**Задачи по алгебре к 11 сентября 1997**

1. При каких $n$ уравнение $n = x^2 + y^2$ разрешимо в целых числах?

2. Пусть $\theta(n)$ — одна четверть числа целых решений уравнения $x^2 + y^2 = n$. Докажите, что $\theta(nm) = \theta(n)\theta(m)$, если $m, n$ — взаимно простые натуральные числа.

3. Пусть $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ — разложение на простые сомножители. Найдите $\theta(n)$.

4. Пусть $\tau_1(n)$ (соотв. $\tau_3(n)$) — количество натуральных делителей $n$, имеющих вид $4k+1$ (соотв. $4k+3$). Выразите $\theta(n)$ через $\tau_1(n), \tau_3(n)$.

5. Пусть $\omega = \exp(\frac{2\pi i}{3}) = \sqrt[3]{1}$. Верна ли основная теорема арифметики в кольце $\mathbf{Z}[\omega]$? А в кольце $\mathbf{Z}[\sqrt{-3}]$? А в кольце $\mathbf{Z}[\sqrt{5}]$?

6. Пусть $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ — разложение на простые сомножители. Найдите число Эйлера $\phi(n)$ остатков по модулю $n$, взаимно простых с $n$.

7. Мультипликативная группа $(\mathbf{Z}/n\mathbf{Z})^*$ кольца вычетов по модулю $n$ имеет порядок $\phi(n)$. Найдите эту группу (например, $(\mathbf{Z}/p\mathbf{Z})^* = \mathbf{Z}/(p-1)\mathbf{Z}$, а $(\mathbf{Z}/8\mathbf{Z})^* = \mathbf{Z}/2\mathbf{Z} + \mathbf{Z}/2\mathbf{Z}$).

**Задачи по алгебре к 23 сентября 1997**

1. Пусть векторы $e_1, \ldots, e_n, x$ заданы своими координатами в некотором базисе:

a) $e_1 = (1,1,1),\ e_2 = (1,1,2),\ e_3 = (1,2,3),\ x = (6,9,14)$;

b) $e_1 = (2,1,-3),\ e_2 = (3,2,-5),\ e_3 = (1,-1,1),\ x = (6,2,-7)$;

c) $e_1 = (1,2,-1,-2),\ e_2 = (2,3,0,-1),\ e_3 = (1,2,1,4),\ e_4 = (1,3,-1,0), x = (7,14,-1,2)$.

Доказать, что $(e_1, \ldots, e_n)$ — также базис пространства, и найти координаты вектора $x$ в этом базисе.

2. Доказать, что каждая из двух заданных систем векторов $S, S'$ является базисом. Найти матрицу перехода от $S$ к $S'$: a) $S = \{(1,2,1),(2,3,3),(3,8,2)\},\ S' = \{(3,5,8),(5,14,13),(1,9,2)\}$;

b) $S = \{(1,1,1,1),(1,2,1,1),(1,1,2,1),(1,3,2,3)\}$,

$S' = \{(1,0,3,3),(-2,-3,-5,-4),(2,2,5,4),(-2,-3,-4,-4)\}$.

3. Даны векторы $v_1 = (0,1,0,2,0), v_2 = (7,4,1,8,3), v_3 = (0,3,0,4,0), v_4 = (1,9,5,7,1), v_5 = (0,1,0,5,0)$. Существуют ли числа $c_{ij}$ такие, что векторы $w_i = \sum_{j=1}^{5} c_{ij} v_j$ $(i = 1,2,3,4,5)$ линейно независимы?

4. Доказать, что всякий многочлен положительной степени с целыми коэффициентами имеет корень в поле $\mathbf{F}_p$ для бесконечного множества простых чисел $p$.

5. Пусть $F$ — конечное поле. Доказать, что для всякого отображения $h: F \to F$ существует многочлен $f \in F[x]$ такой, что $h(a) = f(a)$ для любого $a \in F$.

6. Найти a) все неприводимые многочлены степени меньше 5 над полем $\mathbf{F}_2$;

b) все неприводимые многочлены степени 2 над полем $\mathbf{F}_3$;

c) число неприводимых многочленов степени 5 над полем $\mathbf{F}_2$;

d) число неприводимых многочленов степени 3,4 над полем $\mathbf{F}_3$;

e) число неприводимых многочленов степени 2,3 над полем $\mathbf{F}_9$.

