2\sigma_2\sigma_3\right)$;

б) $F=\frac{1}{\sigma_4}\left(2\sigma_1^3\sigma_3-3\sigma_1^2\sigma_4-5\sigma_1\sigma_2\sigma_3+4\sigma_2\sigma_4+3\sigma_3^2\right)$.

31. Пресметнете симетричния полином F от корените на уравнението $f(x)=0$, където:

а) $F=\sum x_1^3x_2$,
$f(x)=x^3-x^2-4x+1$;

б) $F=\sum x_1^3x_2x_3$,
$f(x)=x^4+x^3-2x^2-3x+1$;

в) $F=\sum x_1^2x_2^2$,
$f(x)=x^4+px^3+qx^2+rx+s$;

г) $F=\sum x_1^4 x_2^2$,

$f(x)=x^3+px+q$.

Отг. а) $F=-35$; б) $F=16$; в) $F=q^2-2pr+2s$; г) $F=-2p^3-3q^2$.

32. Пресметнете симетричната дроб F за корените на уравнението $f(x)=0$, където:

а) $F=\sum \frac{x_1}{x_2}$,

$f(x)=x^4-2x^3+7$;

б) $F=\sum \frac{x_1^2 x_2^2}{x^3}$,

$f(x)=x^4-3x+1$;

в) $F=\sum \frac{x_1^3 x_2^2}{x_3}$,

$f(x)=x^4-3x^2+2x-1$.

Отг. а) $F=-4$; б) $F=15$; в) $F=-124$.

33. Пресметнете симетричния полином

$$F=\begin{vmatrix} x_1+x_2 & 1 & 1 & 1 & 1 \\ 1 & x_2+x_3 & 1 & 1 & 1 \\ 1 & 1 & x_1+x_3 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{vmatrix}$$

за корените на уравнението $f(x)=x^3-x^2+1=0$.

Отг. $F=3$.

34. Пресметнете симетричния полином F за корените на уравнението $f(x)=0$, където:

а) $F=\sum x_1^2(x_2+x_3)^2$,

$f(x)=x^4-x^3+2x^2+x-2$;

б) $F=\sum (x_1-x_2)^2(x_3-x_4)^2$,

$f(x)=x^4-5x^2-2x+1$;

в) $F=(x_1^3+x_2^3)(x_2^3+x_3^3)(x_3^3+x_1^3)$,

$f(x)=x^3+x^2-3x-5$.

Отг. а) $F=22$; б) $F=74$; в) $F=140$.

35. Нека x_1, x_2, x_3 са корените на уравнението

$$f(x)=x^3+px+q=0.$$

Пресметнете симетричната функция F, където:

а) $F=(x_1+x_2)^4(x_2+x_3)^4(x_3+x_1)^4$;

б) $F=(x_1^2-x_2x_3)(x_2^2-x_3x_1)(x_3^2-x_1x_2)$;

в) $F=\frac{x_1^2}{x_2x_3}+\frac{x_2^2}{x_3x_1}+\frac{x_3^2}{x_1x_2}$;

г) $F=\frac{1}{x_1^2+x_1x_2+x_2^2}+\frac{1}{x_2^2+x_2x_3+x_3^2}+\frac{1}{x_3^2+x_3x_1+x_1^2}$;

д) $F=\frac{x_1}{x_1^2-x_2x_3}+\frac{x_2}{x_2^2-x_3x_1}+\frac{x_3}{x_3^2-x_1x_2}$;

е) $F=\frac{x_1^2}{(1+x_2)(1+x_3)}+\frac{x_2^2}{(1+x_3)(1+x_1)}+\frac{x_3^2}{(1+x_1)(1+x_2)}$;

ж) $F=\frac{x_1^2}{(1+x_1)^2}+\frac{x_2^2}{(1+x_2)^2}+\frac{x_3^2}{(1+x_3)^2}$;

з) $F=\left(\frac{x_2^2+x_3^2}{x_2x_3}+\frac{x_2+x_3}{x_1}\right)\left(\frac{x_3^2+x_1^2}{x_3x_1}+\frac{x_3+x_1}{x_2}\right)\left(\frac{x_1^2+x_2^2}{x_1x_2}+\frac{x_1+x_2}{x_3}\right)$;

и) $F=\frac{x_1}{x_1^2+x_2x_3}+\frac{x_2}{x_2^2+x_3x_1}+\frac{x_3}{x_3^2+x_1x_2}$;

к) $F=\frac{x_1}{(1+x_1)^2}+\frac{x_2}{(1+x_2)^2}+\frac{x_3}{(1+x_3)^2}$;

л) $F=\frac{x_1^2}{(x_2-x_3)^2}+\frac{x_2^2}{(x_3-x_1)^2}+\frac{x_3^2}{(x_1-x_2)^2}$;

м) $F=\frac{1}{x_1^2+x_2^2}+\frac{1}{x_2^2+x_3^2}+\frac{1}{x_3^2+x_1^2}$;

н) $F=\frac{1}{(x_1-x_2)^2}+\frac{1}{(x_2-x_3)^2}+\frac{1}{(x_3-x_1)^2}$;

о) $F=\frac{(x_1-x_2)^2}{x_3^2}+\frac{(x_2-x_3)^2}{x_1^2}+\frac{(x_3-x_1)^2}{x_2^2}$;

п) $F=\frac{(x_1^2+x_2^2)^2}{x_3}+\frac{(x_2^2+x_3^2)^2}{x_1}+\frac{(x_3+x_1)^2}{x_2}$.

Решение.

а) Като вземем пред вид, че $x_1+x_2+x_3=0$, получаваме

$$F=(-x_3)^4(-x_1)^4(-x_2)^4=(x_1x_2x_3)^4=q^4.$$

б) Като вземем пред вид, че $x_1x_2x_3=-q$, получаваме

$$F=\left(x_1^2+\frac{q}{x_1}\right)\left(x_2^2+\frac{q}{x_2}\right)\left(x_3^2+\frac{q}{x_3}\right)=\frac{x_1^3+q}{x_1}\cdot\frac{x_2^3+q}{x_2}\cdot\frac{x_3^3+q}{x_3}.$$

От друга страна, $x_i^3+px_i+q=0$, т. е. $x_i^3+q=-px_i$, $i=1, 2, 3$. Следователно за симетричния полином F ще имаме $F=-p^3$.

в) Имаме

$$F=\sum\frac{x_1^3}{x_1x_2x_3}=\frac{1}{q}\sum x_1^3=-\frac{1}{q}\sum(-px_1-q)=3.$$

г) За симетричната дроб F имаме

$$F=\sum\frac{1}{(x_1+x_2)^2-x_1x_2}=\sum\frac{1}{x_3^2+\frac{q}{x_3}}=\sum\frac{x_3}{x_3^3+q}=\sum\frac{x_3}{-px_3}=-\frac{3}{p}.$$

д) Аналогично на случая г) получаваме $F=0$.

е) Симетричната дроб F преобразуваме по следния начин:

$$F=\sum\frac{x_1^2(1+x_1)}{(1+x_1)(1+x_2)(1+x_3)}=\frac{S_2+S_3}{(1+x_1)(1+x_2)(1+x_3)}.$$

Но $S_2=-2p$, $S_3=-3p$, от тъждеството

$$f(x)=x^3+px+q=(x-x_1)(x-x_2)(x-x_3),$$

получаваме

$$f(-1)=-1-p+q=(-1-x_1)(-1-x_2)(-1-x_3)=-(1+x_1)(1+x_2)(1+x_3).$$

Следователно

$$F=\frac{2p+3q}{1+p-q}.$$

ж) Очевидно

$$F=\sum\frac{x_1^2}{(1+x_1)^2}=\left(\sum\frac{x_1}{1+x_1}\right)^2-2\sum\frac{x_1x_2}{(1+x_1)(1+x_2)}.$$

Пресмятаме поотделно симетричните дроби в дясната страна на равенството. Имаме

$$\sum\frac{x_1x_2}{(1+x_1)(1+x_2)}=\sum\frac{x_1x_2(1+x_3)}{(1+x_1)(1+x_2)(1+x_3)}=\frac{p-3q}{q-p-1}.$$

За другата симетрична дроб имаме

$$\sum\frac{x_1}{1+x_1}=\sum\left(1-\frac{1}{1+x_1}\right)=3-\sum\frac{1}{1+x_1}.$$

От равенството $\dfrac{f'(x)}{f(x)}=\sum\dfrac{1}{x-x_1}$ получаваме

$$-\sum\frac{1}{1+x_1}=\frac{f'(-1)}{f(-1)}=\frac{3+p}{q-p-1}.$$

Следователно

$$\sum\frac{x_1}{1+x_1}=3-\frac{3+p}{1+p-q}=\frac{2p-3p}{1+p-q}.$$

И така за симетричната дроб F ще имаме $F=\left(\dfrac{2p-3q}{1+p-q}\right)^2+2\dfrac{p-3q}{1+p-q}$.

з) Симетричната дроб пресмятаме по следния начин:

$$F=\prod\left[\frac{(x_2+x_3)^2-2x_2x_3}{x_2x_3}+\frac{-x_1}{x_1}\right]=\prod\left(\frac{x_1^2}{x_2x_3}-3\right)=\prod\left(-\frac{x_1^3}{q}-3\right)=$$

$$=-\frac{1}{q^3}\prod(x_1^3+3q)=-\frac{1}{q^3}\prod(2q-px_1)=-\frac{p}{q^3}\prod\left(\frac{2q}{p}-x_1\right)=$$

$$=\frac{p}{q^3}f\left(\frac{2q}{p}\right)=\frac{p^3-8q^2}{p^2q^2}.$$

и) Имаме $F=\sum\frac{x_1}{x_1^2+x_2x_3}=\sum\frac{x_1}{x_1^2-\frac{q}{x_1}}=\sum\frac{x_1^2}{x_1^3-q}=$

$$=\sum\frac{x_1^2}{-px_1-2q}=-\frac{1}{p^2}\sum\frac{p^2x_1^2-4q^2+4q^2}{px_1+2q}=-\frac{1}{p^2}\sum(px_1-2q)-$$

$$-\frac{4q^2}{p^2}\sum\frac{1}{px_1+2q}=\frac{6q}{p^2}+\frac{4q^2}{p^3}\sum\frac{1}{\frac{-2q}{p}-x_1}=\frac{6q}{p^2}+\frac{4q^2}{p^3}\cdot\frac{f'\left(-\frac{2q}{p}\right)}{f\left(-\frac{2q}{p}\right)}.$$

к) Симетричната дроб F представяме във вида

$$F=\sum\frac{x_1}{(1+x_1)^2}=\sum\left[\frac{1}{1+x^2}-\frac{1}{(1+x_1)^2}\right]=-\frac{f'(-1)}{f(-1)}-\sum\frac{1}{(1+x_1)^2}.$$

От равенството

$$\frac{f'(x)}{f(x)}=\sum\frac{1}{x-x_1}$$

получаваме

$$\frac{f''(x)f(x)-f'^2(x)}{f^2(x)}=-\sum\frac{1}{(x-x_1)^2},$$

от което при $x=-1$ имаме

$$\sum\frac{1}{(1+x_1)^2}=\frac{f'^2(-1)-f(-1)f''(-1)}{f^2(-1)}.$$

л) Симетричната дроб F пресмятаме по следния начин:

$$F=\sum\frac{x_1^2}{(x_2-x_3)^2}=\sum\frac{x_1^2}{(x_2+x_3)^2-4x_2x_3}=\sum\frac{x_1^2}{x_1^2+\frac{4q}{x_1}}=\sum\frac{x_1^3}{x_1^3+4q}=$$

$$=\sum\frac{px_1+q}{px_1-3q}=\sum\left(1+\frac{4q}{px_1-3q}\right)=3-\frac{4q}{p}\sum\frac{1}{\frac{3q}{p}-x_1}=3-\frac{4q}{p}\cdot\frac{f'\left(\frac{3p}{q}\right)}{f\left(\frac{3q}{p}\right)}.$$

В останалите случаи постъпваме по подобен начин. Получаваме

м) $F=-\frac{5p^2}{2p^3+q^2}$;

н) $F=-\frac{9p^3}{4p^3+27q^2}$;

о) $F=\frac{1}{q^2}(9q^2-4p^3)$;

п) $F=-\frac{1}{q}(4p^3+3q^2)$.

36. Нека x_1, x_2, x_3 са корените на уравнението

$$f(x)=x^3+px^2+qx+r=0.$$

Пресметнете стойността на симетричния полином F, където:

а) $F=x_1(x_2-x_3)^2+x_2(x_3-x_1)^2+x_3(x_1-x_2)^2$;

б) $F=x_1^3(x_2+x_3)^2+x_2^3(x_3+x_1)^2+x_3^3(x_1+x_2)^2$;

в) $F=(x_1-x_2)^2(x_1-x_3)^2+(x_2-x_1)^2(x_2-x_3)^2+(x_3-x_1)^2(x_3-x_2)^2$;

г) $F=(x_1^2+x_1x_2+x_2^2)(x_2^2+x_2x_3+x_3^2)(x_3^2+x_3x_1+x_1^2)$;

д) $F=x_1x_2(x_1+x_2)^2+x_1x_3(x_1+x_3)^2+x_2x_3(x_2+x_3)^2$;

е) $F=(x_1^2-x_2^2)^2+(x_2^2-x_3^2)^2+(x_3^2-x_1^2)^2$;

ж) $F=(x_1^2-x_2^2)^2(x_2^2-x_3^2)^2(x_3^2-x_1^2)^2$;

з) $F=(x_1^2x_2+x_2^2x_3+x_3^2x_1)(x_1^2x_3+x_2^2x_1+x_3^2x_2)$;

и)
$$F=\begin{vmatrix} x_1 & x_2 & 0 & 0 & 0 & 0 \\ x_3 & x_1 & 0 & 0 & 0 & 0 \\ 1 & 1 & x_2 & x_3 & 0 & 0 \\ 1 & 1 & x_1 & x_2 & 1 & 1 \\ 0 & 0 & 0 & 0 & x_3 & x_1 \\ 0 & 0 & 0 & 0 & x_2 & x_3 \end{vmatrix}.$$

Отг. а) $F=9r-pq$; б) $F=5qr-pq^2$; в) $F=p^4-6p^2q+9q^2$; г) $F=p^2q^2-q^3-p^3r$; д) $F=p^2q-5pr$; е) $F=2p^4-8p^2q+2q^2+12pr$; ж) $F=(r-pq)^2(p^2q^2-4p^3r-4q^3+18pqr-27r^2)$; з) $F=p^3r+q^2-3pqr$; и) $F=p^3r-q^3$.

37. Нека x_1, x_2, x_3 са корените на уравнението

$$f(x)=x^3+px^2+qx+r=0.$$

Пресметнете стойността на симетричната дроб F, където:

а) $F=\dfrac{x_1}{x_2+x_3}+\dfrac{x_2}{x_3+x_1}+\dfrac{x_3}{x_1+x_2}$;

б) $F=\dfrac{x_1x_2}{x_1+x_2}+\dfrac{x_2x_3}{x_2+x_3}+\dfrac{x_3x_1}{x_3+x_1}$;

в) $F=\dfrac{x_2x_3-x_1^2}{x_2+x_3-2x_1}+\dfrac{x_3x_1-x_2^2}{x_3+x_1-2x_2}+\dfrac{x_1x_2-x_3^2}{x_1+x_2-2x_3}$;

г) $F=\dfrac{x_1^2}{x_2+x_3}+\dfrac{x_2^2}{x_3+x_1}+\dfrac{x_3^2}{x_1+x_2}$;

д) $F=\dfrac{(x_1-x_2)^2}{x_1x_2}+\dfrac{(x_2-x_3)^2}{x_2x_3}+\dfrac{(x_3-x_1)^2}{x_3x_1}$;

е) $F=\dfrac{x_1+x_2}{1+x_1+x_2}+\dfrac{x_2+x_3}{1+x_2+x_3}+\dfrac{x_3+x_1}{1+x_3+x_1}$;

ж) $F=\dfrac{(x_1-x_2)^2}{x_1+x_2}+\dfrac{(x_2-x_3)^2}{x_2+x_3}+\dfrac{(x_3-x_1)^2}{x_3+x_1}$;

з) $F=\dfrac{x_1^2+x_2^2}{x_1+x_2}+\dfrac{x_2^2+x_3^2}{x_2+x_3}+\dfrac{x_3^2+x_1^2}{x_3+x_1}$;

и) $F=\frac{x_1^2+x_2x_3}{x_2+x_3}+\frac{x_2^2+x_3x_1}{x_3+x_1}+\frac{x_3^2+x_1x_2}{x_1+x_2}$;

Отг. а) $F=\frac{-p^3+2pq-3r}{r-pq}$; б) $F=\frac{5pr+q^2}{r-pq}$;

в) $F=-p+\frac{(q-p)(2p^3-9pq+27r)}{81(3q-p^2)}$; г) $F=\frac{p^4-3p^2q+4pr}{r-pq}$;

д) $F=\frac{1}{r}(pq-6r)$; е) $F=\frac{3r+2q-2p-3pq+2p^3}{1-2p+p^2+q-pq+r}$;

ж) $F=\frac{pr+q^2}{r(pq-r)}$; з) $F=\frac{4pr+2q^2-2p^2q}{pq-r}$;

и) $F=\frac{(p-q)(p^2q-q^2-pr-pqr)}{q^2(r-pq)}$.

38. Нека x_1, x_2, x_3, x_4 са корените на уравнението

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

Пресметнете стойността на симетричната дроб F, където

а) $F=(x_1x_2+x_3x_4)(x_1x_3+x_2x_4)(x_1x_4+x_2x_3)$;

б) $F=\sum x_1^3(x_2+x_3)^2$;

в) $F=(x_1-x_2)^2(x_3-x_4)^2+(x_1-x_3)^2(x_2-x_4)^2+(x_1-x_4)^2(x_2-x_3)^2$;

г) $F=(x_1+x_2-x_3-x_4)^2(x_1-x_2+x_3-x_4)^2(x_1-x_2-x_3+x_4)^2$;

д) $F=\frac{1}{x_1x_2+x_3x_4}+\frac{1}{x_1x_3+x_2x_4}+\frac{1}{x_1x_4+x_2x_3}$;

е) $F=\frac{x_1^2}{1+x_1}+\frac{x_2^2}{1+x_2}+\frac{x_3^2}{1+x_3}+\frac{x_4^2}{1+x_4}$.

Отг. а) $F=q^2-4pr$; б) $F=-2pq$; в) $F=2p^2+24r$;
г) $F=64q^2$; д) $F=-\frac{4r}{q^2-4pr}$; е) $F=\frac{-2p+3q-4r}{1+p-q+r}$.

39. Нека x_1, x_2, x_3, x_4 са корените на уравнението

$$f(x)=x^4+px^3+qx^2+rx+s=0.$$

Пресметнете стойността на симетричния полином

$$F=\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \\ x_3 & x_4 & x_1 & x_2 \\ x_4 & x_3 & x_2 & x_1 \end{vmatrix}.$$

Решение. Като прибавим към първия стълб останалите три и вземем пред вид равенството

$$x_1+x_2+x_3+x_4=-p,$$

получаваме

$$F=\begin{vmatrix} -p & x_2 & x_3 & x_4 \\ -p & x_1 & x_4 & x_3 \\ -p & x_4 & x_1 & x_2 \\ -p & x_3 & x_2 & x_1 \end{vmatrix}.$$

По-нататък от втория, третия и четвъртия ред изваждаме първия и развиваме получената детерминанта по първия стълб:

$$F=-p\begin{vmatrix} x_1-x_2 & x_4-x_3 & x_3-x_4 \\ x_4-x_2 & x_1-x_3 & x_2-x_4 \\ x_3-x_2 & x_2-x_3 & x_1-x_4 \end{vmatrix}.$$

Чрез директно пресмятане на последната детерминанта получаваме

$$F=-p[(x_1-x_2)(x_1-x_3)(x_1-x_4)+(x_2-x_1)(x_2-x_3)(x_2-x_4)+$$
$$+(x_3-x_1)(x_3-x_2)(x_3-x_4)+(x_4-x_1)(x_4-x_2)(x_4-x_3)].$$

Но четирите събираеми в тази сума са съответно равни на $f'(x_1)$, $f'(x_2)$, $f'(x_3)$, $f'(x_4)$.
Следователно

$$F=-p[f'(x_1)+f'(x_2)+f'(x_3)+f'(x_4)]=p(p^3-4pq+8r).$$

40. Изразете симетричния полином на n променливи

$$F=\sum_{i<j}(x_i+x_j)^k$$

чрез степенните сборове.

Решение. Имаме

$$\sum_{i=1}^{n}(x+x_i)^k=\sum_{m=0}^{k}\binom{k}{m}S_{k-m}x^m,$$

откъдето

$$\sum_{i=1}^{n}(x_j+x_i)^k=\sum_{m=0}^{k}\binom{k}{m}S_{k-m}x_j^m$$

за всяко j. Като сумираме, получаваме

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(x_j+x_i)^k=\sum_{m=0}^{k}\binom{k}{m}S_{k-m}S_m,$$

откъдето намираме

$$F=\sum_{i<j}(x_i+x_j)^k=\frac{1}{2}\left[\sum_{m=0}^{k}\binom{k}{m}S_{k-m}S_m-2^knS_k\right].$$

41. Изразете симетричния полином на n променливи

$$F=\sum_{i<j}(x_i-x_j)^{2k}$$

чрез степенните сборове.

$$\text{Отг. } F=\frac{1}{2}\sum_{m=0}^{2k}\binom{2k}{m}(-1)^m S_m-S_{2k-m}.$$

42. Нека

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_mx^m$$

е даден полином. Пресметнете стойността на симетричния полином

$$F=n(f(x_1)+f(x_2)+\ldots+f(x_n))$$

за корените на уравнението $x^n-1=0$.

Решение. Лесно се вижда, че за степенните сборове от корените на уравнението $x^n-1=0$ имаме $S_k=0$ при $k\not\equiv 0 \pmod{n}$ и $S_k=1$ при $k\equiv 0 \pmod{n}$: Оттук получаваме

$$F=n(a_0+a_n+a_{2n}+\ldots).$$

43. Нека $\varphi(x)$ е полином. Покажете, че стойността на симетричния полином

$$F=\varphi(x_1)+\varphi(x_2)+\ldots+\varphi(x_n),$$

за корените на полинома $f(x)$ от n-та степен, е равна на коефициента пред $\frac{1}{x}$ в развитието на $\frac{f'(x)\varphi(x)}{f(x)}$ по степените на x.

Решение. От равенството

$$\frac{f'(x)}{f(x)}=\sum_{i=1}^{n}\frac{1}{x-x_i}$$

имаме

$$\frac{\varphi(x)f'(x)}{f(x)}=\sum_{i=1}^{n}\frac{\varphi(x)}{x-x_i}. \tag{1}$$

Но

$$\varphi(x)=\varphi(x_i+x-x_i)=\varphi(x_i)+\varphi'(x_i)(x-x_i)+\frac{\varphi''(x_i)}{2!}(x-x_i)^2+\ldots,$$

$$\frac{\varphi(x)}{x-x_i}=\frac{\varphi(x_i)}{x-x_i}+\varphi'(x_i)+\frac{\varphi''(x_i)}{2!}(x-x_i)+\ldots.$$

Като представим първия член от дясната страна на последното равенство във вида

$$\frac{\varphi(x_i)}{x-x_i}=\frac{\varphi(x_i)}{x\left(1-\frac{x_i}{x}\right)}=\frac{\varphi(x_i)}{x}+\frac{x_i\varphi(x_i)}{x^2}+\frac{x_i^2\varphi(x_i)}{x^3}+\ldots$$

и заместим в (1), получаваме желания резултат.

В следващите няколко задачи се излагат други доказателства на основните теореми от теорията на симетричните полиноми и се правят някои допълнения към тях.

44. Докажете основната теорема от теорията на симетричните полиноми, а именно за всеки симетричен полином

$$F(x_1, x_2, \dots, x_n)$$

на променливите $x_1, x_2, \dots, x_n$ съществува такъв полином $f(t_1, t_2, \dots, t_n)$ на променливите $t_1, t_2, \dots, t_n$, че

$$F(x_1, x_2, \dots, x_n)=f(\sigma_1, \sigma_2, \dots, \sigma_n),$$

където $\sigma_1, \sigma_2, \dots, \sigma_n$ са елементарните симетрични полиноми на променливите $x_1, x_2, \dots, x_n$.

Доказателство. При $n=1$ твърдението е очевидно, защото всеки полином на една променлива е симетричен. Нека $n>1$. Ако в полинома $F(x_1, x_2, \dots, x_n)$ положим $x_n=0$, получаваме симетричен полином $G(x_1, x_2, \dots, x_{n-1})$ на първите $n-1$ променливи. По индукция съществува такъв полином $g(t_1, t_2, \dots, t_{n-1})$, че

$$G(x_1, x_2, \dots, x_{n-1})=g(\tau_1, \tau_2, \dots, \tau_{n-1}),$$

където τ_i, $i=1, 2, \dots, n-1$, са елементарните симетрични полиноми на първите $n-1$ променливи $x_1, x_2, \dots, x_{n-1}$. Да разгледаме полинома на n променливи

$$H(x_1, x_2, \dots, x_n)=F(x_1, x_2, \dots, x_n)-g(\sigma_1, \sigma_2, \dots, \sigma_{n-1}),$$

който очевидно е симетричен. Ако в него положим $x_n=0$ и вземем пред вид, че $\sigma_i(x_1, x_2, \dots, x_{n-1}, 0)=\tau_i(x_1, x_2, \dots, x_{n-1})$, $i=1, \dots, n-1$, получаваме

$$H(x_1, x_2, \dots, x_{n-1}, 0)=0,$$

откъдето следва, че полиномът $H(x_1, x_2, \dots, x_n)$ се дели на x_n. Поради неговата симетричност той ще се дели и на $x_1, x_2, \dots, x_{n-1}$, следователно ще се дели и на произведението $x_1 x_2 \dots x_n$, т. е. ще има вида

$$H(x_1, x_2, \dots, x_n)=x_1 x_2 \dots x_n H_0(x_1, x_2, \dots, x_n)=\sigma_n H_0(x_1, \dots, x_n).$$

Очевидно полиномът $H_0(x_1, \dots, x_n)$ е симетричен и има степен, по-малка от степента на H. Сега можем да направим индукция по степента на разглеждания полином (при фиксиран брой n на променливите). По индукционното предположение H_0 може да се представи във вида

$$H_0(x_1, x_2, \dots, x_n)=h(\sigma_1, \sigma_2, \dots, \sigma_n),$$

откъдето

$$F(x_1, x_2, \dots, x_n)=g(\sigma_1, \sigma_2, \dots, \sigma_n)+\sigma_n h(\sigma_1, \sigma_2, \dots, \sigma_n),$$

с което теоремата е доказана.

45. Докажете, че всеки симетричен полином се изразява чрез елементарните симетрични полиноми еднозначно.

Доказателство. Трябва да се докаже, че ако $f(t_1, t_2, \dots, t_n)$ и $g(t_1, t_2, \dots, t_n)$ са полиноми на променливите $t_1, t_2, \dots, t_n$, за които

$$f(\sigma_1, \sigma_2, \dots, \sigma_n)=g(\sigma_1, \sigma_2, \dots, \sigma_n)$$

(равенство в смисъл на полиноми на променливите $x_1, x_2, \dots, x_n$), то $f(t_1, t_2, \dots, t_n)=g(t_1, t_2, \dots, t_n)$ (като полиноми на $t_1, t_2, \dots, t_n$); или като разгледаме разликата на f и g, трябва да покажем, че ако за полинома $h=f-g$ е изпълнено

$$h(\sigma_1, \sigma_2, \dots, \sigma_n)=0,$$

то и $h(t_1, t_2, \dots, t_n)=0$. При $n=1$ твърдението е очевидно, защото имаме само една променлива и $\sigma_1=x_1$. Нека $n>1$ и $\tau_1, \tau_2, \dots, \tau_{n-1}$ са елементарните симетрични полиноми на първите $n-1$ променливи. Ако в равенството

$$h(\sigma_1, \sigma_2, \dots, \sigma_n)=0$$

положим $\sigma_n=0$, получаваме

$$h(\tau_1, \tau_2, \dots, \tau_{n-1}, 0)=0$$

и по индукция получаваме равенството

$$h(t_1, t_2, \dots, t_{n-1}, 0)=0.$$

Следователно, ако представим полинома $h(t_1, t_2, \dots, t_n)$ във вида

$$h(t_1, t_2, \dots, t_n)=\varphi_0+\varphi_1 t_n+\dots+\varphi_k t^k_n,$$

където φ_i, $i=0, \dots, k$ са полиноми на $t_1, t_2, \dots, t_{n-1}$, то $\varphi_0=0$, т. е. h има вида $h=t_n\psi$, където ψ е полином на $t_1, t_2, \dots, t_n$ от степен, по-ниска от тази на h. Сега имаме

$$h(\sigma_1, \sigma_2, \dots, \sigma_n)=\sigma_n\psi(\sigma_1, \sigma_2, \dots, \sigma_n)$$

и следователно

$$\psi(\sigma_1, \sigma_2, \dots, \sigma_n)=0,$$

понеже $\sigma_n\neq 0$. Сега можем да направим индукция по степента на разглеждания полином. Ако тя е 0, твърдението е очевидно. В общия случай по индукция ще имаме $\psi(t_1, t_2, \dots, t_n)=0$ и още повече $h(t_1, t_2, \dots, t)=0$.

46. Докажете, че всяка симетрична дроб може да се представи като частно на два симетрични полинома.

Решение. Нека дробта $r=\frac{f}{g}$ е симетрична и нека $g=g_1, g_2, \dots, g_N$, $N\leq n!$ са всички полиноми, които се получават от g чрез разместване на променливите. Тогава произведението $g_1 g_2 \dots g_N$ е симетричен полином и имаме

$$r=\frac{fg_2g_3\dots g_N}{g_1g_2\dots g_N}.$$

От равенството $rg_1g_2\dots g_N=fg_2\dots g_N$ следва, че и числителят е симетричен.

47. Покажете, че симетричните дроби с коефициенти от едно поле P образуват подполе на полето $P(x_1, x_2, \dots, x_n)$ от всички рационални дроби на n променливи с коефиенти в P и че това поле е изоморфно с полето $P(x_1, x_2, \dots, x_n)$.

Упътване. Като използувате зад. 45, 46, 47, покажете, че съществува изоморфизъм на полето $P(x_1, x_2, \dots, x_n)$ върху полето от симетрични дроби, при който променливите $x_1, x_2, \dots, x_n$ се изразяват съответно в елементарните симетрични полиноми $\sigma_1, \sigma_2, \dots, \sigma_n$. Покажете също така, че при този изоморфизъм на полиноми съответствуват полиноми и че полето от симетрични дроби е поле от частни на пръстена от симетрични полиноми.

48. Като използувате зад. 46 за еднозначност на изразяването чрез елементарните симетрични полиноми, докажете теоремата за степента и теглото, а именно, че ако $F=F(x_1, \dots, x_n)$ е симетричен полином от степен s и степен относно всяка променлива m, F се представя във вида $F=f(\sigma_1, \sigma_2, \dots, \sigma_n)$, където f

е, полином от степен m и с тегло s. Докажете също, че полиномът F е хомогенен тогава и само тогава, когато f е изобарен. (Под *тегло на един едночлен* $Ct_1^{\alpha_1}t_2^{\alpha_2}\ldots t_n^{\alpha_n}$ разбираме числото $\alpha_1+2\alpha_2+\ldots+n\alpha_n$, а под *тегло на полином* — максимума на теглата на членовете му. Един полином се нарича *изобарен*, ако всичките му членове имат едно и също тегло.)

49. Докажете, че ако основното поле има характеристика 0, всеки симетричен полином на n променливи може да се изрази чрез степенните сборове $S_1, S_2, \ldots, S_n$. Покажете също, че това изразяване е еднозначно (в смисъла, изяснен в решението на зад. 45).

Доказателство. От формулите на Нютон следва, че елементарните симетрични полиноми се изразяват чрез степенните сборове, а оттук и всеки друг полином се изразява чрез тях. Единствеността на изразяването е тривиална при $n=1$. Нека $n>1$ и нека $T_1, T_2, \ldots, T_{n-1}$ означават степенните сборове на първите $n-1$ промеиливи. Трябва да покажем, че ако $f(t_1, t_2, \ldots, t_n)$ е полином и

$$f(S_1, S_2, \ldots, S_n)=0,$$

то $f(t_1, t_2, \ldots t_n)=0$. Да допуснем, че $f\neq 0$. Тогава f непременно зависи от последната проминлива t_n. Наистина в противен случай от равенството

$$f(S_1, S_2, \ldots, S_{n-1})=0,$$

като положим $x_n=0$, ще последва

$$f(T_1, T_2, \ldots, T_{n-1})=0$$

и съгласно индукционното предположение $f=0$. И така f има вида

$$f=\varphi_0 t_n^N+\varphi_1 t_n^{N-1}+\ldots+\varphi_N,$$

където φ_i са полиноми на $t_1, t_2, \ldots, t_{n-1}$ и $\varphi_0\neq 0$. По формулите на Нютон съществуват полиноми $h_1(u_1), h_2(u_1, u_2), \ldots, h_n(u_1, u_2, \ldots, u_n)$, така че $S_i=h_i(\sigma_1, \sigma_2, \ldots, \sigma_i)$, при това h_n има вида $h_n=\pm nu_n+g(u_1, u_2, \ldots, u_{n-1})$. Да разгледаме полинома p на променливите $u_1, u_2, \ldots, u_n$:

$$p=f(h_1(u_1), h_2(u_1, u_2), \ldots, h_n(u_1, u_2, \ldots, u_n)).$$

Ясно е, че той ще има вида

$$p=q(u_1, u_2, \ldots, u_{n-1})\, u_n^N+r(u_1, u_2, \ldots, u_n),$$

където

$$q=\pm n^N\varphi_0(h_1(u_1), \ldots, h_{n-1}(u_1, u_2, \ldots, u_{n-1})),$$

а полиномът r по отношение на u_n има степен, по-малка от N. Имаме

$$p(\sigma_1, \sigma_2, \ldots, \sigma_n)=f(S_1, S_2, \ldots, S_n)=0$$

и съгласно зад. 45 $p=0$. Но от посочения вид на полинома p следва, че това е възможно само ако $q(u_1, u_2, \ldots, u_{n-1})=0$. И така $q=0$. Но $q(\sigma_1, \ldots, \sigma_{n-1})=\pm n N\varphi_0(S_1, \ldots, S_{n-1})$. И така

$$\varphi_0(S_1, S_2, \ldots, S_{n-1})=0.$$

Като положим $x_n=0$, получаваме $\varphi_0(T_1, T_2, \ldots, T_{n-1})=0$, откъдето съгласно индукционното предположение $\varphi_0=0$, което противоречи на условието $\varphi_0\neq 0$. С това доказателството е завършено.

50. Нека $F=F(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$ е полином, който не се променя при произволно разместване както на промен-

ливите $x_1, x_2, \dots, x_n$ помежду им, така и на променливите $y_1, y_2, \dots, y_m$. Покажете, че полиномът F може да се представи във вида

$$F(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m)=f(\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m),$$

където $\sigma_1, \sigma_2, \dots, \sigma_n$ са елементарните симетрични полиноми на променливите $x_1, x_2, \dots, x_n$, а $\tau_1, \tau_2, \dots, \tau_m$ са елементарните симетрични полиноми на $y_1, y_2, \dots, y_m$.

Решение. При доказателството, изложено в зад. 44, коефициентите на разглеждания полином могат да принадлежат на произволен пръстен. Да разгледаме полинома F като полином на променливите $y_1, y_2, \dots, y_m$ с коефициенти в пръстена от полинома на променливите $x_1, x_2, \dots, x_n$. Съгласно зад. 44 F може да се представи във вида

$$F=\sum \varphi_{i_1 i_2 \dots i_m} \tau_1^{i_1} \tau_2^{i_2} \dots \tau_m^{i_m},$$

където $\varphi_{i_1 i_2 \dots i_m}$ са полиноми на $x_1, x_2, \dots, x_n$. Но от условието следва, че тези полиноми са симетрични и следователно се изразяват чрез $\sigma_1, \sigma_2, \dots, \sigma_n$, с което доказателството е завършено.

51. Нека P е поле с характеристика 0 и $\alpha_1, \alpha_2, \dots, \alpha_n$ и $\beta_1, \beta_2, \dots, \beta_n$ са такива елементи от P, че

$$\sum_{i=1}^{n} \alpha_i^k=\sum_{i=1}^{n} \beta_i^k,$$

за $k=1, 2, \dots, n$. Покажете, че с точност до реда на записване елементите α_i съвпадат с елементите β_i. Опровергайте това твърдение в случая на поле с характеристика, различна от 0.

Решение. Условието на задачата изразява, че

$$S_k(\alpha_1, \alpha_2, \dots, \alpha_n)=S_k(\beta_1, \beta_2, \dots, \beta_n),$$

за $k=1, 2, \dots n$, откъдето съгласно зад. 49 имаме

$$\sigma_1=\tau_1, \sigma_2=\tau_2, \dots, \sigma_n=\tau_n.$$

Оттук следва, че полиномът с корени $\alpha_1, \alpha_2, \dots, \alpha_n$ съвпада с полинома с корени $\beta_1, \beta_2, \dots n, \beta_n$ и следователно α_i с точност до реда на записването съвпадат с β_i.

52. Нека $x_1, x_2, \dots, x_n$ са корени на полинома

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

Покажете, че всеки симетричен полином от $x_2, x_3, \dots, x_n$ може да се представи като полином на x_1.

Решение. Достатъчно е да се докаже твърдението за елементарните симетрични полиноми τ_i на променливите $x_2, x_3, \dots, x_n$. Нека $\tau_1, \tau_2, \dots, \tau_{n-1}$ са елементарните симетрични полиноми на $x_2, x_3, \dots, x_n$. Очевидно $\tau_k=\sigma_k-x_1\tau_{k-1}$, откъдето имаме

$$\tau_k=\sigma_k-x_1\sigma_{k-1}+x_1^2\sigma_{k-2}-\ldots+(-x_1)^{k-1}\sigma_1+(-x_1)^k,$$

$$(-1)^k\tau_k=a_k+a_{k-1}x_1+\ldots+a_1x_1^{k-1}+x_1^k.$$

53. Пресметнете $\sum_{i=1}^{n}\frac{\partial\sigma_k}{\partial x_1}$ където σ_k е k-тият елементарен симетричен полином на променливите $x_1, x_2, \ldots, x_n$.

Отг. $\sum_{i=1}^{n}\frac{\partial\sigma_k}{\partial x_i}=(n-k+1)\sigma_{k-1}$.

54. Нека

$$F=F(x_1, x_2, \ldots, x_n)=f(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

е представянето на симетричния полином F чрез елементарните симетрични полиноми. Изразете чрез елементарните симетрични полиноми полинома $\sum_{i=1}^{n}\frac{\partial F}{\partial x_i}$.

Отг. $\sum_{i=1}^{n}\frac{\partial F}{\partial x_i}=n\frac{\partial f}{\partial\sigma_1}+(n-1)\frac{\partial f}{\partial\sigma_2}\sigma_1+\ldots+\frac{\partial f}{\partial\sigma_n}\sigma_{n-1}$.

55. Нека $F(x_1, x_2, \ldots, x_n)$ е симетричен полином, за който

$$F(x_1+a, x_2+a, \ldots, x_n+a)=F(x_1, x_2, \ldots, x_n).$$

и $F=f(\sigma_1, \sigma_2, \ldots, \sigma_n)$ е представянето му чрез елементарните симетрични полиноми. Покажете, че

$$n\frac{\partial f}{\partial\sigma_1}+(n-1)\sigma_1\frac{\partial f}{\partial\sigma_2}+\ldots+\sigma_{n-1}\frac{\partial f}{\partial\sigma_n}=0$$

и обратно.

Решение. Нека

$$\varphi(a)=F(x_1+a, x_2+a, \ldots, x_n+a).$$

Тогава

$$\varphi'(a)=\sum_{i=1}^{n}\frac{\partial F(x_1+a, x_2+a, \ldots, x_n+a)}{\partial x_i}.$$

Тъй като $\varphi(a)$ не зависи от a, то $\varphi'(a)=0$, откъдето следва $\sum_{i=1}^{n}\frac{\partial F}{\partial x_i}=0$. Обратно ако $\sum_{i=1}^{n} \frac{\partial F}{\partial x_i}=0$, то

$$\varphi'(a)=\sum_{i=1}^{n} \frac{\partial F(x_1+a, \ldots, x_n+a)}{\partial x_i}=0,$$

откъдето следва, че $\varphi(a)$ не зависи от a, следователно $\varphi(a)=\varphi(0)$, т. е.

$$F(x_1+a, x_2+a, \ldots, x_n+a)=F(x, x_2, \ldots, x_n).$$

Съгласно предната задача условието $\sum_{i=1}^{n} \frac{\partial x}{\partial x_i}=0$ е еквивалентно на условието

$$n\frac{\partial f}{\partial \sigma_1}+(n-1)\sigma_1\frac{\partial f}{\partial \sigma_2}+\ldots+\sigma_{n-1}\frac{\partial f}{\partial \sigma_n}=0.$$

56. Покажете, че всеки хомогенен симетричен полином от втора степен, който притежава свойството от предната задача, има вида

$$c\sum_{i<k}(x_i-x_k)^2,$$

където c е константа.

Решение. Нека $F(x_1, x_2, \ldots, x_n)$ е хомогенен симетричен полином от втора степен. Съгласно основната теорема от теорията на симетричните полиноми F има вида

$$F=A\sigma_1^2+B\sigma_2.$$

Но от зад. 55 следва

$$n\cdot 2A\sigma_1+(n-1)B\sigma_1=0,$$

откъдето $A=(n-1)c$, $B=-2nc$ и следователно

$$F(x_1, x_2, \ldots, x_n)=c[(n-1)\sigma_1^2-2n\sigma_2]=c\sum_{i<k}(x_i-x_k)^2.$$

57. Намерете общия вид на хомогенните симетрични полиноми от трета степен, които притежават свойството от зад. 55.

Решение. Всеки хомогенен симетричен полином от трета степен има вида

$$F=A\sigma_1^3+B\sigma_1\sigma_2+C\sigma_3.$$

Съгласно зад. 55 имаме

$$3An\sigma_1^2+nB\sigma_2+(n-1)B\sigma_1^2+(n-2)C\sigma_2=0,$$

откъдето

$$F=c[(n-1)(n-2)\sigma_1^3-3n(n-2)\sigma_1\sigma_2+3n^2\sigma_3].$$

58. Изразете симетричния полином

$$F=\sum_{i<j<k}(x_i-x_j)^2(x_j-x_k)^2(x_k-x_i)^2$$

чрез елементарните симетрични полиноми, като използувате зад. 55.

Отг. $F=(n-2)\sigma_1^2\sigma_2^2-2(n-1)\sigma_1^3\sigma_3-4(n-2)\sigma_2^3+(10n-12)\sigma_1\sigma_2\sigma_3-$
$-4(n-1)\sigma_1^2\sigma_4-9n\sigma_3^2+8n\sigma_2\sigma_4$.

59. Покажете, че между симетричните полиноми F, които притежават свойството

$$F(x_1, x_2, \ldots, x_n)=F(x_1+a, x_2+a, \ldots, x_n+a),$$

съществуват $n-1$ полинома $\varphi_1, \varphi_2, \ldots, \varphi_{n-1}$, такива че всеки полином от разглеждания вид може да се изрази посредством $\varphi_1, \varphi_2, \ldots, \varphi_{n-1}$.

Решение. Може да вземем

$$\varphi_k=\sigma_{k+1}\left(x_1-\frac{\sigma_1}{n}, x_2-\frac{\sigma_1}{n}, \ldots, x_n-\frac{\sigma_1}{x}\right).$$

Очевидно всеки от полиномите φ_k притежава исканото свойство. По-нататък, ако F притежава желаното свойство и

$$F(x_1, x_2, \ldots, x_n)=f(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

е представянето на F чрез елементарните симетрични полиноми, то

$$F(x_1, x_2, \ldots, x_n)=f(0, \varphi_1, \varphi_2, \ldots, \varphi_{n-1}).$$

60. Изразете чрез полиномите φ_1, φ_2, дефинирани в решението на зад. 59, следните симетрични полиноми:

а) $F=(x_1-x_2)^2(x_1-x_3)^2(x_3-x_2)^2$;
б) $F=(x_1-x_2)^4+(x_2-x_3)^4+(x_3-x_1)^4$.

Отг. а) $F=-4\varphi_1^3-27\varphi_2^2$;
б) $F=18\varphi_1^2$.

61. Изразете чрез полиномите $\varphi_1, \varphi_2, \varphi_3$, дефинирани в решението на зад. 59, следните симетрични полиноми:

а) $F=(x_1+x_2-x_3-x_4)(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4)$;
б) $F=(x_1-x_2)^2(x_1-x_3)^2(x_1-x_4)^2(x_2-x_3)^2(x_2-x_4)^2(x_3-x_4)^2$.

Отг. а) $F=8\varphi_2$;
б) $F=-4\varphi_1^3\varphi_2^2+16\varphi_1^4\varphi_3-27\varphi_2^4+144\varphi_1\varphi_2^2\varphi_3-128\varphi_1^2\varphi_3^2+256\varphi_3^3$.

62. Нека $F(x_1, \ldots, x_n)$ е полином, за който

$$F(x_{i_1}, x_{i_2}, \ldots, x_{i_n})=(-1)^{[i_1 i_2 \ldots i_n]}F(x_1, x_2, \ldots, x_k)$$

при произволна пермутация $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ на променливите $x_1, x_2, \ldots, x_n$ (в такъв случай полиномът F се нарича алтернативен). Покажете, че F се представя във вида

$$F=\Delta G,$$

където $\Delta=\prod_{i<j}(x_i-x_j)$, а полиномът G е симетричен.

Решение. От условието на задачата следва, че

$$F=(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n)=-F(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n);$$

в частност при $x_i=x_j$ получаваме

$$F(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n)=0,$$

откъдето следва, че полиномът F се дели на x_i-x_j. Тъй като това е вярно за всяка двойка $i, j, i\neq j$, F ще се дели на произведението $\Delta=\prod_{i<j}(x_i-x_j)$. Но това произведение също е алтернативен полином, откъдето следва, че частното $G=\frac{F}{\Delta}$ е симетричен полином.

63. Полиномът $F(x_1, x_2, \ldots, x_n)$ се нарича *двузначен*, ако не променя стойността си при произволна четна пермутация на променливите, т. е. ако

$$F(x_{i_1}, x_{i_2}, \ldots, x_{i_n})=F(x_1, x_2, \ldots, x_n)$$

при произволна четна пермутация $i_1, i_2, \ldots, i_n$ на индексите 1, 2, ..., n. Да се докаже, че полиномът F е двузначен тогава и само тогава, когато може да се представи във вида

$$F=G+\Delta H,$$

където H и G са симетрични полиноми, а Δ е полиномът, дефиниран в предната задача.

Решение. Тъй като полиномът Δ не се променя при четни пермутации на променливите, ясно е, че всеки полином от вида $G+\Delta H$, където G и H са симетрични, е двузначен. Обратно, нека F е двузначен полином. Ще покажем, че ако $i_1, i_2, \ldots, i_n$ е произволна нечетна пермутация, полиномът

$$\bar{F}(x_1, \ldots, x_n)=F(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$$

не зависи от избора на тази пермутация (този факт оправдава наименованието „двузначен"). Действително нека $j_1, j_2, \ldots, j_n$ е обратната пермутация на разглежданата, $k_1, k_2, \ldots, k_n$ е произволна друга нечетна пермутация и $l_1, l_2, \ldots, l_n$ е произведението на $k_1, k_2, \ldots, k_n$ с $j_1, j_2, \ldots, j_n$. Тогава от

$$F(x_{i_1}, x_{i_2}, \ldots, x_{i_n})\neq F(x_{k_1}, x_{k_2}, \ldots, x_{k_n})$$

ще последва

$$F(x_1, x_2, \ldots, x_n)\neq F(x_{l_1}, x_{l_2}, \ldots, x_{l_n}),$$

което е невъзможно, защото пермутацията $l_1, l_2, \ldots, l_n$ е четна.

Сега да положим $G=\frac{1}{2}(F+\bar{F})$ и $h=\frac{1}{2}(F-\bar{F})$. Лесно се вижда, че полиномът G е симетричен, а h — алтернативен. Съгласно предната задача $h=\Delta H$, H — симетричен. Равенството

$$F=G+\Delta H$$

е очевидно.

§ 2. РЕЗУЛТАНТА. ДИСКРИМИНАНТА

Нека

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

и

$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m$$

са два полинома с коефициенти от дадено поле P. С $\alpha_1, \alpha_2, \ldots, \alpha_n$, съответно $\beta_1, \beta_2, \ldots, \beta_m$, да означим корените на $f(x)$ и $g(x)$. (Корените α_i и β_j принадлежат на подходящо разширение на полето P.) Изразът

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

$(i=1, 2, \ldots, n, j=1, 2, \ldots, m)$ се нарича *резултанта на полиномите* $f(x)$ и $g(x)$.

Като симетрична функция на α_i и β_j съгласно основната теорема за симетричните полиноми резултантата $R(f, g)$ се изразява като цяла рационална функция от коефициентите на $f(x)$ и $g(x)$ и е елемент на основното поле P.

Анулирането на резултантата $R(f, g)$ е необходимо и достатъчно, за да имат уравненията $f(x)=0$ и $g(x)=0$ общ корен.