7. Доказать, что при $a \in \mathbf{F}_p^*$ многочлен $x^p - x - a$

a) неприводим над $\mathbf{F}_p$;

b) неприводим над $\mathbf{F}_{p^n}$ тогда и только тогда, когда $n$ не делится на $p$.

8*. Доказать, что $x^{2n} + x^n + 1$ неприводим над $\mathbf{F}_2$ тогда и только тогда, когда $n = 3^k$ для некоторого $k \geq 0$.

9*. Пусть $I_m$ — число различных неприводимых многочленов степени $m$ со старшим коэффициентом единица над конечным полем $\mathbf{F}_q$. Доказать, что в формальных рядах от $z$ имеет место тождество $1 - qz = \prod_{m=1}^{\infty}(1 - z^m)^{I_m}$.

### Задачи по алгебре к 30 сентября 1997

1. Доказать неприводимость над полем рациональных чисел следующих многочленов:

a) $x^4 - 8x^3 + 12x^2 - 6x + 2$;

b) $x^5 - 12x^3 + 36x - 12$;

c) $x^{105} - 9$;

d) $(x - a_1)(x - a_2)\dots(x - a_n) - 1$, где $a_1, \dots, a_n$ — различные целые числа;

e) $(x - a_1)^2 \dots (x - a_n)^2 + 1$, где $a_1, \dots, a_n$ — различные целые числа.

2. Выразить через квадратные корни $\sqrt[5]{1}$ и $\sqrt[17]{1}$.

3. Континуанта $(a_1 a_2 \dots a_n)$ — это определитель

$$\begin{vmatrix} a_1 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & a_2 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & a_3 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 & a_n \end{vmatrix}$$

a) Выразить $(a_1 a_2 \dots a_n)$ в виде многочлена от $a_1, \dots, a_n$;

b) Написать разложение континуанты по первым $k$ строкам;

c) Доказать

$$\frac{(a_1 a_2 \dots a_n)}{(a_2 \dots a_n)} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots + \cfrac{1}{a_n}}}$$

4. Определитель Вандермонда $\Delta(x_1, x_2, \dots, x_n)$ — это

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix}$$

a) Вычислить $\Delta(x_1, x_2, \dots, x_n)$ как многочлен от $x_1, \dots, x_n$;

b) Пусть $y_1, \dots, y_n$ — другой набор чисел, причем $x_i y_j \neq 1$ для всех $1 \leq i, j \leq n$. Доказать

$$\Delta(x_1, \dots, x_n)\Delta(y_1, \dots, y_n) \prod_{i,j=1}^{n} (1 - x_i y_j)^{-1} = \det\left(\frac{1}{1 - x_i y_j}\right)$$

5. Вычислить определитель матрицы $(a_{ij})$ порядка $n$, где

a) $a_{ij}$ равно 1, если $i$ делит $j$, и равно 0 иначе;

b) $a_{ij}$ равно количеству общих натуральных делителей чисел $i$ и $j$.

6*. Пусть $p$ — простое число, и $\zeta = \exp(\frac{2\pi i}{p})$ — первообразный корень из единицы. Выразить через $\zeta$

a) $\sqrt{p}$, если $p = 4k + 1$;

b) $\sqrt{-p}$, если $p = 4k + 3$.

7*. a) Классифицировать все тройки многочленов $X, Y, Z \in \mathbf{C}[t]$ такие, что $X^2 + Y^2 = Z^2$;

b) Доказать, что для $n > 2$ не бывает непостоянных многочленов $X, Y, Z \in \mathbf{C}[t]$ таких, что $X^n + Y^n = Z^n$.

**Задачи по алгебре к 7 октября 1997**

1. Найти минимальные многочлены для

a) $\sqrt{2} + \sqrt{3}$ над $\mathbf{Q}$;

b) $1 + \sqrt{2}$ над $\mathbf{Q}(\sqrt{2} + \sqrt{3})$.