Резултантата може да се представи във вида

$$R(f, g)=a_0^m g(\alpha_1)\, g(\alpha_2) \ldots g(\alpha_n),$$

или още така:

$$R(f, g)=(-1)^{mn} b_0^n f(\beta_1) f(\beta_2) \ldots f(\beta_m).$$

Ясно е, че

$$R(f, g)=(-1)^{mn} R(g, f).$$

Формула на Силвестър. Резултантата $R(f, g)$ се представя в явен вид чрез коефициентите на полиномите $f(x)$ и $g(x)$ в следната детерминантна форма:

$$R(f, g)=\begin{vmatrix} a_0 & a_1 & a_2 & \ldots & a_n & & & \\ & a_0 & a_1 & a_2 & \ldots & a_n & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\ & & & a_0 & a_1 & a_2 & \ldots & a_n \\ b_0 & b_1 & b_2 & \ldots & b_m & & & \\ & b_0 & b_1 & b_2 & \ldots & b_m & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & & b_0 & b_1 & b_2 & \ldots & b_m \end{vmatrix}$$

Система от две алгебрични уравнения с две неизвестни. Нека $f(x; y)$ и $g(x, y)$ са два полинома на променливите x, y и да разгледаме системата

$$(1) \qquad \begin{cases} f(x, y)=0 \\ g(x, y)=0. \end{cases}$$

Всеки един от полиномите $f(x, y)$ и $g(x, y)$ може да се представи като полином на x с коефициенти, които са полиноми на y:

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

Нека $R_y(f, g)$ е резултантата на полиномите $f(x, y)$ и $g(x, y)$, разглеждани като полиноми на x. Очевидно $\varphi(y)=R_y(f, g)$ ще представлява полином на y. Ако (α, β) е решение на системата (1), уравненията $f(x, \beta)=0$ и $g(x, \beta)=0$ ще имат общ корен $x=\alpha$ и следователно $\varphi(\beta)=0$. Обратно, ако β е корен на алгебричното уравнение $\varphi(y)=0$ и старшите коефициенти $a_0(y)$ и $b_0(y)$ не се анулират едновременно за $y=\beta$, уравненията $f(x, \beta)=0$ и $g(x, \beta)=0$ ще имат корен $x=\alpha$, откъдето получаваме решението (α, β) на системата (1). В случая дадената система (1) се сведе до решаване на алгебрични уравнения с едно неизвестно чрез елиминация на x. (Разбира се, когато това е по-целесъобразно, можем да елиминираме y и тогава вместо резултантата $R_y(f, g)$ ще разглеждаме резултантата $\psi(x)=R_x(f, g)$ на полиномите $f(x, y)$ и $g(x, y)$, считайки ги като полиноми на y.)

Дискриминанта. Нека

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n \in P[x]$$

е полином на x и $\alpha_1, \alpha_2,\ldots,\alpha_n$ да означават корените на уравнението $f(x)=0$. Изразът

$$D(f)=a_0^{2n-2}\prod_{i>j}(\alpha_i-\alpha_j)^2$$

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

Като симетрична функция на корените α_i дискриминантата $D(f)$ се изразява във вид на полином от коефициентите на $f(x)$ и следователно е елемент от основното поле P.

Анулирането на дискриминантата $D(f)$ е необходимо и достатъчно условие, за да има уравнението $f(x)=0$ кратни корени.

Дискриминантата може да се представи още така:

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

В сила е още формулата

$$D(f)=a_0^{2n-2}\begin{vmatrix} n & S_1 & S_2 & \ldots & S_{n-1} \\ S_1 & S_2 & S_3 & \ldots & S_n \\ \vdots & \vdots & \vdots & & \vdots \\ S_{n-1} & S_n & S_{n+1} & \ldots & S_{2n-2} \end{vmatrix},$$

където $S_k=\alpha_1^k+\ldots+\alpha_n^k$, $k=1, 2, \ldots$, са степенните сборове от корените на уравнението $f(x)=0$.

Връзка между дискриминанта и резултанта. Между дискриминантата $D(f)$ и резултантата $R(f, f')$ на полинома $f(x)$ и неговата производна $f'(x)$ е в сила следната зависимост:

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

Примери. За дискриминантата D на квадратния тричлен

$$f(x)=ax^2+bx+c$$

получаваме

$$D=-a^{-1}R(f, f')=-a^{-1}\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix}=-a^{-1}(-ab^2+4a^2c),$$

т. е. $D=b^2-4ac$.

За дискриминантата D на кубичния полином

$$x^3+ax^2+bx+c$$

получаваме

$$D=\begin{vmatrix} 3 & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{vmatrix}$$

и като пресметнем степенните сборове S_k и заместим в горната детерминанта, ще имаме

$$D=a^2b^2-4b^3-4a^3c+18abc-27c^2.$$

В частност за дискриминантата D на кубичния тричлен

$$x^3+px+q$$

получаваме

$$D=-4p^3-27q^2.$$

1. Пресметнете резултантата $R(f, g)$ на полиномите $f(x)$ и $g(x)$, където:

а) $f(x)=3x^2+x-2$;
$g(x)=x^2-2x-2$;
б) $f(x)=x^3+2x^2+2x-2$;
$g(x)=x^2-2x+4$;
в) $f(x)=x^3-3x^2+2x+1$;
$g(x)=2x^2-x-1$;
г) $f(x)=2x^3-3x^2+2x+1$;
$g(x)=x^2+x+3$;

д) $f(x)=2x^4-x^3+3;$
$g(x)=3x^3-x^2+4;$
е) $f(x)=x^4-2x^3-3x+4;$
$g(x)=2x^3-3x^2-x-2.$

Отг. а) -26; б) 252; в) -7; г) 247; д) 4854; е) 0.

2. Пресметнете резултантата $R(f, g)$ на полиномите

$$f(x)=a_0x^2+a_1x+a_2 \text{ и } g(x)=b_0x^2+b_1x+b_2.$$

Отг. $(b_0a_2-b_2a_0)^2-(b_0a_1-b_1a_0)(b_1a_2-b_2a_1)$.

3. Пресметнете резултантата на полиномите

$$f(x)=x^3+px+q \text{ и } g(x)=x^3+mx+n.$$

Решение. Нека $\alpha_1, \alpha_2, \alpha_3$ са корените на полинома $f(x)$. Тогава

$$R(f, g)=g(\alpha_1)g(\alpha_2)g(\alpha_3)=(\alpha_1^3+m\alpha_1+n)(\alpha_2^3+m\alpha_2+n)(\alpha_3^3+m\alpha_3+n)=(\alpha_1\alpha_2\alpha_3)^3+$$
$$+m\alpha_1\alpha_2\alpha_3\sum\alpha_1^2\alpha_2^2+m^2\alpha_1\alpha_2\alpha_3\sum\alpha_1^2+mn\sum\alpha_1^3\alpha_2+n\sum\alpha_1^3\alpha_2^3+m^3\alpha_1\alpha_2\alpha_3+n^2\sum\alpha_1^3+$$
$$+m^2n\sum\alpha_1\alpha_2+mn^2\sum\alpha_1+n^3.$$

За фигуриращите симетрични полиноми на $\alpha_1, \alpha_2, \alpha_3$ имаме

$$\sum\alpha_1^2\alpha_2^2=\frac{1}{2}(S_2^2-S_4)=p^2,$$
$$\sum\alpha_1^2=-2p, \quad \sum\alpha_1^3=-3q,$$
$$\sum\alpha_1^3\alpha_2=S_1S_3-S_4=-2p^2,$$
$$\sum\alpha_1^3\alpha_2^3=\frac{1}{2}(S_3^2-S_6)=3q^2+p^3,$$
$$\sum\alpha_1\alpha_2=p,$$
$$\sum\alpha_1=0, \quad \alpha_1\alpha_2\alpha_3=-q.$$

Като ги заместим в израза за R, получаваме
$$R(f, g)=-q^3-qp^2m+2m^2pq-2p^2mn+3q^2n+p^3n-qm^3-3n^2q+m^2np+n^3.$$

4. Намерете стойностите на параметъра λ, при които полиномите

$$f(x)=x^3-\lambda x+2 \text{ и } g(x)=x^2+\lambda x+2$$

имат общи корени.

Решение. Очевидно търсените стойности на λ ще анулират резултантата $R(f, g)$ на полиномите $f(x)$ и $g(x)$. Имаме

$$R(f, g)=-4(\lambda^3-\lambda^2-5\lambda-3).$$

Корените на уравнението $R(f, g)=0$ са $\lambda_1=3$, $\lambda_2=\lambda_3=-1$. Следователно полиномите $f(x)$ и $g(x)$ имат общи корени само при $\lambda=-1$ и $\lambda=3$. Да намерим тези общи корени.

Нека $\lambda=-1$. Тогава полиномите приемат вида

$$f(x)=x^3+x+2 \text{ и } g(x)=x^2-x+2.$$

Общите корени на $f(x)$ и $g(x)$ са корените на най-големия им общ делител, който в случая съвпада с $g(x)$. Следователно общите корени са $x_1=\frac{1}{2}(1+i\sqrt{7})$ и $x_2=\frac{1}{2}\cdot(1-i\sqrt{7})$.

При $\lambda=3$ намираме един общ корен $x=-2$.

5. Намерете при какви стойности на параметъра λ полиномите $f(x)$ и $g(x)$ имат общи корени и пресметнете тези общи корени, където:

а) $f(x)=x^2-(7\lambda+4)x+4\lambda^2+20\lambda$, $g(x)=x^2-(14\lambda+6)x+9\lambda^2+42\lambda$;

б) $f(x)=x^2-3x+\lambda^2-\lambda$, $g(x)=x^2+(6\lambda-7)x-\lambda^2-11\lambda+12$;

в) $f(x)=x^3-6\lambda x^2+11\lambda x-6\lambda$, $g(x)=x^3-\lambda x^2-4\lambda x+4\lambda$;

г) $f(x)=x^3+\lambda x^2-9$, $g(x)=x^3+\lambda x-3$;

д) $f(x)=x^3-2x^2-6x+8-\lambda$, $g(x)=2x^3-8x^2+5x+2-\lambda$;

е) $f(x)=x^4+3\lambda x^2+4x+12$, $g(x)=x^3+\lambda x^2+4$;

ж) $f(x)=x^3+3x^2+2x+\lambda$, $g(x)=x^3-3x+2$;

з) $f(x)=x^3-2\lambda x+\lambda^3$, $g(x)=x^2+\lambda^2-2$;

и) $f(x)=x^3-5x^2-9\lambda x+5$, $g(x)=3x^2-10x-9\lambda$.

6. Намерете стойностите на параметрите λ и, μ, при които полиномите

$$f(x)=x^3+5x^2+\lambda x+2,$$
$$g(x)=x^3+\mu x-8$$

имат два общи корена.

Решение. Очевидно полиномите $f(x)$ и $g(x)$ ще имат два общи корена тогава и само тогава, когато най-големият им общ делител е от втора степен. Като приложим алгоритъма на Евклид, получаваме остатъци

$$r(x)=5x^2+(\lambda-\mu)+10, \quad r_1(x)=[5\mu-10+\frac{1}{5}(\lambda-\mu)^2]x+2(\lambda-\mu)-40.$$

За да бъде изпълнено условието $(f(x), g(x))=r(x)$, е необходимо и достатъчно $r_1(x)=0$, т. е.

$$\left| \begin{array}{l} 5\mu-10+\frac{1}{5}(\lambda-\mu)^2=0 \\ 2(\lambda-\mu)-40=0. \end{array} \right.$$

Като решим получената система, намираме $\lambda=6$, $\mu=-16$.

Да намерим общите корени на полиномите при получените стойности на λ и μ. За това е достатъчно да решим уравнението

$$5x^2+20x+10=0,$$

откъдето намираме $x_1=-2-\sqrt{2}$, $x_2=-2+\sqrt{2}$.

Второ решение. За да имат двата полинома два общи корена, е необходимо и достатъчно те да могат да се представят във вида

$$x^3+5x^2+\lambda x+2=(x^2+px+q)(x+\alpha),\quad x^3+\mu x-8=(x^2+px+q)(x+\beta).$$

Коефициентите $p,\ q,\ \alpha,\ \beta,\ \lambda,\ \mu$ намираме от системата

$$\begin{aligned} p+\alpha&=5, & p+\beta&=0,\\ q+p\alpha&=\lambda, & q+p\beta&=\mu,\\ q\alpha&=2, & q\beta&=-8, \end{aligned}$$

откъдето получаваме $p=4,\ \ q=2,\ \ \alpha=1,\ \ \beta=-4,\ \ \lambda=6,\ \ \mu=-14.$

7. Намерете стойностите на параметрите λ и μ, при които полиномите $f(x)$ и $g(x)$ имат два общи корена, където:

а) $f(x)=x^3-6x^2+\lambda x-3,\quad g(x)=x^3-x^2+\mu x+2;$
б) $f(x)=x^3-4x^2+5\lambda x+\mu,\quad g(x)=x^3-2x^2-\lambda x-\mu;$
в) $f(x)=x^3+\lambda x+\mu,\quad g(x)=\mu x^3+\lambda x^2+1;$
г) $f(x)=x^4-\lambda x^3-2x^2-2x-\mu,\ g(x)=x^4-\lambda x^3-5x^2+4x+2\mu.$

Отг. а) $\lambda=10,\ \mu=-5;$ б) $\lambda=\mu=0;\ \lambda=-\frac{7}{9},\ \ \mu=0;\ \lambda=1,\ \mu=-2;$ в) $\lambda=\pm 1,$ $\mu=0;\ \ \lambda=1-\mu^2,\ \ \mu\neq 0;$ г) $\lambda=2,\ \ \mu=3;\ \ \lambda=\frac{1}{2},\ \ \mu=\frac{1}{2}.$

8. Намерете резултантата на полиномите

$$\begin{aligned} f(x)&=a_0x^n+a_1x^{n-1}+\ .\ .\ .\ +a_n,\\ g(x)&=a_0x^{n-1}+a_1x^{n-2}+\ .\ .\ .\ +a_{n-1}. \end{aligned}$$

Решение. Нека $\alpha_1,\ \alpha_2,\dots,\alpha_n$ са корените на полинома $f(x)$. Тогава

$$R(f,\ g)=a_0^{n-1}g(\alpha_1)g(\alpha_2)\dots g(\alpha_n).$$

Но

$$\varphi(\alpha_i)=a_0\,\alpha_i^{n-1}+\dots+\alpha_{n-1}=\frac{1}{\alpha_i}[f(\alpha_i)-a_n]=-\frac{a_n}{\alpha_i}.$$

Следователно

$$R(f,\ g)=a_0^n\,a_n^{n-1}$$

9. Намерете резултантата на полиномите

$$\begin{aligned} f(x)&=x^n+x^{n-1}+\dots+x+1,\\ g(x)&=x^n-1. \end{aligned}$$

Отг. $R(f,\ g)=(-1)^n\,(n+1.$

10. Намерете резултантата на полиномите

$$\begin{aligned} f(x)&=x^n+x^{n-1}+\dots+x^2+x+1,\\ g(x)&=x^{n+1}-ax^n-x+a. \end{aligned}$$

Отг. $R(f,\ g)=(n+1)(1+a+a^2+\dots+a^n.)$

11. Нека $f(x)$, $g_1(x)$ и $g_2(x)$ са полиноми. Докажете, че

$$R(f,\ g_1g_2)=R(f,\ g_1)R(f,\ g_2).$$

Решение. Нека $f(x)=a_0(x-x_1)(x-x_2)\dots(x-x_n)$, $g_1(x)=b_0x^k+$ $+b_1x^{k-1}+\dots+b_k,$ $g_2(x)=c_0x^m+c_1x^{m-1}+\dots+c_m.$

Тогава имаме $R(f,\ g_1g_2)=a_0^{k+m}\prod_{i=1}^{n}g_1(x_i)g_2(x_i)=\left[a_0^k\prod_{i=1}^{n}g_1(x_i)\right]\left[a_0^m\prod_{i=1}^{n}g_2(x_i)\right]=$ $=R(f,\ g_1)R(f,\ g_2).$

12. Намерете резултантата на полиномите $\Phi_n(x)$ и x^m-1, където $\Phi_n(x)$ е n-тият циклотомичен полином, т. е. полиномът, чиито корени са всички примитивни корени от n-та степен от единицата.

Решение. Интересно е да разгледаме само случая, когато $n>2$. Нека $d=(m, n)$, $\xi_1, \xi_2, \ldots$ са примитивните корени на единицата от степен n, а $\eta_1, \eta_2, \ldots$, са примитивните корени от единицата от степен $n_1=\frac{n}{d}$. Тогава имаме

$$R(\Phi_n, x^m-1)=\prod(\xi_i^m-1)=\prod(1-\xi_i^m)=\left[\prod(1-\eta_i)\right]^{\frac{\varphi(n)}{\varphi(n_1)}}=\left[\Phi_{n_1}(1)\right]^{\frac{\varphi(n)}{\varphi(n_1)}}.$$

Ако n дели m, то $R(\Phi_n, x^m-1)=0$. Нека n не дели m. Тогава $n_1\neq 1$ и съгласно зад. 33, §4, гл. VIII имаме $\Phi_{n_1}(1)=1$ при $n_1\neq p^\lambda$ и $\Phi_{n_1}(1)=p$ при $n_1=p^\lambda$ (p — просто число). И така

$$R(\Phi_n, x^m-1)=0 \text{ при } n_1=\frac{n}{d}=1;$$

$$R(\Phi_n, x^m-1)=p^{\frac{\varphi(n)}{\varphi(n_1)}} \text{ при } n_1=\frac{n}{d}=p^\lambda;$$

$$R(\Phi_n, x^m-1)=1 \text{ в останалите случаи.}$$

13. Намерете резултантата на полиномите $\Phi_n(x)$ и $\Phi_m(x)$.

Решение. При $n=m$, $R(\Phi_n, \Phi_m)=0$. Нека $n\neq m$. Ще покажем, че $R(\Phi_n, \Phi_m)$ е цяло положително число, което дели както $R(\Phi_n, x^m-1)$, така и $R(\Phi_m, x^n-1)$. Че $R(\Phi_n, \Phi_m)$ е цяло число, е очевидно. Имаме $x^m-1=\prod\limits_{d|m}\Phi_d(x)$, откъдето съгласно зад. 11, $R(\Phi_n, x^m-1)=\prod R(\Phi_n, \Phi_d)$. Оттук вече следва, че $R(\Phi_n, \Phi_m)$ дели $R(\Phi_n, x^m-1)$. Освен това, ако допуснем, че сме доказали, че резултантите $R(\Phi_n, \Phi_d)$ са положителни за всички собствени делители d на m, от това следва, че и $R(\Phi_n, \Phi_m)$ е положителна. По същия начин се вижда, че и $R(\Phi_m, \Phi_n)$ дели $R(\Phi_m, x^n-1)$.

Нека $d'=(n, m)$. Ако $n\nmid m$, $m\nmid n$, числата $\frac{m}{d'}$ и $\frac{n}{d'}$ са взаимно прости и различни от единица. Съгласно предната задача $R(\Phi_n, x^m-1)$ и $R(\Phi_m, x^n-1)$ са взаимно прости, откъдето $R(\Phi_n, \Phi_m)=1$.

Остава да се разгледа случаят, когато едно от числата n и m дели другото. Нека например n/m. Ако $\frac{m}{n}$ не е степен на просто число, съгласно предната задача $R(\Phi_m, x^n-1)=1$ и следователно $R(\Phi_m, \Phi_n)=1$. Нека накрая $m=np^\lambda$, p — просто число. Съгласно зад. 31, §4, гл. VIII имаме $\Phi_n(x)=\prod\limits_{\delta|n}(x^\delta-1)^{\mu\left(\frac{n}{\delta}\right)}$, откъдето съгласно зад. 11 имаме

$$R(\Phi_m, \Phi_n)=\prod_{\delta|n}R\left(\Phi_m, (x^\delta-1)^{\mu\left(\frac{n}{\delta}\right)}\right).$$

Всички множители отдясно освен тези, за които $\frac{m}{\delta}$ е степен на p, са равни на 1.

Ако n не се дели на p, остава само един различен от 1 множител, именно $R(\Phi_m, x^\delta-1)$; следователно

$$R(\Phi_m, \Phi_n)=R(\Phi_m(x^n-1)=p^{\frac{\varphi(m)}{\varphi(m:n)}}=p^{\varphi(n)}.$$

Ако n се дели на p, остават два различни от единица множителя, които се получават при $\delta=n$ и $\delta=\frac{n}{p}$, откъдето $R(\Phi_m, \Phi_n)=\dfrac{R(\Phi_m, x^n-1)}{R(\Phi_m, x^{\frac{n}{p}}-1)}=$

$$=p^{\frac{\varphi(m)}{\varphi(m:n)}-\frac{\varphi(m)}{\varphi(mp:n)}}=p^{\varphi(n)}.$$

И така:

$$R(\Phi_m, \Phi_n)=0 \qquad \text{при } n=m;$$

$$R(\Phi_m, \Phi_n)=p^{\varphi(n)} \text{ при } m=np^\lambda, \quad p\text{ — просто};$$

$$R(\Phi_m, \Phi_n)=1 \qquad \text{в останалите случаи.}$$

14. Докажете, че резултантата на два полинома

$$f(x)=x^n+a_1x^{n-1}+\ldots+a_n,$$
$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m$$

е равна на детерминантата, образувана от коефициентите на остатъците при деление на полиномите $g(x), xg(x), \ldots, x^{n-1}g(x)$ с $f(x)$. (*Метод на Хермит.*)

Решение. Нека $f(x)=(x-x_1)(x-x_2)\ldots(x-x_n)$. По-нататък нека

$$x^{k-1}g(x)=f(x)q_k(x)+r_k(x)$$

и

$$r_k(x)=c_{k1}+c_{k2}x+\ldots+c_{kn}x^{n-1}.$$

Очевидно коефициентите c_{kl} представляват някакви полиноми от $x_1, x_2, \ldots, x_n$. По-нататък имаме

$$\begin{vmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{vmatrix} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} = \begin{vmatrix} r_1(x_1) & r_1(x_2) & \ldots & r_1(x_n) \\ r_2(x_1) & r_2(x_2) & \ldots & r_2(x_n) \\ \ldots & \ldots & \ldots & \ldots \\ r_n(x_1) & r_n(x_2) & \ldots & r_n(x_n) \end{vmatrix} =$$

$$= \begin{vmatrix} g(x_1) & g(x_2) & \ldots & g(x_n) \\ x_1g(x_1) & x_2g(x_2) & \ldots & x_ng(x_n) \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1}g(x_1) & x_2^{n-1}g(x_2) & \ldots & x_n^{n-1}g(x_n) \end{vmatrix} =$$

$$=g(x_1)g(x_2)\ldots g(x_n) \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix},$$

откъдето следва

$$\begin{vmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{vmatrix} = g(x_1)g(x_2)\ldots g(x_n)=R(f, g).$$

15. Докажете, че резултантата на полиномите

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n,$$
$$g(x)=b_0x^n+b_1x^{n-1}+\ldots+b_n$$

е равна на детерминантата, образувана от коефициентите на полиномите от степен, ненадминаваща $n-1$:

$$\varphi_k(x)=(a_0x^{k-1}+a_1x^{k-2}+\ldots+a_{k-1})g(x)-(b_0x^{k-1}+b_1x^{k-2}+\ldots+b_{k-1})f(x),$$

$k=1, 2, \ldots, n$ (*метод на Безу*).