2. Найти степень минимального поля разложения над $\mathbf{Q}$ для многочленов

a) $x^4-2$;

b) $x^p-a$ ($p$ — простое число; $a\in\mathbf{Q}$ не является $p$-ой степенью).

3. Являются ли числа $a=-\frac{1}{2}+i\frac{\sqrt{2}}{2}$ и $b=\sqrt{2}+i$ примитивными элементами $\mathbf{Q}(\sqrt{2},i)/\mathbf{Q}$?

4. Пусть $K$ — поле характеристики $p>0$.

a) Доказать, что многочлен $f(x)=x^p-x-a$ либо неприводим над $K$, либо разлагается в произведение линейных множителей, и указать это разложение, если $f(x)$ имеет корень $x_0$;

b) Доказать, что всякое расширение Галуа $L/K$ степени $p$ имеет вид $L=K(\theta)$, где $\theta$ — корень многочлена $x^p-x-a$ ($a\in K$), и обратно, всякое такое расширение является расширением Галуа степени 1 или $p$.

5. Найти поле инвариантов $\mathbf{C}(x_1,\ldots,x_n)^G$, где $G$ — это группа, порожденная

a) всеми перестановками переменных $x_1,\ldots,x_n$;

b) автоморфизмом $x_i\mapsto\zeta^ix_i$ ($i=1,\ldots,n$), где $\zeta$ — первообразный корень степени $n$ из 1;

c) циклической перестановкой переменных $x_1,\ldots,x_n$.

6. Найти группу Галуа расширения $\mathbf{Q}$

a) $\mathbf{Q}(\sqrt{2}+\sqrt{3})$;

b) полученного присоединением всех корней $\sqrt[7]{5}$;

c) полученного присоединением всех корней многочлена $x^3+ax+b$ (в зависимости от рациональных чисел $a$ и $b$).

7. Пусть $L/K$ — конечное расширение полей, $a\in L$. След, определитель и характеристический многочлен (т.е. $\det(a-t\mathrm{Id})$) $K$-линейного оператора $l\mapsto al$, $L\to L$, обозначаются соответственно через $Tr_{L/K}(a), N_{L/K}(a), \chi_{L/K}(a,t)$ и называются *следом, нормой* и *характеристическим многочленом* элемента $a$ над $K$. Доказать, что если $K\subset L\subset M$ — башня конечных расширений и $a\in M$, то

a) $Tr_{M/K}(a)=Tr_{L/K}(Tr_{M/L}(a))$;

b) $N_{M/K}(a)=N_{L/K}(N_{M/L}(a))$;

c) $\chi_{M/K}(a,t)=N_{L(t)/K(t)}(\chi_{M/L}(a,t))$;

d) Минимальный многочлен элемента $a$ над $K$ равен $\pm\chi_{K(a)/K}(a,t)$;

e) $\chi_{M/K}(a,t)$ является, с точностью до знака, степенью минимального многочлена $a$ над $K$.

f) Если $M/K$ — расширение Галуа с группой Галуа $G$, то $Tr_{M/K}(a)=\sum_{g\in G}g(a),\ N_{M/K}(a)=\prod_{g\in G}g(a)$,
$\chi_{M/K}(a,t)=\prod_{g\in G}(g(a)-t)$.

8. a) Доказать, что $Tr_{M/K}(a)=0\ \forall a\in M$ тогда и только тогда, когда расширение $M/K$ несепарабельно.

b) Доказать, что если расширение $M/K$ сепарабельно, то $K$-билинейная форма на $M: \ (x,y) \mapsto Tr_{M/K}(xy)$ невырождена.

9. Доказать, что в расширении Галуа $M/K$ с группой Галуа $G$ найдется такой элемент $a \in M$, что множество $\{g(a), \ g \in G\}$ составляет базис поля $M$ над $K$.

### Задачи по алгебре к 14 октября 1997

1. Какое из следующих двух утверждений верно: a) $\sin 36° \in \mathbf{Q}(\cos 36°)$; b) $\cos 36° \in \mathbf{Q}(\sin 36°)$?