Решение. Първо ще покажем, че степените на полиномите $\varphi_k(x)$ не надминават $n-1$. Да въведем следните означения:

$$f_k(x)=a_0x^{k-1}+\ldots+a_{k-1},$$
$$\overline{f}_k(x)=a_kx^{n-k}+\ldots+a_n,$$
$$g_k(x)=b_0x^{k-1}+\ldots+b_{k-1},$$
$$\overline{g}_k(x)=b_kx^{n-k}+\ldots+b_n.$$

Тогава

$$f(x)=x^{n-k+1}f_k(x)+\overline{f}_k(x),$$
$$g(x)=x^{n-k+1}g_k(x)+\overline{g}_k(x).$$

$$\varphi_k(x)=f_k(x)(x^{n-k+1}g_k(x)+\overline{g}_k(x))-g_k(x)(x^{n-k+1}f_k(x)+\overline{f}_k(x))=$$
$$=f_k(x)\overline{g}_k(x)-g_k(x)\overline{f}_k(x)=(a_0b_k-b_0a_k)x^{n-1}+\ldots$$

Нека $\varphi_k(x)=c_{k1}c_{k2}x+\ldots+c_{kn}x^{n-1}$ и $x_1, x_2, \ldots, x_n$ са корените на полинома $f(x)$. Имаме

$$\begin{vmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{vmatrix} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} = \begin{vmatrix} \varphi_1(x_1) & \varphi_1(x_2) & \ldots & \varphi_1(x_n) \\ \varphi_2(x_1) & \varphi_2(x_2) & \ldots & \varphi_2(x_n) \\ \ldots & \ldots & \ldots & \ldots \\ \varphi_n(x_1) & \varphi_n(x_2) & \ldots & \varphi_n(x_n) \end{vmatrix} =$$

$$= \begin{vmatrix} f_1(x_1)g(x_1) & f_1(x_2)g(x_2) & \ldots & f_1(x_n)g(x_n) \\ f_2(x_1)g(x_1) & f_2(x_2)g(x_2) & \ldots & f_2(x_n)g(x_n) \\ \ldots & \ldots & \ldots & \ldots \\ f_n(x_1)g(x_1) & f_n(x_2)g(x_2) & \ldots & f_n(x_n)g(x_n) \end{vmatrix} =$$

$$=g(x_1)g(x_2)\ldots g(x_n)\begin{vmatrix} f_1(x_1) & f_2(x_2) & \ldots & f_1(x_n) \\ f_2(x_1) & f_2(x_2) & \ldots & f_2(x_n) \\ \ldots & \ldots & \ldots & \ldots \\ f_n(x_1) & f_n(x_2) & \ldots & f_n(x_n) \end{vmatrix} =$$

$$=g(x_1)g(x_2)\ldots g(x_n)\begin{vmatrix} a_0 & 0 & \ldots & 0 \\ a_1 & a_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{n-1} & a_{n-2} & \ldots & a_0 \end{vmatrix} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} =$$

$$=a_0^n g(x_1)g(x_2)\ldots g(x_n)\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix},$$

откъдето следва

$$\begin{vmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{vmatrix} = a_0^n g(x_1) g(x_2) \dots g(x_n) = R(f,\ g)$$

16. Нека $f(x)=a_0+a_1x+\dots+a_nx^n$ и $g(x)=b_0+b_1x+\dots+b_mx^m$ са два полинома. Да положим

$$\Delta_1(f,\ g)=\begin{vmatrix} 0 & 0 & 0\dots 0 & a_0 & a_1\dots a_n \\ 0 & 0 & 0\dots a_0 & a_1 & a_2\dots 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_0 & a_1 & a_2 \dots & \dots & 0 \\ b_0 & b_1 & b_2 \dots & \dots & 0 \\ 0 & b_0 & b_1 \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0\dots & b_0 & b_1\dots b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}0\\0\\0\\0\end{matrix}}\right\} m \text{ реда} \\ , \\ \left.\vphantom{\begin{matrix}0\\0\\0\\0\end{matrix}}\right\} n \text{ реда} \end{matrix}$$

$$\Delta_2(f,\ g)=\begin{vmatrix} 0 & 0\dots 0 & a_0 & a_1 & a_2\dots a_n \\ 0 & 0\dots a_0 & a_1, & a_2 & a_3\dots 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 \dots & \dots & \dots & 0 \\ b_1 & b_2 \dots & \dots & \dots & 0 \\ b_0 & b_1 \dots & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & b_0 & b_1 \dots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}0\\0\\0\\0\end{matrix}}\right\} m-1 \text{ реда} \\ \left.\vphantom{\begin{matrix}0\\0\\0\\0\end{matrix}}\right\} n-1 \text{ реда} \end{matrix}$$

и т. н. до $\Delta_p(f,g)$, където $p=\min(m,\ n)$. Детерминантата $\Delta_{k+1}(f,g)$ се получава от $\Delta_k(f,\ g)$ чрез зачеркване на първия и последния ред и на първия и последния стълб. Докажете, че за да имат полиномите $f(x)$ и $g(x)$ точно k общи корена $(0\leq k\leq p)$, е необходимо и достатъчно да са изпълнени условията:

$$\Delta_1(f,\ g)=\Delta_2(f,\ g)=\dots=\Delta_k(f,\ g)=0,\ \Delta_{k+1}(f,\ g)\neq 0.$$

Решение. Ясно е, че с точност до знак $\Delta_1(f,\ g)$ съвпада с резултантата $R(f,\ g)$ на полиномите $f(x)$ и $g(x)$. Ще покажем, че ако ξ е какъв да е общ корен на $f(x)$ и $g(x)$ и $f(x)=(x-\xi)\varphi(x)$, $g(x)=(x-\xi)\psi(x)$, то $\Delta_1(\varphi,\ \psi)=\Delta_2(f,\ g)$. За простота ще предположим, че $n=4$, $m=3$, от което доказателството няма да пострада. Нека

$$\varphi(x)=\alpha_0+\alpha_1x+\alpha_2x^2+\alpha_3x^3,\quad \psi(x)=\beta_0+\beta_1x+\beta_2x^2,$$

откъдето получаваме

$$a_0=\xi\alpha_0,\ a_1=\alpha_0+\xi\alpha_1,\ a_2=\alpha_1+\xi\alpha_2,\ a_3=\alpha_2+\xi\alpha_3,$$
$$a_4=\alpha_3,\ b_0=\xi\beta_0,\ b_1=\beta_0+\xi\beta_1,\ b_2=\beta_1+\xi\beta_2,\ b_3=\beta_2.$$

Имаме

$$\Delta_1(\varphi, \psi)=\begin{vmatrix} 0 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 0 \\ \beta_0 & \beta_1 & \beta_2 & 0 & 0 \\ 0 & \beta_0 & \beta_1 & \beta_2 & 0 \\ 0 & 0 & \beta_0 & \beta_1 & \beta_2 \end{vmatrix}.$$

Като умножим втория стълб с ξ и го прибавим към първия, след това умножим третия с ξ и го прибавим към втория и направим същото с четвъртия и петия, получаваме

$$\Delta_1(\varphi, \psi)=\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_3 & a_4 & 0 \\ b_1 & b_2 & b_3 & 0 & 0 \\ b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 \end{vmatrix}=\Delta_2(f, g).$$

И така $\Delta_1(\varphi, \psi)=\Delta_2(f, g)$. По същия начин се установяват и равенствата $\Delta_k(\varphi, \psi)=\Delta_{k+1}(f, g)$. Сега твърдението се доказва лесно с индукция по броя k на общите корени на $f(x)$ и $g(x)$. Ако $k=0$, имаме $\Delta_1(f, g)\neq 0$ и всичко е доказано. При $k>0$ нека ξ е един общ корен и $\varphi(x)$, $\psi(x)$ са полиномите, разгледани по-горе. Имаме

$$\Delta_1(\varphi, \psi)=\Delta_2(\varphi, \psi)=\ldots=\Delta_{k-1}(\varphi, \psi)=0,\ \Delta_k(\varphi, \psi)\neq 0,$$

откъдето

$$\Delta_2(f, g)=\Delta_3(f, g)=\ldots=\Delta_k(f, g)=0,\ \Delta_{k+1}(f, g)\neq 0.$$

Освен това и $\Delta_1(f, g)=0$, понеже $f(x)$ и $g(x)$ имат общи корени, с което доказателството е завършено.

17. Като използувате предната задача, определете колко общи корена имат полиномите $f(x)$ и $g(x)$, където

а) $f(x)=2x^3+x^2+x+1, \quad g(x)=3x^3+2x^2+2x-1;$

б) $f(x)=2x^4+x^3+2x+1, \quad g(x)=x^5-2x^4+2x^3+x^2-2x+2;$

в) $f(x)=x^4+3x^3+x^2-3x-2, \quad g(x)=x^4+3x^3+3x^2+3x+2.$

Отг. а) 2; б) 3; в) 2

18. Решете системата уравнения

$$\begin{cases} f(x, y)=y^2-7xy+4x^2+13x-2y-3=0 \\ g(x, y)=y^2-14xy+9x^2+28x-4y-5=0. \end{cases}$$

Решение. Нека (x_0, y_0) е произволно решение на системата. Тогава полиномите $f(x_0, y)$ и $g(x_0, y)$ имат общ корен y_0, следователно тяхната резултанта $R(x)$ (която се получава, като разглеждаме дадените полиноми като полиноми на y с коефициенти полиноми на x) се анулира при $x=x_0$. Обратно, ако за някое x_0 имаме $R(x_0)=0$, то уравненията $f(x_0, y)=0$ и $g(x_0, y)=0$ ще имат общ корен y_0 и тогава (x_0, y_0) ще бъде решение на дадената система. Следователно, за да решим системата, първо трябва да решим уравнението $R(x)=0$ и след това за всеки негов корен x_0 да намерим общите корени на полиномите $f(x_0, y)$, $g(x_0, y)$. Имаме

$$R(x)=\begin{vmatrix} 1 & -7x-2 & 4x^2+13x-3 & 0 \\ 0 & 1 & -7x-2 & 4x^2+13x-3 \\ 1 & -14x-4 & 9x^2+28x-5 & 0 \\ 0 & 1 & -14x-4 & 9x^2+28x-5 \end{vmatrix}$$

или, като пресметнем детерминантата, получаваме

$$R(x)=-24x(x+2)(x^2-3x+2).$$

Корените на полинома $R(x)$ са $x_1=0$, $x_2=-2$, $x_3=1$, $x_4=2$. За всеки от тях намираме общите корени на уравненията $f(x, y)=0$, $g(x, y)=0$.

При $x=0$ общ корен е $y=-1$; при $x=-2$, $y=1$; при $x=1$, $y=2$; при $x=2$, $y=3$.

И така решенията на системата са $(0, -1)$, $(-2, 1)$, $(1, 2)$, $(2, 3)$.

19. Решете системите уравнения;

а) $\begin{cases} 11x^2+36xy+30y^2-14x-24y=0 \\ 10x^2+28xy+19y^2-8x-10y=0; \end{cases}$

б) $\begin{cases} 3x^2-4xy-2y^2+6x+24y-24=0 \\ 8x^2+20xy+11y^2-12x-6y-8=0; \end{cases}$

в) $\begin{cases} 2x^2+10xy+13y^2-2x-4y+1=0 \\ x^2+2xy-y^2-4x-8y-1=0; \end{cases}$

г) $\begin{cases} 4x^2-7xy+y^2+28x-11y+24=0 \\ 9x^2-14xy+y^2+60x-20y+51=0; \end{cases}$

д) $\begin{cases} y^3-3x^2y+8xy-6y=0 \\ x^3-4x^2+6x-3xy^2+4y^2-4=0; \end{cases}$

е) $\begin{cases} x^4-6x^2y^2+y^4+6x^3-12xy^2+13x^2-6y^2+14x+6=0 \\ x^3-xy^2+5x^2-y^2+7x+3=0. \end{cases}$

Отг. а) $(0, 0)$, $(-2, 2)$, $(4, -2)$, $(-6, 4)$; б) $(2, 0)$, $(-2, 2)$, $(-4, 4)$, $(-8, 6)$; в) $(2i, -i)$, $(-2i, i)$, $(6+2i, -2-i)$, $(6-2i, -2+i)$; г) $(0, 3)$, $(1, 4)$, $(-1, 0)$, $(-3, 2)$; д) $(2, 0)$, $(1+i, 0)$, $(1-i, 0)$, $(1, 1)$, $(1, -1)$, $\left(\frac{1}{2}(3+i), \frac{1}{2}(1+i)\right)$, $\left(\frac{1}{2}(3+i), -\frac{1}{2}(1+i)\right)$, $\left(\frac{1}{2}(3-i), \frac{1}{2}(1-i)\right)$, $\left(\frac{1}{2}(3-i), -\frac{1}{2}(1-i)\right)$; е) $(-1, 0)$, $(-3, 0)$, $\left(\frac{1}{4}(-3+\sqrt{5}), \frac{1}{4}\sqrt{14+10\sqrt{5}}\right)$, $\left(-\frac{1}{4}(-3+\sqrt{5}), -\frac{1}{4}\sqrt{14+10\sqrt{5}}\right)$, $\left(-\frac{1}{4}(3+\sqrt{5}), \frac{1}{4}\sqrt{14+10\sqrt{5}}\right)$, $\left(-\frac{1}{4}(3+\sqrt{5}), -\frac{1}{4}\sqrt{14+10\sqrt{5}}\right)$.

20. Пресметнете дискримнантата $D(f)$ на полинома $f(x)$, където:

а) $f(x)=x^3-x^2-2x+1$;
б) $f(x)=x^3+2x^2+4x+1$;
в) $f(x)=3x^3+3x^2+5x+2$;
г) $f(x)=x^4-x^3-3x^3+x+1$;
д) $f(x)=2x^4-x^3-4x^2+x+1$.

Отг. а) 49; б) −107; в) −843; г) 725; д) 2777.

21. Пресметнете дискриминантата на полинома $f(x)=x^3+$ $+px+q$.

Решение. Имаме

$$R(f, f')=\prod_{i=1}^{3} f'(x_i)=\prod_{i=1}^{3}(3x_i^2+p)=27(x_1x_2x_3)^2+9p\sum x_1^2x_2^2+$$

$$+3p^2\sum x_1^2+p^3=27q^2+4p^3,$$

откъдето

$$D(f)=\frac{1}{a_0}(-1)^{\frac{n(n-1)}{2}}R(f, f')=-4p^3-27q^2.$$

22. Пресметнете дискриминантата на полинома

$$f(x)=x^3+ax^2+bx+c.$$

Отг. $D(f)=a^2b^2-4b^3-4a^3c+18abc-27c^3$.

23. Пресметнете дискриминантата на полинома

$$f(x)=x^5-5ax^3+5a^2x-b.$$

Отг. $D(f)=3125(b^2-4a^5)^2$.

24. Намерете стойностите на параметъра λ, при които полиномът $f(x)=x^4-4x+\lambda$ има кратни корени.

Решение. Пресмятаме дискриминантата на полинома $f(x)$. Имаме

$$D(f)=R(f,f')=\prod_{i=1}^{4}f'(x_i)=256\prod_{i=1}^{4}(x_i^3-1)=256\prod_{i=1}^{4}\frac{x_i^4-x_i}{x_i}=$$

$$=\frac{256}{\lambda}\prod_{i=1}^{4}(\lambda-3x_i)=\frac{256}{\lambda}81f\left(\frac{\lambda}{3}\right)=256(\lambda^3-27).$$

Търсените стойности на λ ще бъдат корените на уравнението

$$D(f)=256(\lambda^3-27)=0,$$

откъдето получаваме $\lambda_1=3$, $\lambda_2=3\omega$, $\lambda_3=3\omega^2$, където $\omega=-\frac{1}{2}+\frac{i\sqrt{3}}{2}$. Да намерим кратните корени например при $\lambda=3\omega$. Очевидно ω е общ корен на $f(x)$ и $f'(x)$; следователно той е кратен на $f(x)$. Останалите корени на $f(x)$ не са корени на $f'(x)$ и следователно единственият кратен корен на $f(x)$ е ω и той е двукратен.

25. Намерете стойностите на параметъра λ, при които полиномът $f(x)$ има кратни корени, където:

а) $f(x)=x^3-3x+\lambda$;

б) $f(x)=x^3-8x^2+(13-\lambda)x-(6+2\lambda)$;

в) $f(x)=x^4-4x^3+(2-\lambda)x^2+2x-2$;

г) $f(x)=x^3+\lambda x^2+\lambda x+2$;
д) $f(x)=(x^2-x+1)^3-\lambda(x^2-x)^2$.

Отг. а) $\lambda=\pm 2$; б) $\lambda_1=0$, $\lambda_2=-3$, $\lambda_3=125$; в) $\lambda_1=-1$, $\lambda_2=-\frac{3}{4}$, $\lambda_{3,4}=-\frac{7}{2}\pm\frac{9}{2}i\sqrt{3}$; г) $\lambda_{1,2}=3\pm\sqrt{9+\sqrt{108}}$, $\lambda_{3,4}=3\pm\sqrt{9-\sqrt{108}}$; д) $\lambda=0$, $\lambda=\frac{27}{4}$.

26. Намерете дискриминантата на полинома $f(x)=x^n+a$.

Отг. $D(f)=(-1)^{\frac{n(n-1)}{2}}n^n a^{n-1}$.

27. Покажете, че дискриминантите на полиномите

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$
$$g(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$$

са равни

Решение. Дадените полиноми са реципрочни. Следователно, ако α_1, $\alpha_2,\ldots,\alpha_n$ са корените на полинома $f(x)$, корените на $g(x)$ ще бъдат $\frac{1}{\alpha_1}$, $\frac{1}{\alpha_2},\ldots,\frac{1}{\alpha_n}$. Имаме

$$D(g)=a_n^{2n-2}\prod_{i<j}\left(\frac{1}{\alpha_i}-\frac{1}{\alpha_j}\right)^2=a_n^{2n-2}\prod_{i<j}\frac{(\alpha_i-\alpha_j)^2}{\alpha_i^2\alpha_j^2}=$$
$$=\frac{a_n^{2n-2}}{(\alpha_1\alpha_2\ldots\alpha_n)^2}\prod_{i<j}(\alpha_i-\alpha_j)^2=a_0^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2=D(f).$$

28. Намерете дискриминантата на полинома $qx+px^{n-1}+1$.

Отг. $(-1)^{\frac{n(n-1)}{2}}[p^n(1-n)^{n-1}+n^nq^{n-1}]$.

29. Намерете дискриминантата на полинома $f(x)=x^n+qx+q$.
Упътване. Използувайте предните две задачи.

30. Пресметнете дискриминантата на полинома

$$f(x)=n!\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\ldots+\frac{x^n}{n!}\right).$$

Решение. Имаме

$$f'(x)=n!\left[1+\frac{x}{1!}+\frac{x^2}{2!}+\ldots+\frac{x^{n-1}}{(n-1)!}\right]=f(x)-x^n,$$

откъдето

$$D(f)=(-1)^{\frac{n(n-1)}{2}}a_0^{n-2}f'(\alpha_1)f'(\alpha_2)\dots f'(\alpha_n)=$$

$$=(-1)^{\frac{n(n-1)}{2}}(-1)^n(\alpha_1\alpha_2\dots\alpha_n)^n=(-1)^{\frac{n(n-1)}{2}}(n!)^n.$$

31. Пресметнете дискриминантата на полинома

$$f(x)=(x-a)^n+(x-b)^n.$$

Решение. Нека u_k са корените на уравнението $u^n+1=0$. Тогава корените α_k на полинома $f(x)$ се определят от уравненията $(x-a)=u_k(x-b)$ ($k=1, 2, \dots, n$). Имаме

$$f'(\alpha_k)=n[(\alpha_k-a)^{n-1}+(\alpha_k-b)^{n-1}]=n(\alpha_k-b)^{n-1}(u_k^{n-1}+1),$$

откъдето

$$D(f)=a_0^{n-2}(-1)^{\frac{n(n-1)}{2}}\prod_{k=1}^{n}f'(\alpha_k)=(-1)^{\frac{n(n-1)}{2}}2^{n-2}n^n\prod_{k=1}^{n}(\alpha_k-b)^{n-1}\times$$

$$\times\prod_{k=1}^{n}(u_k^{n-1}+1)=(-1)^{\frac{n(n-1)}{2}}n^n(a-b)^{n(n-1)}.$$

32. Нека $f(x)$ е произволен полином. Покажете, че

$$D((x-a)f(x))=[f(a)]^2D(f(x)).$$

33. Намерете дискриминантата на полинома

$$f(x)=x^{n-1}+x^{n-2}+\dots+x+1.$$

Упътване. Използувайте предната задача.

Отг. $D(f)=(-1)^{\frac{n(n-1)}{2}}n^{n-2}$.

34. Намерете дискриминантата на полинома

$$f(x)=x^n+ax^{n-1}+ax^{n-2}+\dots+a.$$

Упътване. Умножете полинома $f(x)$ с $x-1$ и използувайте зад. 32.

Отг. $D(f)=(-1)^{\frac{n(n-1)}{2}}a^{n-1}\frac{(n+1)^{n+1}a+n^n(1-a)^{n+1}}{(1+na)^2}$.

35. Намерете дискриминантата на полинома

$$f(x)=x^{n+1}-ax^n-x+a.$$

Упътване. Използвайте равенството $f(x)=(x^n-1)(x-a)$.

Отг. $D(f)=(-1)^{\frac{(n-1)(n-2)}{2}}n^n(a^n-1)^2$.

36. Докажете, че дискриминантата на произведението на два полинома е равна на произведението на дискриминантите на множителите, умножено с квадрата на тяхната резултанта.

Решение. Нека

$$f(x)=a_0(x-x_1)(x-x_2)\dots(x-x_n),$$
$$g(x)=b_0(x-y_1)(x-y_2)\dots(x-y_m).$$

Тогава имаме

$$D(fg)=(a_0b_0)^{2m+2n-2}\prod_{i<k}(x_i-x_k)^2\prod_{i<k}(y_i-y_k)^2\prod_{i=1}^{n}\prod_{k=1}^{m}(x_i-y_k)^2=$$

$$=\left[a_0^{2n-2}\prod_{i<k}(x_i-x_k)^2\right]\left[b_0^{2m-2}\prod_{i<k}(y_i-y_k)^2\right]\left[a_0^mb_0^n\prod_{i=1}^{n}\prod_{k=1}^{m}(x_i-y_k)\right]^2=$$

$$=D(f)\,D(g)\,[R(f\cdot g)]^2.$$

37. Намерете дискриминантата на n-тия циклотомичен полином $\Phi_n(x)$.

Решение. Съгласно зад. 31, § 4, гл. VIII имаме

$$\Phi_n(x)=\prod_{d/n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}=(x^n-1)\prod_{d/n,\ d\neq n}(x^d-1)^{\mu\left(\frac{n}{d}\right)},$$

откъдето, като диференцираме

$$\Phi'(x)=nx^{n-1}\prod_{d/n,\ d\neq n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}+(x^n-1)\left[\prod_{d/n,\ d\neq n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}\right]'.$$

Нека $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\varphi(n)}$ са корените на полинома $\Phi_n(x)$. От последното равенство следва

$$\Phi_n'(\varepsilon_i)=n\,\varepsilon_i^{n-1}\prod_{d/n,\ d\neq n}(\varepsilon_i^d-1)^{\mu\left(\frac{n}{d}\right)}.$$

По-нататък

$$R(\Phi_n,\Phi_n')=\prod_{i=1}^{\varphi(n)}\Phi_n'(\varepsilon_i)=n^{\varphi(n)}\prod_{i=1}^{\varphi(n)}\varepsilon_i^{n-1}\left(\prod_{i=1}^{\varphi(n)}\prod_{d/n,\ d\neq n}(\varepsilon_i^d-1)^{\mu\left(\frac{n}{d}\right)}\right).$$

При фиксиран делител d на n имаме

$$\prod_{i=1}^{\varphi(n)}(\varepsilon_i^d-1)=\Phi_{\frac{n}{d}}(1)^{\frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)}},$$

защото $\varepsilon_1^d, \varepsilon_2^d, \ldots, \varepsilon_{\varphi(n)}^d$ са точно примитивните корени от степен $\frac{n}{d}$ и при това всеки се повтаря $\frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)}$ пъти. Следователно

$$R(\Phi_n, \Phi_n')=n^{\varphi(n)}\left(\prod_{i=1}^{\varphi(n)}\varepsilon_i^{n-1}\right)\prod_{d/n,\, d\neq n}\Phi_{d/n}(1)^{-\frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)}\mu\left(\frac{n}{d}\right)}.$$

По-нататък известно е, че $\Phi_{\frac{n}{d}}(1)$ е различно от 1 само в случай, че $\frac{n}{d}$ е степен на просто число. Освен това $\mu\left(\frac{n}{d}\right)=0$, ако $\frac{n}{d}$ се дели на квадрат на просто число. Оттук следва, че в последното равенство различни от единица могат да бъдат само тези множители, които съответствуват на тези d, за които $\frac{n}{d}$ е просто число. Тогава, ако $p_1, p_2, \ldots, p_k$ са различните прости делители на n, имаме

$$R(\Phi_n, \Phi_n')=n^{\varphi(n)}\left(\prod\varepsilon_i^{n-1}\right)\left(\prod_{i=1}^{k}\Phi_{p_i}(1)^{-\frac{\varphi(n)}{\varphi(p_i)}}\right)=$$

$$=n^{\varphi(n)}\left(\prod\varepsilon_i^{n-1}\right)\frac{1}{\prod_{i=1}^{k}p_i^{\varphi(n)/p_i-1}}$$

Остава да пресметнем произведението $\prod_{i=1}^{\varphi(n)}\varepsilon_i^{n-1}$. Имаме

$$\prod_{i=1}^{\varphi(n)}\varepsilon_i^{n-1}=\prod_{i=1}^{\varphi(n)}\varepsilon_i=(-1)^{\varphi(n)}\Phi_n(0).$$

Но $\varphi(n)$ е четно и

$$\Phi_n(0)=\prod_{d/n}(-1)^{\mu\left(\frac{n}{d}\right)}=(-1)^{\sum\mu\left(\frac{n}{d}\right)}=1,$$

защото $\sum_{d|n}\mu\left(\frac{n}{d}\right)=0$. Следователно

$$R(\Phi_n,\Phi_n')=\frac{n^{\varphi(n)}}{\prod_{i=1}^{k}p_i^{\frac{\varphi(n)}{p_i-1}}}.$$

Оттук за дискриминантата намираме

$$D(\Phi_n)=(-1)^{\frac{\varphi(n)(\varphi(n)-1)}{2}}\frac{n^{\varphi(n)}}{\prod_{i=1}^{k}p_i^{\frac{\varphi(n)}{p_i-1}}}=(-1)^{\frac{\varphi(n)}{2}}\frac{n^{\varphi(n)}}{\prod_{i=1}^{k}p_i^{\frac{\varphi(n)}{p_i-1}}}.$$

38. Пресметнете дискриминантата на полинома

$$f(x)=x^{n+m}+px^m+q.$$

Решение. Имаме $f'(x)=(n+m)x^{n+m-1}+mpx^{m-1}$. Корените на f' са

$$\xi_1=\xi_2=\dots=\xi_{m-1}=0,\ \xi_m, \xi_{m+1}=\xi_m\omega,\dots,\xi_{m+i}=\xi_m\omega^i,\dots,$$

където $\xi_m^n=-\frac{mp}{m+n}$ и ω е примитивен корен на единицата от степен n. Да положим $(n, m)=d$, $n=n_1d$, $m=m_1d$. Имаме

$$D(f)=(-1)^{\binom{n+m}{2}}R(f, f')=(-1)^{\binom{m+n}{2}}(m+n)^{(m+n)}\prod_{i=1}^{m+n-1}f(\xi_i).$$ Но $$\prod_{i=1}^{n+m-1}f(\xi_i)=$$

$$=q^{m-1}\prod_{i=0}^{n-1}f(\omega^i\xi_m),$$

$$f(\omega^i\xi_m)=\omega^{i(n+m)}\xi_m^{n+m}+p\omega^{im}\xi_m^m+q=\xi_m^m\frac{np}{n+m}\omega^{im}+q.$$

По-нататък да положим $\eta=\omega^m$. Тогава η ще бъде примитивен корен от степен n_1, следователно η^i се повтарят периодически с период n_1, откъдето

$$\prod_{i=1}^{m+n-1}f(\xi_i)=q^{n-1}\left(\prod_{i=0}^{n-1}\left(\frac{np}{n+m}\xi_m^m\eta^i+q\right)\right)^d.$$

От формулата

$$\prod_{i=0}^{n_1-1}(\alpha\eta^i+\beta)=\beta^{n_1}-(-1)^{n_1}\alpha^{n_1},$$

получаваме

$$\prod f(\xi_i)=q^{m-1}\left(q^{n_1}-(-1)^{n_1}\xi^{n_1m}\left(\frac{np}{n+m}\right)^{n_1}\right)^d=$$

$$=q^{m-1}\left(q^{n_1}-(-1)^{n_1+m}\frac{m^{m_1}n^n p^{n_1+m_1}}{(m+n)^{n_1+m_1}}\right)^d$$

и

$$D(f)=(-1)^{\binom{n+m}{2}}q^{m-1}\left((m+n)^{n_1+m_1}q^{n_1}-(-1)^{m_1+n_1}m^{m_1}n^{n_1}p^{m_1+n_1}\right)d.$$

39. Нека $f(x)$ е полином. Изразете дискриминантата на полинома $f(x^k)$, k — естествено число, чрез дискриминантата на полинома $f(x)$.

Решение. Нека $f(x)=\sum_{\nu=0}^{n}a_\nu x^{n-\nu}$, $f(x^k)=g(x)$ и $\xi_1, \xi_2, \ldots, \xi_n$ са корените на полинома $f(x)$. Тогава корените на $g(x)$ ще бъдат всички k-ти степени на корените на $f(x)$ и следователно можем да номерираме корените ξ_{ij} на $g(x)$ ($i=1, 2, \ldots, n$; $j=1, 2, \ldots, k$) по такъв начин, че при фиксирано i, ξ_{ij} да са всички k-ти корени на ξ_i. По-нататък $g'(x)=kx^{k-1}f'(x^k)$ и

$$D(g)=(-1)^{\binom{nk}{2}}\frac{1}{a_0}R(g, g')=(-1)^{\binom{nk}{2}}a_0^{nk-2}\prod_{i,j}g'(\xi_{ij})=$$

$$=(-1)^{\binom{nk}{2}}a_0^{nk-2}k^{nk}\left(\prod_{ij}\xi_{ij}\right)^{k-1}\left(\prod_{ij}f'(\xi_{ij}^k)\right).$$

Но

$$\left(\prod_{ij}\xi_{ij}\right)^{k-1}=\left((-1)^{nk}\frac{a_n}{a_0}\right)^{k-1}a_n^{k-1}a_0^{1-k},$$

$$\prod_{ij}f'(\xi_{ij}^k)=\left(\prod_{i=1}^{n}f'(\xi_i)\right)^k=(-1)^{k\binom{n}{2}}a_0^{2k-nk}D(f)^k.$$

Следователно

$$D(g)=(-1)^{k\binom{n}{2}}k^{nk}a_0^{k-1}a_n^{k-1}(D(f))^k.$$

40. Нека старшите коефициенти на полиномите $f(x)$ и $\varphi(x)$ са равни на единица. Докажете равенството

$$D(f(\varphi(x)))=D(f)^m\prod_{i=1}^{n}D(\varphi(x)-\xi_i),$$

където m е степента на $\varphi(x)$, а $\xi_1, \xi_2, \ldots, \xi_n$ са корените на $f(x)$.

Решение. Нека $F(x)=f(\varphi(x))$. Имаме $F(x)=\prod_{i=1}^{n}(\varphi(x)-\xi_i)$. Като приложим неколкократно зад. 36, получаваме

$$D(F)=\prod_{i=1}(D(\varphi(x)-\xi_i)).\prod_{i<j}R(\varphi(x)-\xi_i,\ \varphi(x)-\xi_j).$$

По-нататък имаме

$$R(\varphi(x)-\xi_i,\ \varphi(x)-\xi_j)=(\xi_i-\xi_j)^m,$$

откъдето

$$D(F)=\prod_{i=1}^{n}D(\varphi(x)-\xi_i).\prod_{j<i}(\xi_j-\xi_i)^m=D(f)^m\prod_{i=1}^{n}D(\varphi(x)-\xi_i).$$

41. Пресметнете дискриминантата на n-тия хермитов полином

$$P_n(x)=(-1)^n e^{\frac{x^2}{2}}\frac{d^n}{dx^n}\left(e^{-\frac{x^2}{2}}\right).$$

Решение. Имаме

(1) $$P'_n(x)=nP_{n-1}(x),$$

(2) $$(P_n(x)=xP_{n-1}(x)-(n-1)P_{n-2}(x).$$

От (1) получаваме

$$R(P_n,\ P'_n)=n^nR(P_n,\ P_{n-1}).$$

По-нататък, ако ξ_i са корените на P_{n-1}, от (2) следва

$$P_n(\xi_i)=-(n-1)P_{n-2}(\xi_i),$$

откъдето

$$R(P_n,\ P_{n-1})=\prod_{i=1}^{n-1}P_n(\xi_i)=(-1)^{n-1}(n-1)^{n-1}\prod_{i=1}^{n-1}P_{n-2}(\xi_i)=$$

$$=(-i)^{n-1}(n-1)^{n-1}R(P_{n-1},P_{n-2}),$$

Като вземем пред вид, че $R(P_1,\ P_0)=1$, по индукция получаваме

$$R(P_n,\ P_{n-1})=(-1)^{\frac{n(n-1)}{2}}1.2^2.3^3,\ldots,(n-1)^{n-1},$$

откъдето

$$D(f)=1.2^2.3^3\ldots(n-1)^{n-1}n^n.$$

42. Пресметнете дискриминантата на n-тия лагеров полином

$$P_n(x)=(-1)^n e^x\frac{d^n}{dx^n}(x^n e^{-x}).$$

Решение. Имаме

(1) $$xP'_n(x)=nP_n(x)+n^2P_{n-1}(x),$$

(2) $$P_n(x)=(x-2n+1)P_{n-1}(x)-(n-1)^2P_{n-2}(x).$$

Нека ξ_i са корените на P_n. От (1) получаваме

$$\xi_i P'_n(\xi_i)=n^2P_{n-1}(\xi_i)$$

и следователно

$$R(P_n, P'_n)=\prod_{i=1}^{n} P'_n(\xi_i)=\frac{1}{\xi_1\xi_2\ldots\xi_n}\prod_{i=1}^{n}\xi_i P'_n(\xi_i)=\frac{n^{2n}}{\xi_1\xi_2\ldots\xi_n}\prod_{i=1}^{n}P_{n-1}(\xi_i).$$

Имаме

$$\prod_{i=1}^{n}P_{n-1}(\xi_i)=R(P_n, P_{n-1}),\quad \xi_1\ldots\xi_n=(-1)^nP_n(0)=n\,!,$$

откъдето

$$R(P_n, P'_n)=\frac{n^{2n}}{n!}R(P_n, P_{n-1}).$$

По-нататък нека η_j са корените на P_{n-1}. От (2) получаваме

$$P_n(\eta_j)=-(n-1)^2P_{n-2}(\eta_j)$$

и следователно

$$R(P_n, P_{n-1})=\prod P_n(\eta_j)=(-1)^{n-1}(n-1)^{2(n-1)}\prod P_{n-2}(\eta_j)=$$

$$=(-1)^{n-1}(n-1)^{2(n-1)}R(P_{n-1},P_{n-2}).$$

Като вземем пред вид, че $R(P_1, P_0)=1$, по индукция намираме

$$R(P_n, P_{n-1})=(-1)^{\frac{n(n-1)}{2}}1^2\,.\,2^4\,.\,3^6\ldots(n-1)^{2n-2},$$

откъдето

$$R(P_n, P'_n)=(-1)^{\frac{n(n-1)}{2}}1\,.\,2^3\,.\,3^5\ldots(n-1)^{2n-3}n^{2n-1}$$

и

$$D(P_n)=1\,.\,2^3\,.\,3^5\ldots(n-1)^{2n-3}n^{2n-1}.$$

43. Намерете дискриминантата на полинома

$$P_n(x)=\frac{(-1)^n}{n!}(1+x^2)^{n+1}\frac{d^n}{dx^n}\left(\frac{1}{1+x^2}\right).$$

Решение. Имаме

1) $P_n(x)=2xP_{n-1}(x)-(x^2+1)P_{n-2}(x)$,

2) $P'_n(x)=(n+1)\;P_{n-1}(x)$.

От (1) по индукция лесно следва, че старшият коефициент на P_n е $n+1$. По-нататък от (2) получаваме

$$R(P_n, P'_n)=(n+1)^nR(P_n, P_{n-1}).$$

Нека ξ_k са корените на полинома P_{n-1}. От (1) имаме

$$P_n'(\xi_k)=-(\xi_k^2+1)P_{n-2}(\xi_k)$$

и следователно

$$R(P_n, P_{n-1})=n^n\prod P_n(\xi_k)=(-1)^{n-1}n^n\left(\prod(\xi_k^2+1)\right)\left(\prod P_{n-2}(\xi_k)\right).$$

Но

$$\prod P_{n-2}(\xi_k)=\frac{1}{n^{n-2}}R(P_{n-1}, P_{n-2}),$$

$$\prod(\xi_k^2+1)=\prod(i-\xi_k)(-i-\xi_k)=\frac{1}{n^2}P_{n-1}(i)P_{n-1}(-i).$$

За да пресметнем $P_{n-1}(i)$, използваме формулата

$$P_k(i)=2i\,P_{k-1}(i),$$

която се получава от (1) при $x=i$. Понеже $P_0(i)=1$, получаваме $P_k(i)=(2i)^k$. Аналогично $P_k(-i)=(-2i)^k$.

По такъв начин

$$R(P_n, P_{n-1})=(-1)^{n-1}2^{2(n-1)}R(P_{n-1}, P_{n-2}).$$

По индукция намираме

$$R(P_n, P_{n-1})=(-1)^{\frac{n(n-1)}{2}}2^{n(n-1)},$$

откъдето

$$R(P_n, P_n')=(-1)^{\frac{n(n-1)}{2}}(n+1)^n 2^{n(n-1)}$$

и

$$D(P_n)=(n+1)^{n-1}2^{n(n-1)}.$$

Задачата може да се реши и друго яче, като се използва представянето

$$P_n(x)=\frac{1}{2i}\left((x+i)^{n+1}-(x-i)^{n+1}\right).$$

Лесно се вижда, че корените на P_n са

$$\xi_k=\operatorname{ctg}\frac{k\pi}{n+1},\quad k=1,\ 2,\dots,n.$$

По-нататък

$$P_n'(x)=\frac{n+1}{2i}((x+i)^n-(x-i)^n)$$

и

$$P_n'(\xi_k)=(n+1)\frac{\sin\frac{kn\pi}{n+1}}{\left(\sin\frac{k\pi}{n+1}\right)^n}=\frac{(-1)^{k-1}(n+1)}{\left(\sin\frac{k\pi}{n+1}\right)^{n-1}}.$$

Следователно

$$R_n(P_n, P'_n)=(n+1)^{n-1}\prod P'_n(\xi_k)=(-1)^{\frac{n(n-1)}{2}}(n+1)^{2n-1}\prod_{k=1}^{n}\left(\sin\frac{k\pi}{n+1}\right)^{1-n}.$$

Ще пресметнем произведението $\prod \sin\frac{k\pi}{n+1}$. За удобство полагаме $\frac{\pi}{n+1}=\varphi$. Имаме

$$\sin k\varphi=\frac{e^{ik\varphi}-e^{-ik\varphi}}{2i}=-\frac{e^{-ik\varphi}}{2i}(1-e^{2ik\varphi}),$$

откъдето

$$\prod_{k=1}^{n}\sin\frac{k\pi}{n+1}=\frac{(-1)^n}{2^n i^n}e^{-i\varphi-2i\varphi-\ldots-ni\varphi}\prod_{k=1}^{n}(1-e^{2ki\varphi}).$$

По-нататък при $k=1, 2, \ldots, n$ числата $e^{2ki\varphi}$ са всички различни от 1 корени на единицата от степен $n+1$, т. е. корените на полинома

$$x^n+x^{n-1}+\ldots+x+1,$$

откъдето следва

$$\prod_{k=1}^{n}(1-e^{2ki\varphi})=n+1.$$

Освен това

$$e^{-i\varphi-2i\varphi-\ldots-ni\varphi}=e^{\frac{-n(n+1)}{2}i\varphi}=e^{-\frac{n\pi}{2}i}=(-1)^n i^n.$$

Следователно

$$\prod_{k=1}^{n}\sin\frac{k\pi}{n+1}=\frac{n+1}{2^n}.$$

Като заместим в израза за $R(P_n, P'_n)$, получаваме

$$R(P_n, P'_n)=(-1)^{\frac{n(n-1)}{2}}(n+1)^n 2^{n(n-1)}.$$

Остава да отбележим, че $D(P_n)=(-1)^{\frac{n(n-1)}{2}}\frac{1}{n+1}R(P_n, P'_n)$.

44. Пресметнете дискриминантата на полинома

$$P_n(x)=(-1)^n(1+x^2)^{n+\frac{1}{2}}\frac{d^n}{dx^n}\frac{1}{\sqrt{1+x^2}}.$$

Упътване. Използувайте равенствата

$$P_n=(2n-1)\,x\,P_{n-1}-(n-1)^2(x^2+1)P_{n-2},\ P_n'=n^2P_{n-1}.$$

Отг. $D(P_n)=1.\ 2^3.\ 3^5\ldots n^{2n-1}.\ 1^{2(n-1)}.\ 2^{2(n-2)}\ldots(2n-3)^2.$

45. Пресметнете дискриминантата на полинома

$$P_n(x)=(-1)^n x^{2n+2} e^{-\frac{1}{x}}\frac{d^n}{dx^n}e^{\frac{1}{x}}.$$

Упътване. Използувайте равенствата

$P_n=(2nx+1)\,P_{n-1}+n\,(n-1)x^2\,P_{n-2}.\ P_n'=(n+1)\,n\,P_{n-1}.$

Отг. $D(P_n)=2^2.\ 3^4\ldots n^{2n-2}.\ (n+1)^{n-1}.$

46. Пресметнете дискриминантата на n-тия чебишов полином

$$P_n(x)=2\cos\left(n\ \arccos\ \frac{x}{2}\right).$$

Решение. Имаме равенствата

(1) $$(4-x^2)\,P_n'(x)+nxP_n(x)=2nP_{n-1}(x),$$

(2) $$P_n(x)-xP_{n-1}(x)+P_{n-2}(x)=0.$$

Нека ξ_i са корените на P_n. От (1) следва, че

$$(4-\xi_i^2)P_n'(\xi_i)=2n\ P_{n-1}(\xi_i),$$

откъдето

$$R(P_n,\ P_n')=\prod P_n'(\xi_i)=\prod\frac{2n}{4-\xi_i^2}P_{n-1}(\xi_i)=(2^n)^nR(P_n,\ P_{n-1})\prod\frac{1}{4-\xi_i^2}.$$

По-нататък

$$\prod\frac{1}{4-\xi_i^2}=(-1)^n\prod\frac{1}{(2-\xi_i)(-2-\xi_i)}=\frac{(-1)^n}{P_n(2)P_n(-2)}.$$

Непосредствено от дефиницията на $P_n(x)$ намираме

$$P_n(2)=2,$$
$$P_n(-2)=(-1)^n2.$$

Следователно

$$R(P_n,\ P_n')=2^{n-2}n^nR(P_n,\ P_{n-1}).$$

По нататък нека η_i са корените на P_{n-1}. От (2) следва

$$P_n(\eta_i)=-P_{n-2}(\eta_i),$$

от което получаваме

$$R(P_n,\ P_{n-1})=\prod P_n(\eta_i)=(-1)^{n-1}\prod P_{n-2}(\eta_i)=(-1)^{n-1}R(P_{n-1},\ P_{n-2}).$$

Като вземем пред вид, че $R(P_1,\ P_0)=2$, получаваме

$$R(P_n,\ P_{n-1})=(-1)^{\frac{n(n-1)}{2}}2,$$

откъдето

$$R(P_n,\ P_n')=2^{n-1}n^n(-1)^{\frac{n(n-1)}{2}}$$

и

$$D(P_n)=2^{n-1}n^n.$$

§ 3. ТРАНСФОРМАЦИИ НА АЛГЕБРИЧНИ УРАВНЕНИЯ

1. Дробно линейна трансформация. Нека $f(x)$ е полином от n-та степен и $x_1, x_2, \ldots, x_n$ да са корените на уравнението $f(x)=0$. Да разгледаме дробно линейната трансформация

$$(1) \qquad x \to \frac{ax+b}{cx+d}, \quad ad-bc \neq 0$$

и да положим $y=\frac{ax+b}{cx+d}$. Като изразим x чрез y, ще получим

$$x=\frac{-dy+b}{cy-a}.$$

Заместваме в даденото уравнение x с $\frac{-dy+b}{cy-a}$ и след освобождаване от знаменателите получаваме алгебричното уравнение

$$(2) \qquad (cy-a)^n f\left(\frac{-dy+b}{cy-a}\right)=0.$$

Казваме, че уравнението (2) е получено от $f(x)=0$ чрез трансформацията (1). За корените на трансформираното уравнение (2) имаме

$$y_k=\frac{ax_k+b}{cx_k+d}, \quad k=1, 2, \ldots, n.$$

Като вземем пред вид тъждеството

$$\frac{ax+b}{cx+d}=\frac{a}{c}+\frac{bc-ad}{c(cx+d)},$$

се убеждаваме, че трансформацията (1) е резултат от последователни трансформации от вида: а) $x \to x+a$; б) $x \to ax$; в) $x \to \frac{1}{x}$. В случая а) трансформираното уравнение е $f(y-a)=0$ с корени $y_k=x_k+a$; в случая б) трансформираното уравнение е $f\left(\frac{y}{a}\right)=0$ с корени $y_k=ax_k$; в случая в) трансформираното уравнение е $y^n f\left(\frac{1}{y}\right)=0$ с корени $y_k=\frac{1}{x_k}$.

Трансформациите от вида б) и в) се извършват непосредствено, а трансформацията от вида а) е удобно да се извърши с помощта на схемата на Хорнер.

2. Трансформация на Чирнхаус. Нека $x_1, x_2, \ldots, x_n$ да са корените на алгебричното уравнение

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

и $y=\varphi(x)$ е даден полином на x. Да намерим уравнение от n-та степен

$$y^n+A_1y^{n-1}+\ldots+A_n=0$$

с корени $y_j=\varphi(x_j)$, $j=1, 2,\ldots, n$. За целта образуваме степените на y: $y, y^2,\ldots, y^n$. По модул $f(x)$ всеки от полиномите y^s е сравним с полином $r_s(x)$ от степен $<n$. Ясно е, че $y_i^s=r_s(x_i)$, $i=1, 2, \ldots, n$. Можем да пишем

$$
(3)\qquad
\begin{aligned}
y_i&=p_0+p_1x_i+p_2x_i^2+\ldots+p_{n-1}x_i^{n-1},\\
y_i^2&=q_0+q_1x_i+q_2x_i^2+\ldots+q_{n-1}x_i^{n-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
y_i^n&=t_0+t_1x_i+t_2x_i^2+\ldots+t_{n-1}x_i^{n-1},
\end{aligned}
$$

където коефициентите $p, q,\ldots, t$ се изразяват като полиноми на $a_1, a_2,\ldots,a_n$ и на коефициентите на $\varphi(x)$.

Нека $S_1, S_2,\ldots, S_{n-1}$ да са степенните сборове от корените $x_1, x_2, \ldots, x_n$ и $T_1, T_2,\ldots, T_n$ да са степенните сборове на $y_1, y_2,\ldots, y_n$. От (3) получаваме

$$
(4)\qquad
\begin{aligned}
T_1&=np_0+p_1S_1+p_2S_2+\ldots+p_{n-1}S_{n-1},\\
T_2&=nq_0+q_1S_1+q_2S_2+\ldots+q_{n-1}S_{n-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
T_n&=nt_0+t_1S_1+t_2S_2+\ldots+t_{n-1}S_{n-1}.
\end{aligned}
$$

По формулите на Нютон

$$
\begin{aligned}
S_1+a_1&=0,\\
S_2+a_1S_1+2a_2&=0\\
&\ldots\ldots
\end{aligned}
$$

намираме $S_1, S_2,\ldots,S_{n-1}$; след това от (4) пресмятаме $T_1, T_2,\ldots, T_n$ и накрая, също по формулите на Нютон

$$
\begin{aligned}
T_1+A_1&=0,\\
T_2+A_1T_1+2A_2&=0,\\
&\ldots\ldots
\end{aligned}
$$

(в случая на поле с характеристика 0), определяме коефициентите на трансформираното уравнение

$$y^n+A_1y^{n-1}+A_2y^{n-2}+\ldots+A_n=0.$$

3. **Обща трансформация.** Тази трансформация е използувана от Лагранж за алгебрично решаване на уравненията и се състои в следното: От дадено уравнение $f(x)=0$, с корени $x_1, x_2,\ldots,x_n$, да се получи ново уравнение

$$y^N+A_1y^{N-1}+\ldots+A_N=0,$$

корените на което са различните N стойности, които приема дадена рационална функция $y=\varphi(x_1, x_2,\ldots, x_n)$ при произволно пермутиране на корените $x_1, x_2,\ldots, x_n$. (Разбира се, може $\varphi(x_1, x_2$

$\ldots, x_n)$ да не зависи от всички корени, например, ако $y=\varphi(x_1)$ не зависи от $x_2, x_3, \ldots, x_n$ и $\varphi(x_1)$ е полином само на x_1, трансформацията се свежда в частност до трансформация на Чирнхаус). Съгласно формулите на Виет ще имаме

$$
\begin{aligned}
-A_1 &= y_1+y_2+\ldots+y_N,\\
A_2 &= y_1y_2+y_1y_3+\ldots+y_{N-1}y_N,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
(-1)^n A_N &= y_1y_2\ldots y_N.
\end{aligned}
$$

Ясно е, че $A_1, A_2, \ldots, A_N$ са симетрични функции на корените $x_1, x_2, \ldots, x_n$ и следователно се изразяват рационално чрез коефициентите на $f(x)$.

1. Намерете полином $g(y)$, корените на който да са с 2 по-големи от корените на полинома $f(x)=x^4-3x^2+7x+5$.

Отг. $g(y)=y^4-8y^3+27y^2-51y+47$.

2. Нека $g(y)$ е полиномът, корените на който са с α по-малки от корените на полинома $f(x)=x^3-3x^2-9x+5$.

Определете α така, че:

а) коефициентът пред y^2 в $g(y)$ да бъде равен на нула;

б) коефициентът пред y в $g(y)$ да бъде равен на нула.

Отг. а) $\alpha=3$; б) $\alpha=\frac{3}{2}(1\pm\sqrt{5})$.

3. Намерете полином $g(y)$, корените на който да са три пъти по-малки от корените на полинома

$$f(x)=2x^3-5x^2+4x+7.$$

Отг. $g(y)=54y^3-45y^2+12y+7$.