2. Пусть $p$ — простое число, и $a \in \mathbf{Q}$ не является $p$-ой степенью. Пусть $K$ — расширение $\mathbf{Q}$, полученное присоединением всех корней $\sqrt[p]{a}$. Доказать, что группа Галуа $Gal(K/\mathbf{Q})$ изоморфна группе аффинных преобразований $\mathbf{F}_p$, т.е. преобразований вида $x \mapsto ax+b, \ a \in \mathbf{F}_p^*, b \in \mathbf{F}_p$.

3. Пусть $f(t)$ — многочлен степени $n$ с рациональными коэффициентами; $\alpha_1, \ldots, \alpha_n$ — его комплексные корни. Известно, что $\alpha_3 = \alpha_1 + \alpha_2$, но между другими корнями нет такого соотношения (т.е. если $\alpha_k = \alpha_i + \alpha_j$, то $k=3$, а $(i,j) = (1,2)$ или $(2,1)$). Доказать, что $\alpha_3 \in \mathbf{Q}$, а $\alpha_1, \alpha_2$ лежат в квадратичном расширении $\mathbf{Q}$.

4. Известно, что всякий квадратный многочлен с вещественными коэффициентами имеет корень в $\mathbf{C}$, а всякий многочлен нечетной степени с вещественными коэффициентами имеет корень в $\mathbf{R}$ (т.к. непрерывная функция принимает промежуточные значения). Пользуясь этими двумя фактами доказать, в рамках теории Галуа, что $\mathbf{C}$ алгебраически замкнуто (т.е. не имеет конечных расширений).

5. Пусть $K$ — поле, полученное из $\mathbf{F}_p$ присоединением всех примитивных корней $l$-ой степени из 1 для всех простых чисел $l \neq p$. Доказать, что $K$ алгебраически замкнуто.

6. Доказать, что $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}$ линейно независимы над $\mathbf{Q}$.

7. Пусть $\psi(t) = \frac{f(t)}{g(t)} \in K(t)$ — рациональная функция, представленная как отношение двух взаимно простых многочленов. Определим $\deg(\psi)$ как $\max(\deg(f), \deg(g))$ и положим $u = \psi(t)$.

a) Доказать, что $\deg(\psi) = [K(t) : K(u)]$;

b) Доказать, что всякий автоморфизм поля $K(t)$ над $K$ имеет вид $t \mapsto \psi(t)$, где $\psi(t)$ — рациональная функция степени 1;

c) Доказать, что эта группа автоморфизмов порождается следующими отображениями $(a \in K^*, b \in K): \ t \mapsto at; \ t \mapsto t+b; \ t \mapsto \frac{1}{t}$. Эта группа состоит из преобразований вида $t \mapsto \frac{at+b}{ct+d}, \ ad - bc \neq 0$ и обозначается $PGL(2,K)$;

d) Пусть $K = \mathbf{F}_q$. Доказать, что $\sharp PGL(2, \mathbf{F}_q) = q^3 - q$;

e) Доказать, что поле инвариантов $PGL(2, \mathbf{F}_q)$ равно $\mathbf{F}_q(u)$, где $u = \frac{(t^{q^2}-t)^{q+1}}{(t^q-t)^{q^2+1}}$;

f) Пусть $P \subset PGL(2, \mathbf{F}_q)$ — подгруппа, состоящая из отображений $t \mapsto at + b,\ a \in \mathbf{F}_q^*, b \in \mathbf{F}_q$. Доказать, что поле инвариантов $P$ равно $\mathbf{F}_q(y)$, где $y = (t^q - t)^{q-1}$;

g) Пусть $N \subset P \subset PGL(2, \mathbf{F}_q)$ — подгруппа, состоящая из отображений $t \mapsto t + b,\ b \in \mathbf{F}_q$. Доказать, что поле инвариантов $N$ равно $\mathbf{F}_q(z)$, где $z = t^q - t$;

h) Для каких $q$ из следующего списка группа $PGL(2, \mathbf{F}_q)$ разрешима: $q = 2, 3, 4, 5, 7$?

## Задачи по алгебре к 21 октября 1997

1. Найти сумму чисел, обратных комплексным корням многочлена

a) $3x^3 + 2x^2 - 1$; b) $x^4 - x^2 - x - 1$.

2. Сумма двух корней многочлена $2x^3 - x^2 - 7x + \lambda$ равна 1. Найти $\lambda$.