4. Намерете полином $g(y)$, корените на който са стойностите на полинома $y=2x-3$, когато x приема за стойности всички корени на полинома $f(x)=4x^3+x^2-x+1$.

Отг. $g(y)=2y^3+19y^2+48y+61$.

5. Намерете полином $g(y)$, корените на който да са стойностите на дробно линейната функция $y=\frac{x+1}{x-1}$, когато x приема за стойности корените на полинома $f(x)=x^4+x^2+x+3$.

Отг. $g(y)=6y^4-11y^3+22y^2-6y+4$.

6. Намерете полином $g(y)$, корените на който са стойностите на полинома $y=1-2x-x^2$, когато x приема за стойности всички корени на полинома $f(x)=x^3-2x-3$.

Решение. Ще извършим трансформация на Чирнхаус. Нека x_1, x_2, x_3 са корените на дадения полином и y_1, y_2, y_3 са корените на търсения. Имаме

$$y_i=1-2x_i-x_i^2,$$
$$y_i^2=13+7x_i+4x_i^2,$$
$$y_i^3=-32-61x_i-31_i^2,$$

откъдето, ако S_1, S_2 са степенните сборове на дадения полином, а T_1, T_2, T_3 — тези на търсения, имаме

$$T_1=3-2S_1-S_2,$$
$$T_2=39+7S_1+4S_2,$$
$$T_3=-96-61S_1-31S_2.$$

Понеже $S_1=0$, $S_2=4$, то

$$T_1=-1,\ T_2=55,\ T_3=-220.$$

Нека

$$g(y)=y^3+b_1y^2+b_2y+b_3.$$

Тогава от формулите на Нютон

$$T_1+b_1=0$$
$$T_2+T_1b_1+2b_2=0,$$
$$T_3+T_2b_1+T_1b_2+3b_3=0$$

намираме

$$b_1=1,\ b_2=-27,\ b_3=46,$$

откъдето

$$g(y)=y^3+y^2-27y+46.$$

Ще изложим и друго решение на задачата. От равенствата

$$y_i=1-2x_i-x_i^2,\ i=1,\ 2,\ 3,$$

следва

$$y_ix_i=x_i-2x_i^2-x_i^3,$$

или като вземем пред вид, че $x_i^3=2x_i+3$,

$$y_ix_i=-3-x_i-2x_i^2.$$

По същия начин намираме

$$y_ix_i^2=-6-7x_i-x_i^2.$$

И така x_i и x_i^2 удовлетворяват уравненията

$$x_i^2+2x_i+y_i-1=0$$
$$2x_i^2+(1+y_i)x_i+3=0,$$
$$x_i^2(1+y_i)+7x_i+6=0,$$

от които, като елиминираме x_i, x_i^2, получаваме

$$\begin{vmatrix} 1 & 2 & y_i-1 \\ 2 & 1+y_i & 3 \\ 1+y_i & 7 & 6 \end{vmatrix}=0$$

или развито

$$y_i^3+y_i^2-27y_i+46=0.$$

Следователно

$$g(y)=y^3+y^2-27y+46.$$

7. Намерете полином $g(y)$, корените на който са стойностите на полинома $y=\varphi(x)$, когато x приема за стойности корените на полинома $f(x)$, където:

а) $f(x)=x^3-x^2-4x+4, \quad \varphi(x)=x^2+x-1;$

б) $f(x)=2x^3-5x^2+x+2, \quad \varphi(x)=2x^2+3x-1;$

в) $f(x)=x^3-x^2+2x+1, \quad \varphi(x)=2-x^2;$

г) $f(x)=x^4-3x+1, \quad \varphi(x)=x^3+x;$

д) $f(x)=x^4-x-2, \quad \varphi(x)=x^3-2;$

е) $f(x)=x^4+2x^3-13x^2-14x+48, \quad \varphi(x)=x^2+x-7.$

Отг. а) $g(y)=y^3-7y^2+11y-5$; б) $g(y)=y^3-15y^2+18y+104$; в) $g(y)=y^3-9y^2+2y+1$; г) $g(y)=y^4-9y^3+31y^2-45y+13$; д) $g(y)=y^4+5y^3+9y^2+7y-6$; е) $g(y)=y^4-2y^2+1$.

8. Нека $g(v)$ е полиномът, корените на който са стойностите на полинома $y=x^2+\lambda x$, когато x приема за стойности всички корени на полинома $f(x)=x^3-2x+4$. Намерете при какви стойности на параметъра λ сборът на два от корените на $g(v)$ е равен на третия.

9. Нека $g(y)$ е полиномът, корените на който са стойностите на полинома $y=x^2+1$, когато x приема за стойности всички корени на полинома $f(x)=x^4+\lambda x+1$. Намерете при какви стойности на λ сборът на два от корените на $g(y)$ е равен на сбора на другите два.

10. Намерете полином $g(y)$, корените на който да са квадратите на корените на полинома

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

Решение. Нека

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n=a_0(x-x_1)(x-x_2)\ldots(x-x_n).$$

Тогава

$$a_0x^n-a_1x^{n-1}+\ldots+(-1)^na_n=a_0(x+x_1)(x+x_2)\ldots(x+x_n).$$

Умножавайки горните две равенства, получаваме

$$a_0^2(x^2-x_1^2)(x^2-x_2^2)\ldots(x^2-x_n^2)=(a_0x^n+a_2x^{n-2}+\ldots)^2-(a_1x^{n-1}+a_3x^{n-3}+ +\ldots)^2.$$

Ясно е, че в полинома отдясно фигурират само четни степени на x. Търсения полином $g(y)$ ще получим, като в последния положим $x^2=y$.

11. Намерете полином $g(y)$, корените на който са третите степени на корените на полинома

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

Решение. Представяме полинома $f(x)$ във вида

$$f(x)=f_0(x^3)+xf_1(x^3)+x^2f_2(x^3)$$

и разглеждаме полинома

$$F(y)=f_0^3(y)+yf_1^3(y)+y^2f_2^3(y)-3yf_0(y)f_1(y)f_2(y).$$

Ще покажем, че неговите корени са точно третите степени на корените на $f(x)$. Действително, ако $f(x)=0$ и $y=x^3$, то

$$(f_0(y)+xf_1(y)+x^2f_2(y))(f_0(y)+\alpha xf_1(y)+\alpha^2x^2f_2(y))(f_0(y)+\alpha^2xf_1(y)+\alpha x^2f_2(y))=0,$$

където $\alpha^3=1$, $\alpha\neq 1$. Но изразът отляво е точно $g(y)$.

12. Намерете полином $g(y)$, корените на който да са стойностите на рационалната функция $y=\frac{1}{x^2+x}$, когато x приема за стойности всички корени на полинома $f(x)=x^3+x+2$.

Решение. Имаме

$$y_1=\frac{1}{x_1^2+x_1}=\frac{(x_2^2+x_2)(x_3^2+x_3)}{(x_1^2+x_1)\,(x_2^2+x_2)(x_3^2+x_3)}.$$

Но

$$(x_1^2+x_1)(x_2^2+x_2)(x_3^2+x_3)=x_1x_2x_3\,(1+x_1)(1+x_2)(1+x_3)=-(-2)f(-1)=4.$$

За да изразим $(x_2^2+x_2)(x_3^2+x_3)$ чрез x_1, представяме $f(x)$ във вида $f(x)=(x-x_1)\varphi(x)$, $\varphi(x)=x^2+x_1x+(x_1^2-1)$. Имаме

$$(x_2^2+x_2)(x_3^2+x_3)=x_2x_3(1+x_2)(1+x_3)=(x_1^2-1)\,\varphi(-1)=(x_1^2-1)(x_1^2-x_1)=$$

$$=x_1^4-x_1^3-x_1^2+x_1=x_1^2-2x_1-x_1+2-x_1^2+x_1=2-2x_1,$$

откъдето получаваме $2y_1=1-x_1$. Аналогично имаме

$$2y_2=1-x_2,\ 2y_3=1-x_3.$$

Следователно стойностите на дробната функция $\frac{1}{x^2+x}$ за корените на полинома $f(x)$ съвпадат със стойностите на полинома $\frac{1}{2}(1-x)$ за корените на $f(x)$. Като постъпим по известния вече начин, намираме

$$g(y)=4y^3-6y^2+2y-1.$$

Задачата може да се реши и така. Имаме следните равенства:

$$x^2y+xy+1=0,$$
$$x^2y+(y-1)x-2y=0,$$
$$x^2(y-1)-xy-2y=0,$$

които лесно следват от условията $x^3+x+2=0$ и $y=\frac{1}{x^2+x}$. Като елиминираме от тях x, получаваме

$$4y^3-6y^2+2y-1=0.$$

13. Намерете полином $g(y)$, корените на който да са стойностите на рационалната функция $\varphi(x)=y$, когато x приема за стойности всички корени на полинома $f(x)$, където:

а) $f(x)=x^3+2x^2-3x-2$, $\varphi(x)=\frac{1}{1-x^2}$;

б) $f(x)=x^3-3x+1$, $\varphi(x)=\frac{x^3+2x-3}{x^2-3}$;

в) $f(x)=x^3+2x^2-x-3$, $\varphi(x)=\frac{x^2+2}{x^2+2x+1}$;

г) $f(x)=x^3+3x^2-4x+3$, $\varphi(x)=\frac{x^3+3}{3x^2+3}$.

Отг. а) $g(y)=4y^3-7y-1$; б) $g(y)=y^3+y^2+14y-8$;
г) $g(y)=243y^3+228y^2-153y+145$.

14. Нека x_1, x_2, x_3 са корените на полинома

$$f(x)=x^3+px+q.$$

Намерете полином $g(y)$ с корени

$$y_1=x_1^2x_2,\ y_2=x_1^2x_3,\ y_3=x_1x_2^2,\ y_4=x_2^2x_3,\ y_5=x_1x_3^2,\ y_6=x_2x_3^2.$$

Решение. Нека търсеният полином е

$$g(y)=y^6+b_1y^5+b_2y^4+b_3y^3+b_4y^2+b_5y+b_6.$$

Съгласно формулите на Виет за коефициентите b_i имаме

$$-b_1=\sum y_1=\sum x_1^2x_2=3q;$$

$$b_2=\sum y_1y_2=\sum x_1^4x_2x_3+\sum x_1^2x_2^3x_3+\sum x_1^3x_2^3+3\sum x_1^2x_2^2x_3^2=$$

$$=x_1x_2x_3\sum x_1^3+x_1x_2x_3\sum x_1^2x_2+\sum x_1^3x_2^3+3x_1^2x_2^2x_3^2=p_3+6q^2;$$

$$-b_3=\sum y_1y_2y_3=\sum x_1^5x_2^3x_3+2\sum x_1^4x_2^3x_3^2+2x_1^3x_2^3x_3^3=27qp^3+7q^3;$$

$$b_4=\sum y_1y_2y_3y_4=\sum x_1^5x_2^5x_3^2+\sum x_1^3x_2^3x_3^6+\sum x_1^5x_2^4x_3^3+$$

$$+3\sum x_1^4x_2^4x_3^4=p^3q^2+64q^4;$$

$$-b_5=\sum y_1y_2y_3y_4y_5=\sum x_1^6x_2^5x_3^4=3q^5;$$

$$b_6=y_1y_2y_3y_4y_5y_6=x_1^6x_2^6x_3^6=q^6.$$

И така

$$g(y)=y^6-3qy^5+(p^3+6q^2)y^4-(2p^3q+9q^3)y^3+(p^3q^2+6q^4)y^2-3q^5y+q^6.$$

Същата задача може да се реши и така: непосредствено се проверява, че (y_1, x_1), (y_2, x_1), (y_3, x_2), (y_4, x_2), (y_5, x_3), (y_6, x_3) са решения на системата

$$\begin{cases} y^3+pyx^4+qx^3=0 \\ x^3+px+q=0. \end{cases}$$

Следователно y_i ще бъдат корени на резултантата $R(y)$. Тази резултанта е от девета степен, но както лесно се вижда, освен посочените решения горната система има още три: (x_1^3, x_1), (x_2^3, x_2), (x_3^3, x_3); следователно $R(y)$ ще има за корени и x_1^3, x_2^3, x_3^3. Като отделим последните три корена, получаваме търсения полином.

15. Нека x_i са корените на полинома $f(x)$. Намерете полином $g(y)$ с корени y_i, където:

а) $f(x)=x^3+2x-1$,

$y_1=x_2x_3,\ y_2=x_3x_1,\ y_3=x_1x_2$;

б) $f(x)=x^3+px+q$,

$y_1=x_2^2+x_2x_3+x_3^2,\ y_2=x_3^2+x_3x_1+x_1^2,\ y_3=x_1^2+x_1x_2+x_2^2$;

в) $f(x)=x^3+ax^2+bx+c$,

$y_1=(x_1-x_2)(x_1-x_3),\ y_2=(x_2-x_1)(x_2-x_3),\ y_3=(x_3-x_1)(x_3-x_2)$

г) $f(x)=x^3+ax^2+bx+c$,

$y_1=x_1^2-x_2x_3,\ y_2=x_2^2-x_3x_1,\ y_3=x_3^2-x_1x_2$.

Отг. а) $g(y)=y^3-2y^2-1$; б) $g(y)=(y+p)^3$;

в) $g(y)=y^3+9(b-a^2)y^2-108(b-a^2)^3y-27(2a^3-3abc+bc^2)^2$.

г) $g(y)=y^3+(3b-a^2)y^2+b(3b-a^2)y+b^3-a^3c$;

16. Нека корените на полинома $f(x)$ са $x_1, x_2, \ldots, x_n$. Намерете полином с корени квадратите на разликите от корените на полинома $f(x)$.

Решение. Степента на търсения полином очевидно е равна на $m=\frac{n(n-1)}{2}$. Нека корените му са $y_1, y_2, \ldots, y_m$. За да намерим коефициентите на търсения полином, достатъчно е да пресметнем степенните сборове $T_1, T_2, \ldots, T_m$ от корените му. Да разгледаме полинома

$$\varphi_k(x)=(x-x_1)^{2k}+(x-x_2)^{2k}+\ldots+(x-x_n)^{2k}.$$

По формулата на Нютон

$$(x-x_i)^{2k}=x^{2k}-\binom{2k}{1}x^{2k-1}x_i+\binom{2k}{2}x^{2k-2}x_i^2-\ldots-\binom{2k}{1}xx_i^{2k-1}+x_i^{2k},$$

за $i=1, 2, \ldots, n$. Като съберем тези равенства, получаваме

$$\varphi_k(x)=nx^{2k}-\binom{2k}{1}S_1x^{2k-1}+\binom{2k}{2}S_2x^{2k-2}-\ldots-\binom{2k}{1}S_{2k-1}x+S_{2k},$$

където S_i са степенните сборове от корените на $f(x)$. Очевидно имаме

$$\varphi_k(x_1)+\varphi_k(x_n)+\ldots+\varphi_k(x_n)=2\sum_{i<j}(x_i-x_j)^{2k}=2T_k.$$

съгласно второто представяне на полинома $\varphi_k(x)$

$$2T_k=nS_{2k}-\binom{2k}{2}S_1S_{2k-1}+\binom{2k}{2}S_2S_{2k-2}-\ldots+nS_{2k}$$

или окончателно

$$T_k=nS_{2k}-\binom{2k}{1}S_1S_{2k-1}+\binom{2k}{2}S_2S_{2k-2}-\ldots+\frac{(-1)^k}{2}\binom{2k}{k}S_k^2.$$

17. Нека x_i са корените на полинома $f(x)$. Намерете полином чиито корени са квадратите на всевъзможните суми на два от корените на $f(x)$.

Упътване. Вж. предната задача.

18. Нека x_i са корените на полинома $f(x)$. Намерете полином $g(y)$ с корени y_i, където:

а) $f(x)=x^3-x^2-3$, $y_1=\frac{x_1}{x_2+x_3-x_1}$, $y_2=\frac{x_2}{x_3+x_1-x_2}$,

$y_3=\frac{x_3}{x_1+x_2-x_3}$;

б) $f(x)=x^3+px+q$,

$y_1=\frac{1}{x_2^2+x_3^2}$, $y_2=\frac{1}{x_3^2+x_1^2}$, $y_3=\frac{1}{x_1^2+x_2^2}$;

в) $f(x)=x^3+px^2+qx+r$,

$y_1=\frac{x_2x_3}{x_2+x_3}$, $y_2=\frac{x_3x_1}{x_3+x_1}$, $y_3=\frac{x_1x_2}{x_1+x_2}$;

г) $f(x)=x^3+px^2+qx+r$,

$y_1=\frac{x_2}{x_3}+\frac{x_3}{x_2}$, $y_2=\frac{x_3}{x_1}+\frac{x_1}{x_3}$, $y_3=\frac{x_1}{x_2}+\frac{x_2}{x_1}$;

д) $f(x)=x^3+px^2+qx+r$,

$y_1=\frac{x_1}{x_2x_3-q}$, $y_2=\frac{x_2}{x_3x_1-q}$, $y_3=\frac{x_3}{x_1x_2-q}$.

19. Нека x_1, x_2, x_3 са корените на полинома

$$f(x)=x^3+px+q.$$

Намерете полином с корени

$$y_1=(x_1+\alpha x_2+\alpha^2 x_3)^3,\quad y_2=(x_2+\alpha x_1+\alpha^2 x_3)^3,$$

където $\alpha^3=1$, $\alpha\neq 1$.

Решение. Нека $g(y)=y^2+my+n$ е полином с корени y_1 и y_2. По формулите на Виет $m=-y_1-y_2$ и $n=y_1y_2$, така че m и n се представят като симетрични полиноми от x_i. Изразяването им чрез коефициентите намираме с помощта на теоремата за степента и теглото. Полиномът

$$m=-(x_1+\alpha x_2+\alpha^2x_3)^3+(x_2+\alpha x_1+\alpha^2x_3)^3$$

има степен 3 и тегло 3, следователно ще има вида $m=Aq$. За да пресметнем A, взимаме $x_1=1$, $x_2=\alpha$, $x_3=\alpha^2$. Намираме $A=+27$. По-нататък полиномът

$$n=(x_1+\alpha x_2+\alpha^2x_3)^3\,(x_2+\alpha x_1+\alpha^2x_3)^3$$

има степен 6 и тегло 6, следователно

$$n=Bp^3+Cq^2.$$

Коефициентите B, C можем да намерим, като положим последователно $x_1=1$, $x_2=\alpha$, $x_3=\alpha^2$ и $x_1=0$, $x_2=1$, $x_3=-1$. Намираме $B=-27$ и $C=0$. И така търсеният полином е

$$g(y)=y^2+27qy-27p^3.$$

20. Нека x_1, x_2, x_3, x_4 са корените на полинома

$$f(x)=x^4+px^2+qx+r.$$

Намерете полином $g(y)$ с корени y_i, където:

а) $y_1=x_1x_2+x_3x_4,\ y_2=x_1x_3+x_2x_4,\ y_3=x_1x_4+x_2x_3;$
б) $y_1=(x_1+x_2-x_3-x_4)^2, y_2=(x_1+x_3-x_2-x_4)^2,$
$y_3=(x_1+x_4-x_2-x_3)^2.$

Отг. а) $g(y)=y^3-py^2-4ry+4pr-q^2;$

б) $g(y)=y^3-8py^2+(16q^2-64r)y-64r^2$

21. Като използувате резултата от зад. 19, получете формула за решенията на уравнението от трета степен

$$x^3+px+q=0.$$

Решение. Нека y_1 и y_2 са корените на уравнението

$$y^2+27qy-27p^3=0.$$

Тогава x_1, x_2, x_3 удовлетворяват системата

$$\begin{cases} x_1+x_2+x_3=0 \\ x_1+\alpha x_2+\alpha^2x_3=\sqrt[3]{y_1} \\ \alpha x_1+x_2+\alpha^2x_3=\sqrt[3]{y_2}, \end{cases}$$

откъдето получаваме

$$x_1=\frac{\sqrt[3]{y_1}+\alpha^2\sqrt[3]{y_2}}{3},\quad x_2=\frac{\alpha^2\sqrt[3]{y_1}+\sqrt[3]{y_2}}{3},\quad x_3=\frac{\alpha\sqrt[3]{y_1}+\alpha\sqrt[3]{y_2}}{3}.$$

Не е трудно да се съобрази, че получените формули са еквивалентни на формулите на Кардано.

22. Нека x_1, x_2, x_3 са корените на полинома

$$f(x)=x^3+px^2+qx+r.$$

Покажете, че полиномът $x_1^2x_2+x_2^2x_3+x_3^2x_1$ приема само две стойности, които са корени на квадратно уравнение със старши коефициент 1, дискриминантата на което е равна на дискриминантата на $f(x)$.

ГЛАВА X

ГРУПИ

Определение за група и основни свойства. Нека G е множество, в което е зададена бинарна операция, т. е. на всяка наредена двойка елементи a, b от G е съпоставен еднозначно елемент c от G. Пишем $c=ab$ и казваме, че c е произведение на елемента a с елемента b. Множеството G се нарича *група* относно дадената операция, когато тази операция удовлетворява следните две условия

1) $a(bc)=(ab)c$ за произволни елементи a, b, $c \in G$;

2) за произволни a, $b \in G$, всяко едно от уравненията $ax=b$ и $ya=b$ има единствено решение в G.

С други думи, операцията трябва да бъде *асоциативна и обратима.*

Теорема. Множеството G е група относно асоциативната бинарна операция $c=ab$ тогава и само тогава, когато:

а) съществува елемент $e \in G$, за който $ea=a$ при всяко $a \in G$;

б) за всяко $a \in G$ съществува елемент $a' \in G$, такъв че $a'a=e$.

Доказва се, че елементът e от условието а) е единствен и за всеки елемент $a \in G$ е в сила

$$ae=ea=a.$$

Този елемент e се нарича *единичен елемент* на групата G. Често единичният елемент ще означаваме с 1. Елементът a' от условието б) е еднозначно определен чрез a, като е в сила равенството

$$a'a=aa'=e.$$

Ще означаваме a' с a^{-1} и ще казваме, че a^{-1} е *обратен елемент* на a. И така за всеки елемент a от G съществува еднозначно определен обратен елемент a^{-1}, такъв че

$$a^{-1}a=aa^{-1}=1.$$

За обратния елемент на произведението ab имаме $(ab)^{-1}=b^{-1}a^{-1}$. Аналогично се намира обратният елемент на произведение от повече от два елемента.

Едно непразно подмножество $H \subset G$ на групата G се нарича *подгрупа* на G, когато произведението на всеки два елемента от H принадлежи на H и обратният елемент на всеки елемент от H също принадлежи на H. Ако под произведение на две подмножества A, B на G разбираме множеството AB, състоящо се от всички произведения ab, $a \in A$, $b \in B$, и под A^{-1} разбираме множеството от всички елементи a^{-1}, където a е произволен елемент на A, условията за подгрупа могат да се запишат така

$$HH \subset H, \; H^{-1} \subset H.$$

От дефиницията за подгрупа директно следва, че единичният елемент e на група G принадлежи на всяка нейна подгрупа H и всяка подгрупа на G може да се разглежда като група относно същата бинарна операция, дефинирана в G.

Броят n на елементите на G се нарича *ред* на групата G и се означава с $|G|=n$. Различаваме *крайни групи* (от краен ред) и *безкрайни групи* (групи с безбройно много елементи).

Ще използваме обичайните означения за степен:

$$\underbrace{aa\ldots a}_{n\text{-пъти}}=a^n, \; a^1=a, \; a^0=1,$$

$$a^{-n}=(a^{-1})^n=(a^n)^{-1}.$$

За всеки цели n и m имаме

$$a^n a^m=a^{n+m} \text{ и } (a^n)^m=a^{nm}.$$

Казваме, че групата G е *абелева* (*комутативна*), когато в G е в сила комутативният закон, т. е. за всеки два елемента a, b от G имаме

$$ab=ba.$$

Освен във вид на произведение (*мултипликативен запис*) груповата операция се означава (*адитивно*) във вид на сбор $a+b$. Адитивният запис на груповата операция се използва главно при разглеждане на абелеви групи. В такъв случай единичният елемент се означава с 0 (нарича се *нулев елемент*), а обратният елемент на a се означава с $-a$ и се нарича *противоположен елемент* на a. В адитивни означения $a+0=a$, $a+(-a)=0$ и в съответствие с определенията и правилата за степенуване ще пишем:

$$\underbrace{a+a+\ldots+a}_{n\text{-пъти}}=na, \quad 1a=a, \quad 0a=0,$$

$$(-n)a=n(-a)=-(na)$$

и за произволни цели числа n и m ще имаме

$$na+ma=(n+m)a, \; m(na)=(nm)a.$$

Циклични групи. Нека a е произволен елемент на дадена група G. Множеството

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

от всички степени на a е група (подгрупа на G), която се нарича циклична група, породена от елемента a. Цикличната група $\{a\}$ е крайна тогава и само тогава, когато съществува естествено число r, за което $a^r=1$. Най-малкото естествено число r за което $a^r=1$, се нарича ред на елемента a. Редът на елемента a съвпада с реда на цикличната група, породена от $\{a\}$. В такъв случай цикличната група $\{a\}$ се състои от следните r на брой различни елементи:

$$1, a, a^2, \ldots, a^{r-1}.$$

Ако за всяко естествено число n имаме $a^n \neq 1$, степените на a са все различни и цикличната група $\{a\}$ е безкрайна, т. е. на елемент от безкраен ред съответствува безкрайна циклична група.

Хомоморфизми и изоморфизъм. Нека G и G' са две групи и φ е изображение на G и G'. Казваме, че φ е *хомоморфно изображение* (*хомоморфизъм*) на G в G', когато при произволни a, $b \in G$ е изпълнено равенството

$$\varphi(ab)=\varphi(a)\varphi(b).$$

Ако φ е взаимно еднозначно изображение на G върху G', казваме, че хомоморфизмът φ е *изоморфизъм*. Две групи G и G' се наричат *изоморфни*, когато съществува изоморфизъм, изобразяващ G върху G'. В такъв случай пишем $G \cong G'$.

Теорема. Всеки две безкрайни циклични групи са изоморфни. Две крайни циклични групи са тогава и само тогава изоморфни, когато са от един и същ ред.

В частност: всяка безкрайна циклична група е изоморфна на групата Z на целите числа относно събирането; всяка крайна циклична група от ред n е изоморфна на мултипликативната група от корените $x_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$, $k=0, 1, 2, \ldots, n-1$, на биномното уравнение $x^n=1$.

Теорема. Всяка подгрупа на циклична група е също циклична.

Разлагане на група по дадена нейна подгрупа. Нека G е група и H е подгрупа на G. Множеството aH, $a \in G$, състоящо се от всички елементи ah, където h пробягва H, се нарича *ляв съседен клас* на подгрупата H, породен от елемента a. Аналогично се дефинира *десен съседен клас* Ha. Лесно се вижда, че $aH=bH$ тогава и само тогава, когато $b^{-1}a \in H$. Следователно за всяко $b \in aH$ имаме $bH=aH$, т. е. левият съседен клас aH се поражда от всеки свой елемент. И така два леви съседни класа или съвпадат, или нямат общи елементи. Ясно е, че $a \in aH$.

Теорема. Всяка група G може да се представи по отношение на коя да е нейна подгрупа H като обединение на всевъзможните различни (и следователно—непресичащи се) съседни класове aH.

Аналогично групата G може да се разбие и на десни съседни класове.

Ако броят на различните съседни класове е краен, той се означава с $(G:H)$ и се нарича *индекс на групата* H в G. Оказва се, че броят на различните десни съседни класове също е равен на $(G:H)$.

Когато групата G е крайна, всяка подгрупа H на G е също крайна и има краен индекс, като при това

$$|G|=|H|.(G:H).$$

Теорема на Лагранж. Редът на всяка подгрупа на крайната група G е делител на реда на G.

Следствие 1. Ако G е крайна група от ред n, то редът на всеки елемент $a \in G$ е делител на n.

Следствие 2. Всяка крайна група от прост ред е циклична.

Следствие 3. Ако G е крайна група от ред n и a е произволен елемент на G, то $a^n=1$.

Нормален делител и факторгрупа. Една подгрупа H на групата G се нарича *нормален делител* на G, когато всеки ляв съседен клас aH е равен на съответния десен съседен клас Ha.

Подгрупата H е нормален делител на G тогава и само тогава, когато $aHa^{-1} \subset H$ за всяко $a \in G$. Оказва се, че в такъв случай е в сила равенството $aHa^{-1}=H$.

Всеки елемент $y=axa^{-1}$ се нарича *спрегнат* на елемента x. Следователно подгрупата H е нормален делител на G тогава и само тогава, когато наред с всеки свой елемент x тя съдържа всички негови спрегнати елементи axa^{-1}, $a \in G$.

Ако H е подгрупа на G и $a \in G$, множеството aHa^{-1} е също подгрупа на G, която се нарича *спрегната* на H. И така подгрупата H е нормален делител на G, когато съвпада с всички свои спрегнати подгрупи aHa^{-1}, $a \in G$. Ето защо вместо нормален делител се употребява още терминът *инвариантна подгрупа*. Нека H е нормален делител на G. Множеството от всичките съседни класове aH, $a \in G$ ще означаваме с G/H. Имаме

$$(aH)(bH)=(ab)H,$$

така че по горната формула можем да въведем бинарна алгебрична операция в G/H. Относно така въведената операция множеството G/H е група с единичен елемент H и обратен елемент на aH, определен от равенството $(aH)^{-1}=a^{-1}H$. Тази група се нарича *факторгрупа* на G по нормалния делител H. Изображението на G в G/H, при което на всеки елемент $a \in G$ се съпоставя съответният му съседен клас aH (т. е. $\nu: a \to aH$) е хомоморфизъм на групата G върху факторгрупата G/H. Нарича се *естествен хомоморфизъм*.

Нека G и G' са групи и φ е хомоморфизъм на G в G'. Множеството

$$\ker \varphi=\{a : a \in G,\ \varphi(a)=e\}$$

е нормален делител на G, който се нарича *ядро на хомоморфизъм* φ.

Множеството

$$\varphi(G)=\{\varphi(a) : a\in G\}$$

е подгрупа на G', която се нарича образ на G при хомоморфизма φ.

Теорема за хомоморфизмите. Нека $G'=\varphi(G)$ е хомоморфен образ на групата G при хомоморфизма φ и $H=\ker\varphi$ да означава ядрото на хомоморфизма φ. Тогава групата $\varphi(G)$ е изоморфна на факторгрупата G/H. По-точно съществува изоморфизъм $\theta: G/H\to\varphi(G)$, така че $\varphi=\theta\circ\nu$, където ν е естественият хомоморфизъм на G върху G/H.

Теорема на Силов

Определение. Нека G е група и p е просто число. Групата G се нарича *p-група*, когато редът на всеки елемент на G е степен на простото число p.

Теорема. Нека G е крайна група от ред, който се дели на простото число p. Тогава G съдържа елемент от ред p.

Следствие. Нека p е просто число. Крайната група G от ред n е p-група тогава и само тогава, когато n е степен на p.

Определение. Нека G е крайна група от ред $n=p^{\lambda}m$, p-просто и $(m,p)=1$. Подгрупата H на G се нарича *силовска p-подгрупа* на G, когато редът на H е p^{λ}.

Теорема на Силов. Нека G е крайна група от ред $n=p^{\lambda}m$, където p е просто и $(m,p)=1$. Тогава:

а) Всяка p-подгрупа на G се съдържа в силовска p-подгрупа.

б) Всеки две силовски p-подгрупи на G са спрегнати.

в) Броят на различните силовски p-подгрупи на G дели m и е сравним с единица по mod p.

Крайни абелеви групи

Определение. Групата G се нарича *декартово* (*директно*) *произведение* на подгрупите си $G_1, G_2,\dots,G_n$, когато всяка G_i е нормална в G и всеки елемент на G еднозначно се представя във вида $x_1x_2\dots x_n$, където $x_i\in G_i$, $i=1,2,\dots,n$.

Основна теорема за крайните абелеви групи. Всяка крайна абелева група се разлага в декартово произведение на циклични групи.

1. Нека P е поле. Покажете, че P е абелева група относно събирането.

2. Нека P е поле. Покажете, че множеството P^* от ненулевите елементи на P е група относно умножението. Покажете, че всички корени на единицата в P образуват подгрупа на P^*.

3. Покажете, че ако R е пръстен с единица, множеството R^* от обратимите елементи на R е група относно умножението.

4. Опишете групата R^* (вж. предната задача), където:

а) $R=Z$ е пръстенът на целите числа;

б) $R=Z[i]$ е пръстенът на целите гаусови числа;

в) $R=Z[\sqrt{2}]$ е пръстенът на числата от вида $a+b\sqrt{2}$; $a, b \in Z$;

г) $R=P[x]$ е пръстенът от полиноми на една променлива над полето P.

5. Покажете, че множеството U от комплексни числа с модул единица е група относно умножението.

6. Нека P е поле. Покажете, че множеството от всички неособени крадратни матрици от даден ред h с елементи от P е група относно обичайното умножение на матрици. Тази група се означава с $GL(n, P)$ и се нарича обща линейна група от ред n над P. При $n>1$ групата не е комутативна.

7. Нека P е поле. Покажете, че всяко едно от следните множества е подгрупа на $GL(n, P)$:

а) множеството от матрици A с детерминанта $|A|=1$;

б) множеството от матрици A с $|A|=\pm 1$;

в) множеството от матрици от вида

$$\begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdot & \cdot & \cdot & \lambda_{1n} \\ 0 & \lambda_{22} & \cdot & \cdot & \cdot & \lambda_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & \lambda_{nn} \end{pmatrix}, \quad \lambda_{ii} \neq 0;$$

г) множеството от матрици от вида

$$\begin{pmatrix} \lambda_{11} & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & \lambda_{22} & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & \lambda_{nn} \end{pmatrix}, \quad \lambda_{ii} \neq 0;$$

д) множеството от неособени матрици с положителни елементи ($P=R$ е полето на реалните числа);

е) множеството от всички ортогонални матрици ($P=R$);

ж) множеството от всички унитарни матрици ($P=C$).

8. Нека P е крайно поле с q елемента. Покажете, че редът на $GL(n, P)$ е $(q^n-q^{n-1})(q^n-q^{n-2}) \dots (q^n-1)$.

Решение. Нека E е n-мерно векторно пространство над полето P с фиксиран базис $l_1, l_2, \dots, l_n$. Съществува еднозначно обратимо съответствие между елементите на $GL(n, P)$ и всевъзможните базиси на E (на матрицата $(\alpha_{ij}) \in GL(n, P)$ съответствува базисът $a_1, a_2, \dots, a_n$, където $a_i = \sum_{j=1}^{n} \alpha_{ij} l_j$). По такъв начин трябва да преброим всичките базиси на пространството E. Елементът a_1 може да бъде кой да е ненулев елемент на E, т. е. той може да бъде избран по q^n-1 различни начина; по-нататък a_2 може да бъде кой да е елемент на E, непринадлежащ на подпространството, породено от a_1. Последното има q елемента. Следователно a_2

може да се избере по q^n-q начина. Продължавайки така a_{k+1} може да бъде произволен елемент, непринадлежащ на пространство, породено от $a_1, a_2, \ldots, a_k$. Последното има q^k елемента и за a_{k+1} остават q^n-q^k възможности. Следователно E има точно $(q^n-q^{n-1})(q^n-q^{n-2})\ldots(q^n-1)$ различни базиса.

9. Нека P е крайно поле с q елемента. Намерете редовете на подгрупите на $GL(n, P)$, въведени в зад. 7, а, б, в, г.

Отг. а) $(q^n-q^{n-1})(q^n-q^{n-2})\ldots(q^n-q^2)$;
б) $2(q^n-q^{n-1})(q^n-q^{n-2})\ldots(q^n-q^2)$
в) $q^{\frac{n(n-1)}{2}}\cdot(q-1)^n$; г) $(q-1)^n$.

10. Нека M е крайно множество с n елемента. Покажете, че всички субституции на M образуват група относно обичайното умножение на субституции (произведението $\sigma\tau$ на две субституции σ и τ се дефинира със $\sigma\tau(x)=\sigma(\tau(x))$ за $x\in M$). Тази група се нарича *симетрична група* от степен n и се означава с S_n. Покажете, че редът на S_n е $n!$.

11. Нека M е крайно множество. Една субституция τ на M се нарича *транспозиция*, когато съществуват елементи $x, y\in M$, така че $x\neq y$, $\tau(x)=y$, $\tau(y)=x$ и $\tau(z)=z$ при $z\neq x, y$. В такъв случай се използува означението $\tau=(x, y)$. Покажете, че всяка транспозиция τ е от втори ред, т. е. $\tau^2=e$; в частност $\tau=\tau^{-1}$. Докажете равенствата

$$(x, y)(z, t)=(z, t)(x, y) \text{ при } \{x, y\}\cap\{z, t\}=\varnothing;$$
$$(x, z)(y, z)=(x, y)(x, z) \text{ при } x\neq y,$$
$$(x, y)(x, z)=(x, z)(v, z) \text{ при } y\neq z.$$

12. Нека M е крайно множество. Покажете, че всяка субституция на M може да се представи като произведение на транспозиции. С други думи, транспозициите пораждат симетричната група S_n.

Решение. Нека σ е произволна субституция на M. Ще разсъждаваме индуктивно по броя k на елементите на M, които действително се разместват от σ, т. е. k е броят на тези елементи на M, за които $\sigma(x)\neq x$. При $k=0$ твърдението е очевидно (σ е единичната субституция, която по дефиниция е произведение на нула транспозиции). Нека $k>0$ и нека $x\in M$ е такъв, че $\sigma(x)=y\neq x$. Да означим с τ транспозицията, разместваща x и y. В такъв случай субситуцията $\tau\sigma$ размества по малко от k елемента на M, следователно $\tau\sigma=\tau_1\tau_2\ldots\tau_e$, където τ_i са транспозиции. Като умножим по τ и вземем пред вид че $\tau^2=e$, получаваме $\sigma=\tau\,\tau_1\ldots\tau_e$.

13. Нека M е крайно множество. Покажете, че ако произведението на няколко транспозиции съвпада с единичната субституция, то броят на тези транспозиции е четен.

Решение. Твърдението ще докажем по индукция по броя s на елементите на M, които участвуват в някоя от разглежданите транспозиции. При $s=2$ очевидно всички транспозиции са равни помежду си, така че имаме равенство от вида $\tau^k=e$. От $\tau^2=e$ следва, че k е четно. Нека сега имаме равенство от вида

$$(x_1, x_2)(x_3, x_4)\ldots(x_{2q-1}, x_{2q})=e,$$

в което измежду елементите $x_1, x_2, \ldots, x_{2q}$ има $s>2$ различни. Нека x е един от тези елементи. Използувайки равенствата от задача 11, от разглежданото равенство можем да получим равенството от вида

$$(x, y_1)\ldots(x, y_p)(z_1, z_2)\ldots(z_{2r-1}, z_{2r})=e,$$

в което лявата страна има същия брой множители и елементите $z_1, z_2, \ldots, z_{2r}$ са различни от x. Ако $p>1$, като използуваме равенството $(a, b)(a, c)=(a, c)(b, c)$ или $(a, b)(a, b)=e$, можем да преминем към произведение със същата четност на броя на множителите, но с по-малко p. Продължавайки така, ще достигнем до произведение, в което или не участвуват транспозиции, съдържащи x, или участвува само една такава. Вторият случай обаче е невъзможен, защото в такъв случай произведението не може да бъде единичната субституция. Следователно налице е първият случай, т. е. в така преобразуваното произведение ще участвуват $<s$ елемента и следователно броят на множителите е четен.

14. Нека M е крайно множество с n елемента. Покажете, че ако една субституция σ на M може да се представи като произведение на четен брой транспозиции, то всяко нейно представяне като произведение на транспозиции съдържа четен брой множители. В такъв случай субституцията σ се нарича *четна.* Покажете, че четните субституции на M образуват подгрупа на S_n, която се нарича *алтернативна група* от степен n и се означава с A_n. Покажете също, че A_n е нормална подгрупа на S_n и че редът на A_n е $\frac{n!}{2}$.

Упътване. Използувайте предната задача.

15. Нека $M=\{1, 2, \ldots, n\}$ и σ е субституция на M. Двойката числа $i, j \in M$ се нарича **инверсия** на σ, ако $i<j$, но $\sigma(j)<\sigma(i)$. Покажете, че субституцията σ е четна тогава, когато има четен брой инверсии.

Упътване. Покажете, че ако τ е транспозиция, броят на инверзиите на $\sigma\tau$ се различава от броя на инверзиите на σ с нечетно число.

16. Една субституция σ на множеството M се нарича *цикъл с дължина* k, когато съществуват k различни елемента $x_1, x_2 \ldots, x_k$ на M, така че $\sigma(x_i)=x_{i+1}$ при $i=1, 2, \ldots, k-1$; $\sigma(x_k)=x_1$ и $\sigma(x)=x$ при $x \neq x_i$. В такъв случай се използува означението $\sigma=(x_1, x_2, \ldots, x_k)$. Два цикъла $\sigma=(x_1, x_2, \ldots, x_k)$ и $\tau=(y_1, y_2, \ldots, y_e)$ се наричат *независими*, ако $\{x_1, \ldots, x_k\} \cap \{y_1, \ldots, y_e\}=\emptyset$. Покажете, че всеки два независими цикъла комутират помежду си (т. е. $\sigma\tau=\tau\sigma$) и че всяка субституция на M еднозначно може да се представи като произведение на независими цикли.

17. Покажете, че редът на цикъл с дължина k е точно k. По-общо редът на една произволна субституция σ е равен на най-малкото общо кратно на дължините на циклите, които участвуват в представянето ѝ като произведение на независими цикли.

18. Един цикъл с дължина k е четна субституция тогава и само тогава, когато k е нечетно. По-общо една субституция е четна тогава и само тогава, когато в представянето ѝ като произведение на независими цикли участвуват четен брой цикли с четна дължина.

19. Разложете на независими цикли и намерете редовете на следните субституции

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 12 & 8 & 11 & 6 & 7 & 5 & 3 & 2 & 4 & 10 & 1 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$;

в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 5 & 1 & 8 & 7 & 2 & 3 & 4 \end{pmatrix}$; г) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 1 & 3 & 5 & 8 & 7 \end{pmatrix}$;

д) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 3 & 4 & 1 \end{pmatrix}$; е) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 8 & 3 & 1 & 6 & 5 & 9 & 4 \end{pmatrix}$.

Отг. а)(1, 9, 2, 12)(3, 8)(4, 11, 10)(5, 6, 7), 12; б) (1, 2, 3)(4, 5, 6, 8), 12; в) (1, 9, 4)(2, 6, 7)(3, 5, 8), 3; г) (1, 2, 4)(3, 6, 5)(7, 8), 6; д) (1, 2, 5, 4, 3, 6), 6; е) (1, 2, 7, 5)(3, 8, 9, 4), 4.

20. Намерете всички подгрупи на симетричната група S_3.

Отг. $\{e\}$, $\{e, (1, 2)\}$, $\{e, (1, 3)\}$, $\{e, (2, 3)\}$, $\{e, (1, 2, 3), (2, 3, 1)\}$, S_3.

21. Нека $a=(1, 2, 3, 4)(5, 6, 7, 8)$, $b=(1, 5, 3, 7)(2, 6, 4, 8)$. Покажете, че подгрупата H на S_8, породена от a и b, е от осми ред и че тази подгрупа съдържа единствен елемент от втори ред.

22. Нека $G=\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$ е множество с осем елемента. В G въвеждаме алгебрична операция с помощта на следната таблица

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_2	x_2	x_5	x_4	x_7	x_6	x_1	x_8	x_3
x_3	x_3	x_8	x_5	x_2	x_7	x_4	x_1	x_6
x_4	x_4	x_3	x_6	x_5	x_8	x_7	x_2	x_1
x_5	x_5	x_6	x_7	x_8	x_1	x_2	x_3	x_4
x_6	x_6	x_1	x_8	x_3	x_2	x_5	x_4	x_7
x_7	x_7	x_4	x_1	x_6	x_3	x_8	x_5	x_2
x_8	x_8	x_7	x_2	x_1	x_4	x_3	x_6	x_5

Покажете, че множеството G е група относно тази операция, която не е абелева, но всяка нейна подгрупа е нормална.

23. Нека G е група и H е подгрупа на G. Покажете, че съседните класове Hx и Hy съвпадат тогава и само тогава, когато $xy^{-1} \in H$. Покажете също, че $Hx=Hz$ за всяко $z \in Hx$. Следователно групата G се разлага в обединение на непресичащи се леви съседни класове по подгрупата H.

24. Покажете, че изображението $Hx \to x^{-1}H$ установява еднозначно обратимо съответствие между левите и десните съседни класове по подгрупата H. Следователно броят (краен или безкраен) на левите съседни класове е равен на броя на десните съседни класове. По дефиниция този брой е индексът на H в G, означаван с $(G:H)$.

25. Покажете, че изображението $h \to hx$ установява еднозначно обратимо съответствие между елементите на подгрупата H и елементите на съседния клас Hx. Следователно броят на елементите на Hx е равен на броя на елементите на H, означаван с $|H|$.

26. Като използувате предните задачи, докажете теоремата на Лагранж: за всяка подгрупа H на крайната група G е изпълнено равенството $|G|=(G:H).|H|$.

27. Нека G е група и $G=G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n=\{e\}$ е редица от подгрупи на G. Докажете, че

$$|G|=(G_0:G_1)(G_1:G_2)\ldots(G_{n-1}:G_n).$$

Упътване. Приложете неколкократно теоремата на Лагранж.

28. Нека G е група и H е подгрупа на G. Покажете, че подгрупата H е нормална тогава и само тогава, когато всеки ляв съседен клас по H е същевременно десен.

Решение. Ако H е нормална, то $x^{-1}Hx=H$ за всяко $x \in G$ или все едно $Hx=xH$, следователно класът Hx съвпада с xH. Обратно, нека всеки ляв съседен клас е десен и нека $x \in G$. Тогава съществува $y \in G$, така че $Hx=yH$. В частност $x \in yH$ и следователно $yH=xH$. По такъв начин $Hx=xH$ или все едно $x^{-1}Hx=H$.

29. Нека G е група. Покажете, че всяка подгрупа на G с индекс 2 е нормална.

Упътване. Използувайте предната задача.

30. Нека G е група и H е нормална подгрупа на G. Покажете, че всяка подгрупа на G/H има вида G'/H, където G' е подгрупа на G, съдържаща H. Покажете също, че ако $H \subset G' \subset G$ и $H \subset G'' \subset G$, то $G'/H=G''/H$ тогава и само тогава, когато $G'=G''$. По такъв начин се установява еднозначно обратимо съответствие между подгрупите на G/H и подгрупите на G, съдържащи H. По-нататък покажете, че $(G:G')=(G/H:G'/H)$; подгрупата G'/H е нормална в G/H тогава и само тогава, когато G' е нормална в G и в такъв случай факторгрупите G/G' и $(G/H)/(G'/H)$ са изоморфни.

Решение. Очевидно, ако G' е подгрупа на G, съдържаща H, то G'/H е подгрупа на G/H. Ако в G' и G'' са две такива подгрупи и $G'/H=G''/H$, то за всеки елемент x на G' съществува $y \in G''$, така че $xy^{-1} \in H \subset G''$. Следователно $x \in G''$, т. е. $G' \subset G''$ и аналогично $G'' \subset G'$. По такъв начин $G'/H=G''/H$ тогава и само тогава, когато $G'=G''$. Сега, ако K е подгрупа на G/H, да означим с G' обединението на елементите на K (които са подмножества на G). Непосредствено се проверява, че G' е подгрупа на G, съдържаща H и че $G'/H=K$. По-нататък, ако $G'x_1, G'x_2, \ldots, G'x_n$ са всички два по два непресичащи се леви съседни класове по подгрупата G', то, както лесно се доказва, $(G'/H)Hx_1, (G'/H)Hx_2, \ldots, (G'/H)Hx_n$ ще изчерпват всички леви съседни класове на G/H по подгрупата G'/H и два по два тези класове не се пресичат, следователно $(G;G')=(G/H:G'/H)$. Твърдението за нормалността се доказва също така непосредствено. Накрая изоморфизмът $G/G' \cong (G/H)/(G'/H)$ се получава, като на $xG' \in G/G'$ се съпостави $(Hx)(G'/H) \in (G/H)/(G'/H)$.

31. Нека G е група и A, B са подгрупи на G. Покажете, че множеството AB съдържа точно $\frac{|A||B|}{|A \cap B|}$ елемента.

32. Нека G е група, H е нормална подгрупа на G и K е произволна подгрупа на G. Покажете, че $HK=KH$ и че множеството HK е подгрупа на G, съдържаща H. Покажете също, че факторгрупата HK/H е изоморфна с $K/H\cap K$.

Упътване. На всеки елемент $x(H\cap K)\in K/H\cap K$ съпоставете елемента $xH\in HK/H$.

33. Нека G е крайна група и H е нормална подгрупа на G, индексът на която е взаимно прост с реда ѝ, т. е. $((G:H), |H|)=1$. Покажете, че всяка подгрупа K на G, чийто ред дели реда на H, се съдържа в H.

Решение. Съгласно предните две задачи HK е подгрупа на G, чийто ред е $|HK|=\frac{|H||K|}{|H\cap K|}$. Но по теоремата на Лагранж $|HK|=|H|(HK:H)$, следователно

$$|H|(HK:H)=\frac{|H||K|}{|H\cap K|}$$

или

$$\frac{(HK:H)|H\cap K|}{|K|}=1.$$

От включванията $G\supset HK\supset H$ следва $(G:H)=(G:HK)(HK:H)$, така че $(HK:H)$ дели $(G:K)$. Следователно $(|K|, (HK:H))=1$ (в противен случай $(G:H)$ и $|H|$ ще имат общ делител $|K|$). Но тогава от горното равенство следва, че $|K|$ дели $|K\cap H|$ и в частност $|K|\leq|K\cap H|$. От друга страна, $K\cap H\subset K$, откъдето $|K\cap H|\leq|K|$ и следователно $|K\cap H|=|K|$, т. е. $K=H\cap K$ или все едно $K\subset H$.