3. Выразить через элементарные симметрические многочлены:

a) $x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2$;

b) $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$;

c) $(x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4)$;

d) $(x_1 - 1)(x_2 - 1)(x_3 - 1)$.

4. Найти значение симметрического многочлена $F$ от корней многочлена $f(x)$:

a) $F = x_1^3(x_2 + x_3) + x_2^3(x_1 + x_3) + x_3^3(x_1 + x_2),\ f(x) = x^3 - x^2 - 4x + 1$;

b) $F = x_1^4x_2 + \ldots,\ f(x) = 3x^3 - 5x^2 + 1$;

c) $F = (x_1^2 + x_1x_2 + x_2^2)(x_2^2 + x_2x_3 + x_3^2)(x_1^2 + x_1x_3 + x_3^2),\ f(x) = 5x^3 - 6x^2 - 7x - 8$.

5. Пусть $x_1, \ldots, x_n$ — корни многочлена $x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Доказать, что любой симметрический многочлен от $x_2, x_3, \ldots, x_n$ можно представить в виде многочлена от $x_1$.

6. Рассмотрим многочлен $\lambda_t = (1 + x_1t)\ldots(1 + x_nt)$ от переменных $x_1, \ldots, x_n, t$.

a) Доказать, что $\lambda_t = 1 + \sigma_1t + \sigma_2t^2 + \ldots + \sigma_nt^n$, где $\sigma_k$ — элементарные симметрические многочлены;

b) Доказать, что $\frac{d}{dt}(\log \lambda_t) = -\sum_{k>0}(-1)^k s_k t^{k-1}$, где $s_k = x_1^k + \ldots + x_n^k$;

c) Доказать формулу Ньютона: $s_k - \sigma_1s_{k-1} + \sigma_2s_{k-2} + \ldots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0$ (при $k > n$ мы полагаем $\sigma_k = 0$).

7. Пусть $\zeta$ — первообразный корень степени $k$ из 1. Доказать, что a) для любого $a \in \mathbf{C}$ имеем $(x - a)(x\zeta - a)\ldots(x\zeta^{k-1} - a) = (-1)^{k+1}(x^k - a^k)$;

b) для любого $f(x) \in \mathbf{C}[x]$ многочлен $f(x)f(x\zeta)\dots f(x\zeta^{k-1})$ представим в виде $h(x^k)$ для некоторого многочлена $h$;

c) корнями многочлена $h$ являются в точности $k$-ые степени корней многочлена $f$.

8. Найти многочлен четвертой степени, корнями которого являются

a) квадраты комплексных корней многочлена $x^4 + 2x^3 - x + 3$;

b) кубы комплесных корней многочлена $x^4 - x - 1$.

9. Доказать, что $s_k$ равняется определителю

$$\begin{vmatrix} \sigma_1 & 1 & 0 & \dots & 0 & 0 \\ 2\sigma_2 & \sigma_1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (k-1)\sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \dots & \sigma_1 & 1 \\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \dots & \sigma_2 & \sigma_1 \end{vmatrix}$$

в то время как $k!\sigma_k$ равняется определителю

$$\begin{vmatrix} s_1 & 1 & 0 & \dots & 0 & 0 \\ s_2 & s_1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ s_{k-1} & s_{k-2} & s_{k-3} & \dots & s_1 & k-1 \\ s_k & s_{k-1} & s_{k-2} & \dots & s_2 & s_1 \end{vmatrix}$$

10. Найти $s_m$ от a) корней многочлена $x^n + \frac{x^{n-1}}{1!} + \frac{x^{n-2}}{2!} + \dots + \frac{1}{n!}$;

b) первообразных корней $n$-ой степени из 1.

11. Решить над $\mathbf{C}$ систему уравнений $x_1 + x_2 + x_3 = 0$; $x_1^2 + x_2^2 + x_3^2 = 0$, $x_1^3 + x_2^3 + x_3^3 = 24$.