34. Нека G е група и x, y са два елемента на G с взаимно прости редове n и m. Покажете, че ако елементите x и y комутират, т. е. ако $xy=yx$, то редът на произведението xy е равен на nm.

Решение. Първо ще отбележим, че ако елементите x и y комутират, то $(xy)^k=x^k y^k$ за всяко k. Нека редът на xy е r. Имаме $(xy)^{nm}=x^{nm}y^{nm}=e$, следователно $r\leq nm$. От друга страна, от $(xy)^r=e$ следва $x^r=y^{-r}$. Повдигайки в степен m, получаваме $x^{rm}=e$, следователно n дели rm. Но $(n, m)=1$, следователно n дели r. Аналогично и m дели r, откъдето и произведението nm дели r, тъй като $(n, m)=1$.

35. Нека G е група и $x\in G$ е елемент с краен ред n. Покажете, че $x^m=e$ тогава и само тогава, когато n дели m. По-общо $x^{m_1}=x^{m_2}$ тогава и само тогава, когато $m_1\equiv m_2 \pmod n$.

Решение. Очевидно, ако $n|m$, то $x^m=e$. Обратно, нека $x^m=e$ и нека $m=qn+r$, $0\leq r<n$. Имаме $x^m=x^{qn}x^r=x^r$, следователно $x^r=e$. От $0\leq r<n$ и $x^r=e$ следва $r=0$, т. е. $n|m$. По-общото твърдение следва от доказаното, като вземем пред вид, че $x^{m_1}=x^{m_2}$ тогава и само тогава, когато $x^{m_1-m_2}=e$.

36. Нека G е крайна група от ред n. Покажете, че редът на всеки елемент на G дели n. В частност $x^n=e$ за всяко $x\in G$.

Упътване. Използвайте факта, че редът на елемента x съвпада с реда на цикличната подгрупа на G, породена от x.

37. Нека G е група и x е елемент с краен ред n. Покажете, че редът на елемента x^k е равен на $\frac{n}{(n, k)}$.

Решение. Нека редът на x^k е r и нека $(n, k)=d$, $n=n_1 d$, $k=k_1 d$. Имаме $(x^k)^{n_1}=x^{nk_1}=e$, следователно $r \leq n_1$. От друга страна, $x^{kr}=e$, откъдето n дели kr, т. е. n_1 дели $k_1 r$. Тъй като $(n_1, k_1)=1$, n_1 дели r и следователно $n_1 \leq r$.

38. Нека G е безкрайна циклична група. Покажете, че G има точно две образуващи — ако едната от тях е g, другата е g^{-1}.

39. Нека G е крайна циклична група от ред n. Покажете, че G има точно $\varphi(n)$ различни образуващи.

Упътване. Използвайте зад. 37.

40. Покажете, че всяка група, чийто ред е просто число, е циклична.

41. Покажете, че всяка подгрупа и факторгрупа на циклична група е циклична група.

Решение. Твърдението за факторгрупа е очевидно. Нека H е подгрупа на цикличната група G с образуващ елемент g и нека k е най-малкото цяло положително число, за което $g^k \in H$. Да означим с K цикличната група, породена от g^k. Ще покажем, че $K=H$. Очевидно $K \subset H$. Нека g^l е произволен елемент на H и нека $l=kq+r$, $0 \leq r<k$. Тогава $g^l=(g^k)^q g^r$ и следователно $g^r \in H$, понеже $g^l \in H$ и $g^{kq} \in H$. Оттук следва $r=0$, т. е. $g^l=(g^k)^q \in K$.

42. Покажете, че произведението на две крайни циклични групи е циклична група тогава и само тогава, когато редовете им са взаимно прости.

Упътване. Използвайте зад. 34.

43. Нека G е безкрайна циклична група. Покажете, че за всяко естествено число[1] n, G съдържа единствена подгрупа с индекс n.

Решение. Нека H е подгрупата на G, породена от g^n. Тогава $(G:H)=n$. Нека $(G:K)=n$. Тогава редът на факторгрупата G/K е n и следователно $(gK)^n=K$, т. е. $g^n \in K$, откъдето $H \subset K$. Съгласно теоремата на Лагранж $(G:H)=(G:K)(K:H)$, откъдето $(K:H)=1$, т. е. $K=H$.

44. Нека G е крайна циклична група от ред n. Покажете, че за всеки делител m на n, G съдържа единствена подгрупа от ред m.

Упътване. Вж. предишната задача.

45. Нека G е група и $a, b \in G$. Покажете, че елементите a и $b^{-1}ab$ имат един и същ ред.

46. Нека G е група и $a, b \in G$. Покажете, че елементите ab и ba имат един и същ ред.

47. Нека G е група, H е подгрупа на G и S е подмножество на G. Покажете, че множеството $N_H(S)=\{x \in H: xSx^{-1}=S\}$ е подгрупа на H. В частност $N(S)=N_G(S)$ е подгрупа на G, която се нарича *нормализатор* на S. Покажете също, че ако S е подгрупа на G, то S е нормална подгрупа на $N(S)$.

48. Нека G е група, H е подгрупа на G и S е подмножество на G. Покажете, че множеството $C_H(S)=\{x \in H: x^{-1}yx=y$ за всяко y от $S\}$ е подгрупа на H, съдържаща се в $N_H(S)$. В частност $C(S)=C_G(S)$ е подгрупа на G, която се нарича *централи-*

затор на G. Подгрупата $C_G(G)$ се нарича *център* на G. (По дефиниция $C(G)$ се състои от всички елементи на G, които комутират с всеки елемент на G.) Покажете, че центърът $C(G)$ е нормална подгрупа на G.

Забележка. Ако $S=\{x\}$ е множество, състоящо се от един елемент x, очевидно $N(x)=C(x)$.

49. Нека G е група и H е нейна подгрупа. Две подмножества S_1 и S_2 на G се наричат спрегнати относно H (означение $S_1 \underset{H}{\sim} S_2$), ако съществува $x \in H$, така че $S_1=xS_2x^{-1}$. (При $H=G$ казваме просто, че S_1 и S_2 са спрегнати.) Покажете, че релацията спрегнатост е релация на еквивалентност, т. е. че са в сила:

а) $S \underset{H}{\sim} S$;

б) ако $S_1 \underset{H}{\sim} S_2$, то и $S_2 \underset{H}{\sim} S_1$;

в) ако $S_1 \underset{H}{\sim} S_2$ и $S_2 \underset{H}{\sim} S_3$, то $S_1 \underset{H}{\sim} S_3$.

50. Нека G е група, H е нейна подгрупа и S е подмножество на G. Покажете, че броят на всички спрегнати относно H с S подмножества на G е равен на $(H:N_H(S))$. В частност броят на спрегнатите с S подмножества на G е равен на $(G:N(S))$.

Упътване. Ако $x_1, x_2, \ldots, x_n$ е система представители на левите съседни класове на групата H по подгрупата $N_H(S)$, покажете, че множествата $x_1Sx_1^{-1}$, $x_2Sx_2^{-1}, \ldots, x_nSx_n^{-1}$ са две по две различни и изчерпват всички H-спрегнати с S подмножества на G.

51. Нека G е крайна група и H е собствена подгрупа на G. Покажете, че G не съвпада с обединението на всички спрегнати с H подгрупи.

Решение. Нека броят на всички спрегнати с H подгрупи на G е m. Съгласно предната задача $m=(G:N_G(H))$. Но $H \subset N(H)$, следователно $m \leq (G:H)$. И така броят на всички спрегнати с H подгрупи на G е по-малък или равен от $(G:H)$ и всяка такава подгрупа има точно $|H|$ елемента. Като вземем пред вид, че тези групи имат общ елемент (единицата) получаваме, че обединението им има по-малко от $|H|.(G:H)=|G|$ елементи.

52. Покажете, че единствената група, която има точно два класа спрегнати елементи, е цикличната група от ред 2.

Упътване. Под клас спрегнати елементи разбираме такова подмножество на G, което се състои от всички елементи на G, спрегнати с даден елемент. Съгласно зад. 50 броят на елементите на всеки клас дели реда на G. Също така множеството, съставено само от единицата, е клас от спрегнати елементи.

53. Опишете всички групи, които имат точно три класа спрегнати елементи.

Решение. Нека G има три класа спрегнати елементи C_0, C_1, C_2 и нека $C_0=\{e\}$. Да означим с n реда на G, а с n_i $i=1, 2$, броя на елементите на C_i. Имаме $1+n_1+n_2=n$, n_1/n, n_2/n. Оттук имаме $n_1/(1+n_2)$, $n_2/(1+n_1)$, откъдето следва $n_1=n_2=1$ или $n_1=2$, $n_2=3$. В първия случай G е циклична група от трети ред, а във втория случай — неабелева група от шести ред.

54. Да се докаже, че ако всички различни от единица елементи на групата G са от втори ред, то тя е абелева.

55. Докажете, че ако a е единствен елемент от втори ред на групата G, то $a \in C(G)$.

56. Докажете, че центърът на групата от неизродените матрици от даден ред е различен от единичната подгрупа.

57. Намерете центъра на симетричната група S_3.

Отг. Единичната подгрупа.

58. Докажете, че всяка група от четвърти ред е абелева.

59. Докажете, че съществуват точно две неизоморфни групи от четвърти ред.

60. Докажете, че съществуват точно две неизоморфни групи от шести ред.

Определение. Елементът $x^{-1}y^{-1}xy$, $x \in G$, $y \in G$, се нарича *комутатор* на елементите x и y и се бележи с $[x, y]$.

61. Проверете равенството

$$xy = yx[x, y]$$

за произволни елементи x, y от групата G.

62. Намерете комутатора на елементите $(1, 2)$, $(1, 3)(2, 4)$ в симетричната група S_4.

Отг. $(12)(34)$.

63. Пресметнете комутаторите $[u, v]$, $[v, w]$ и $[w, u]$ на елементите

$$u=\begin{pmatrix}1&0&0\\0&2&0\\0&0&3\end{pmatrix},\quad v=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix},\quad w=\begin{pmatrix}0&0&1\\0&2&0\\3&0&0\end{pmatrix}$$

в групата на неособените квадратни матрици от трети ред.

Отг. $[u, v]=\begin{pmatrix}1&-1&-1\\0&1&-\frac{1}{2}\\&0&1\end{pmatrix}$, $[v, w]=\begin{pmatrix}-\frac{1}{2}&-1&0\\-\frac{3}{2}&-1&-1\\3&2&1\end{pmatrix}$, $[w, u]=\begin{pmatrix}\frac{1}{3}&0&0\\0&1&0\\0&0&3\end{pmatrix}$

Определение. Нека G е произволна група. Подгрупата на G, породена от всевъзможните комутатори $[x, y]$, $x \in G$, $y \in G$ (т. е. минималната подгрупа на G, съдържаща всичките комутатори $[x, y]$, $x \in G$, $y \in G$) се нарича *комутант* на G и се означава с $[G, G]$.

64. Докажете, че комутанта на всяка група G е нормален делител на G.

65. Докажете, че всяка подгрупа на групата G, която съдържа комутанта $[G, G]$, е нормален делител на G.

Решение. Нека $G \supset H \supset [G, G]$, $h \in H$, $g \in G$. Тъй като $ghg^{-1}h^{-1} \in [G, G]$, то $ghg^{-1}h^{-1} \in H$. Следователно $ghg^{-1} \in H$ за всяко $h \in H$ и всяко $g \in G$, т. е. H е нормален делител на G.

66. Нека H е нормален делител на G. Докажете, че фактор-групата G/H е абелева тогава и само тогава, когато H съдържа комутантата на G.

Решение. Нека H е нормален делител на G, $G \supset H \supset [G, G]$ и ν е естественият хомоморфизъм на G върху G/H. Тъй като $g_1g_2 = g_2g_1[g_1, g_2]$ за всеки два елемента g_1 и g_2 от G, то

$$\nu(g_1)\nu(g_2) = \nu(g_1g_2) = \nu(g_2g_1) = \nu(g_2)\nu(g_1).$$

Следователно G/H е абелева.

Обратно, нека H е нормален делител на G и факторгрупата G/H е абелева. За всеки два елемента g_1 и g_2 от G имаме

$$\nu([g_1, g_2]) = \nu\left(g_1^{-1} g_2^{-1} g_1 g_2\right) = \nu(e) = \bar{e}.$$

Следователно $[g, g_2] \in H$, т. е. $[G, G] \subset H$.

67. Намерете комутанта на симетричната група S_n, $n > 2$.

Отг. Алтернативната група A_n.

68. Нека H е нормален делител, съдържащ се в центъра на групата G. Докажете, че ако факторгрупата G/H е циклична, то G е абелева група.

Решение. Нека $\nu : G \to G/H$ е естественият хомоморфизъм на G върху G/H и нека G/H се поражда от елемента $\bar{a} = \nu(a)$. Тогава всеки елемент $g \in G$ е от вида $a^k h$, където h е елемент от центъра на G. Тъй като всеки два елемента от този вид комутират, то G е абелева.

69. Намерете комутанта на групата на неособените квадратни матрици от втори ред.

Отг. Подгрупата, състояща се от всички матрици с детерминанта 1.

70. Нека G е адитивната група на целите числа. Проверете кои от следните преобразувания φ_1, φ_2 и φ_3 са автоморфизми на G:

а) $\varphi_1(n) = n + 1$;

б) $\varphi_2(n) = 2n$;

в) $\varphi_3(n) = -n$.

Отг. φ_3 е автоморфизъм.

71. Нека G е мултипликативната група на всичките комплексни числа. Проверете кои от следните преобразувания φ_1, φ_2 и φ_3 са автоморфизми на G:

а) $\varphi_1(z) = \bar{z}$;

б) $\varphi_2(r(\cos\varphi + i\sin\varphi)) = r^2(\cos\varphi + i\sin\varphi)$;

в) $\varphi_3(r(\cos\varphi + i\sin\varphi)) = r\left[\cos\left(\varphi + \frac{\pi}{2}\right) + i\sin\left(\varphi + \frac{\pi}{2}\right)\right]$.

Отг. φ_1 и φ_2 са автоморфизми

72. Нека φ е автоморфизъм на групата G. Докажете, че:

а) $\varphi(e) = e$;

б) $\varphi(a^{-1}) = [\varphi(a)]^{-1}$;

в) елементите a и $\varphi(a)$ имат един и същ ред за всеки елемент $a \in G$;

г) всеки клас спрегнати елементи на G се преобразува в клас спрегнати елементи.

73. Покажете, че множеството на всичките автоморфизми на дадена група G е група по отношение на обичайното умножение на преобразувания.

74. Намерете групата от автоморфизмите на безкрайната циклична група.

Отг. Цикличната група от втори ред.

75. Нека G е циклична група от ред n. Докажете, че преобразуванието φ, определено от равенството $\varphi(x)=x^k$, $x \in G$, е автоморфизъм на G тогава и само тогава, когато k е взаимно просто с n. Докажете, че с описаните по-горе преобразувания се изчерпват всичките автоморфизми на G.

76. Нека G е подгрупа на симетричната група S_6, породена от елементите $(1, 2)(3, 4)(5, 6)$, $(3, 4)$. Покажете, че групата G е комутативна и се състои от елементите e, $(1, 2)(3, 4)(5, 6)$, $(3, 4)$, $(1, 2)(5, 6)$. Докажете, че групата от автоморфизмите на G е изоморфна със симетричната група S_3.

77. Докажете, че групата от автоморфизмите на всяка циклична група от ред, по-голям от 2, е комутативна група от четен ред.

Упътване. Използувайте зад. 75.

78. Опишете групата от автоморфизмите на цикличната група от ред 14.

Отг. Циклична група от шести ред.

79. Нека G е група и $a \in G$. Докажете, че преобразуването τ_a, определено с равенството $\tau_a(x)=a x a^{-1}$, $x \in G$, е автоморфизъм на групата G.

Определение. Автоморфизмът τ_a, определен с равенството $\tau_a(x)=a x a^{-1}$, $a \in G$, $x \in G$ (вж. предната задача) се нарича *вътрешен автоморфизъм* на групата G.

80. Намерете вътрешните автоморфизми τ_{a_1} и τ_{a_2} на симетричната група S_3, където $a_1=(1, 2,)$, $a_2=(1, 3, 2)$.

Отг. Ако с a_3, a_4, a_5 са означени съответно елементите $(1, 3)$, $(2, 3)$, $(1, 2, 3)$

то $\tau_{a_1}=\begin{pmatrix} e & a_1 & a_2 & a_3 & a_4 & a_5 \\ e & a_1 & a_5 & a_4 & a_3 & a_2 \end{pmatrix}$, $\tau_{a_2}=\begin{pmatrix} e & a_1 & a_2 & a_3 & a_4 & a_5 \\ e & a_3 & a_2 & a_4 & a_1 & a_5 \end{pmatrix}$

81. Докажете, че вътрешните автоморфизми на групата G образуват инвариантна подгрупа на G, която е изоморфна на факторгрупата $G/C(G)$ на G по нейния център $C(G)$.

82. Докажете, че симетричната група S_n, $n \geq 3$, е изоморфна с групата на нейните вътрешни автоморфизми.

83. Докажете, че при всеки автоморфизъм на S_n, $n \geq 3$, $n \neq 6$, всяка транспозиция се преобразува в транспозиция.

Упътване. Пресметнете броя на елементите във всеки клас спрегнати елементи от втори ред и използувайте предната задача.

84. Докажете, че всеки автоморфизъм на S_n, $n \geq 3$, $n \neq 6$, преобразува множеството от различни транспозиции от вида (i, j_1), $(i, j_2), \ldots, (i, j_s)$ в множеството от транспозиции от вида (k, l_1), $(k, l_2), \ldots, (k, l_s)$.

85. Докажете, че всеки автоморфизъм на групата S_4 е вътрешен.

Упътване. Нека φ е автоморфизъм на групата S_4. Съгласно предната задача за образите на елементите $(1, 2)$, $(1, 3)$ и $(1, 4)$ ще имаме $\varphi((1, 2))=(\alpha, \beta)$, $\varphi((1, 3))=(\alpha, \gamma)$, $\varphi((1, 4))=(\alpha, \delta)$. Разгледайте вътрешния автоморфизъм τ_a, където

$$a=\begin{pmatrix}1 & 2 & 3 & 4\\ \alpha & \beta & \gamma & \delta\end{pmatrix}.$$

86. Намерете реда на групата от автоморфизмите на симетричната група S_4.

Отг. 24.

87. Докажете, че групата от автоморфизмите на адитивната група на целите гаусови числа е изоморфна на групата от целочислените квадратни матрици от втори ред с детерминанта ± 1.

88. Нека K е множество, състоящо се от осем елемента, които ще означаваме с $1, -1, i, j, k, -i, -j, -k$. В множеството K въвеждаме бинарна операция умножение с помощта на следната таблица:

	1	-1	$-i$	i	$-j$	j	$-k$	k
1	1	-1	$-i$	i	$-j$	j	$-k$	k
-1	-1	1	i	$-i$	j	$-j$	k	$-k$
i	i	$-i$	1	-1	$-k$	k	j	$-j$
$-i$	$-i$	i	-1	1	k	$-k$	$-j$	j
j	j	$-j$	k	$-k$	1	-1	$-i$	i
$-j$	$-j$	j	$-k$	k	-1	1	i	$-i$
k	k	$-k$	$-j$	j	i	$-i$	1	-1
$-k$	$-k$	k	j	$-j$	$-i$	i	-1	1

Докажете, че множеството K е група по отношение на въведената по-горе операция. Тази група се нарича *група на кватернионите.*

89. Нека K е групата на кватернионите (вж. предишната задача). Докажете, че:

а) всяка подгрупа на K е инвариантна;

б) комутанта $[K, K]$ съвпада с центъра на K и е циклична група от втори ред;

в) групата от вътрешните автоморфизми на K е директно (Декартово) произведение на две циклични групи от втори ред.

90. Нека H е инвариантна p-подгрупа на крайната група G. Докажете, че H се съдържа във всяка силова p-подгрупа на G.

91. Нека G е група от ред pq, p и q — различни прости числа, $p<q$. Докажете, че ако $p \nmid q-1$, G е циклична.

92. Докажете, че всяка група G от ред p^2q има инвариантна силова подгрупа.

Решение. Нека $p>q$. Броят на силовите p-подгрупи е число от вида $1+kp$ и дели q, т. е. е равно на единица. Силовата p-подгрупа е единствена и следователно инвариантна в G. Нека сега $q>p$. Броят на силовите q-подгрупи на G е от вида $1+lq$ и дели p^2. Но $1+lq>p^2$ и следователно $1+lq=p^2$ или броят на силовите q-подгрупи на G е 1. От $lq=(p-1)(p+1)$ и $q>p$ следва, че $q|p+1$, т. е. $q=p+1$. Това е възможно само при $p=2$, $q=3$. Но в група от ред $2^2.3$ силовите 3-подгрупи са циклични от ред 3, така че две такива или съвпадат, или не се пресичат. Ако броят им е 4, то те съдържат общо $4(3-1)+$ $+1=9$ различни елементи и остават още 3 елемента, които заедно с 1 образуват единствена силова 2-подгрупа от ред 4, която е инвариантна.

93. Докажете, че ако G е група от ред p^2q, $p>q$ и $q\nmid p^2-1$, то G е абелева.

94. Докажете, че всяка група от ред 200 има инвариантна силова подгрупа.

95. Колко елемента от ред 7 има в простата група от ред 168?

Решение. Имаме $168=2^3.3.7$. Броят на силовите 7-подгрупи е число от вида $1+7k$ и дели 24. Понеже G е проста, тя не притежава собствена инвариантна подгрупа. Следователно G притежава точно 8 силови 7-подгрупи, които са циклични от прост ред и нямат общи елементи освен 1. И така в G има точно $8(7-1)=48$ елемента от ред 7.

96. Докажете, че ако P е силова p-подгрупа на крайната група G и H е инвариантна подгрупа на G, то $P\cap H$ е силова p-подгрупа в H, а PH/H е силова p-подгрупа във факторгрупата G/H.

97. Докажете, че ако P е неабелева p-група от ред p^n, то редът на центъра ѝ не надминава p^{n-2}.

Упътване. Използувайте зад. 68.

98. Докажете, че всяка група от ред p^2 е абелева, а центърът на една неабелева група от ред p^3 има ред p.

99. Докажете, че крайната група G има точно една максимална подгрупа тогава и само тогава, когато G е циклична p-група.

100. Нека G е крайна група, която има точно две максимални подгрупи от прости индекси p и q $(p\neq q)$. Докажете, че G е циклична група от ред p^nq^m.

ЛИТЕРАТУРА

1. Обрешков, Н., Висша алгебра, София, 1958 г.
2. Обрешков, Н., Сборник от задачи и теореми по висша алгебра, София, 1952 г.
3. Обрешков, Н., Нули на полиномите, София, 1963 г.
4. Обрешков, Н., Теория на числата, София, 1962 г.
5. Курош, А. Г., Курс высшей алгебры, Москва, 1956 г.
6. Арнольд, В. И., Теория чисел, Учпедгиз, 1939 г.
7. Виноградов, И. М., Теория чисел, Учпедгиз, 1960 г.
8. Ленг, С., Алгебра, „Мир", Москва, 1968 г.
9. Фадеев, Д. К. и И. С. Соминский, Сборник задач по высшей алгебре, Гостехиздат, 1952 г.
10. Окунев, Л. Я., Сборник задач по висшей алгебре, „Просвещение", Москва, 1964 г.
11. Полиа, Г. и Г. Сеге, Задачи и теореми из анализа, ч. I и II, Москва, 1956 г.
12. Ляпин, Е. С., А. Я. Айзенштат, М. М. Лесохин, Упражнения по теории групп, „Наука", Москва, 1967 г.

РЪКОВОДСТВО ЗА УПРАЖНЕНИЯ ПО ВИСША АЛГЕБРА

(Второ издание)

КИРИЛ ГЕЧОВ ДОЧЕВ
ДИМИТЪР ГЕОРГИЕВ ДИМИТРОВ
ВЛАДИМИР СТ. ЧУКАНОВ

Художник Диана Венкова
Худ. редактор Светлозар Писаров Техн. редактор Милка Иванова
Коректор Мария Илчева
Дадена за набор на 11. VI. 1975 г. Подписана за печат на 25. I. 1976 г.
Излязла от печат на 30. I. 1976 г. Издателски № 22 333 Лит. група I-4
Формат 60/90/16 Печатни коли 18,50
Издателски коли 18,50 Тираж 12 073 Цена 0,90 лв.

Държавно издателство „*Наука и изкуство*“
Държавна печатница „*Г. Димитров*“ — Ямбол