## Задачи по алгебре к 28 октября 1997

1. a) Пусть $f(x_1, \dots, x_n)$ — кососимметрический многочлен от $x_1, \dots, x_n$. Доказать, что $f(x_1, \dots, x_n) = \Delta(x_1, \dots, x_n) g(x_1, \dots, x_n)$, где $\Delta(x_1, \dots, x_n)$ — определитель Вандермонда, а $g(x_1, \dots, x_n)$ — симметрический многочлен.

b) Пусть $h(x_1, \dots, x_n)$ — симметрический многочлен от $x_1, \dots, x_n$, причем $h(x_1, x_1, x_3, \dots, x_n) = 0$. Доказать, что $h(x_1, \dots, x_n) = \Delta^2(x_1, \dots, x_n) u(x_1, \dots, x_n)$, где $u(x_1, \dots, x_n)$ — симметрический многочлен.

2. Пусть $h_k = \sum_{1 \le i_1 \le \dots \le i_k \le n} x_{i_1} \dots x_{i_k}$, а $\lambda_t$ — из задачи 6 прошлого раза. Доказать, что

a) $\lambda_t^{-1} = \sum_{k \ge 0} (-1)^k h_k t^k$;

b) $\sigma_k - h_1\sigma_{k-1} + \ldots + (-1)^{k-1}h_{k-1}\sigma_1 + (-1)^k h_k = 0$;

c) Каждый симметрический многочлен является многочленом от $h_1, \ldots, h_n$.

3. Пусть $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\alpha_1 > \alpha_2 > \ldots > \alpha_n \geq 0$ — набор натуральных чисел. Положим $a_\alpha(x_1, \ldots, x_n) = \sum_{\tau\in\Sigma_n}(\mathrm{sgn}\tau)x_{\tau(1)}^{\alpha_1}\ldots x_{\tau(n)}^{\alpha_n}$.

Доказать, что a) $a_\alpha(x_1, \ldots, x_n)$ равняется определителю

$$\begin{vmatrix} x_1^{\alpha_1} & \ldots & x_n^{\alpha_1} \\ \vdots & \ddots & \vdots \\ x_1^{\alpha_n} & \ldots & x_n^{\alpha_n} \end{vmatrix}$$

b) Если $\delta = (n-1, n-2, \ldots, 1, 0)$, то $a_\delta(x_1, \ldots, x_n) = \Delta(x_1, \ldots, x_n)$ — определитель Вандермонда;

4. Пусть $\mu = (\mu_1, \ldots, \mu_n)$ — набор натуральных чисел таких, что $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_n \geq 0$ и $\mu_1 + \ldots + \mu_n = k$, т.е. разбиение числа $k$. Положим $\alpha_i = \mu_i + n - i$ и $S_\mu(x_1, \ldots, x_n) = \frac{a_\alpha}{a_\delta}$ — многочлен Шура. Доказать, что

a) $S_\mu(x_1, \ldots, x_n)$ — целочисленный симметрический многочлен;

b) $S_\mu(x_1, \ldots, x_n)$ при всех $\mu = (\mu_1, \ldots, \mu_n)$ образуют базис пространства симметрических многочленов от $x_1, \ldots, x_n$;

c) Если $\mu = (1, \ldots, 1)$, то $S_\mu(x_1, \ldots, x_n) = \sigma_n$;

d) Если $\mu(n, 0, \ldots, 0)$, то $S_\mu(x_1, \ldots, x_n) = h_n$ из задачи 2.

5. Доказать, что a) $\prod_{i,j=1}^n (1 - x_i y_j)^{-1} = \sum_\mu S_\mu(x_1, \ldots, x_n)S_\mu(y_1, \ldots, y_n)$, суммирование по всем разбиениям на $n$ слагаемых;

b) $\prod_{i,j=1}^n (1 + x_i y_j) = \sum_\mu S_\mu(x_1, \ldots, x_n)S_{\mu'}(y_1, \ldots, y_n)$, где $\mu'$ — сопряженное разбиение, т.е. $\mu'_i$ — количество таких $j$, что $\mu_j \geq i$.

6. Доказать, что $\sum_{\tau\in\Sigma_n}\sigma_k(x_{\tau(1)}y_1, \ldots, x_{\tau(n)}y_n) = k!(n-k)!\sigma_k(x_1, \ldots, x_n)\sigma_k(y_1, \ldots, y_n)$.

7. Вычислить результант многочленов

a) $x^3 - 3x^2 + 2x + 1,\ 2x^2 - x - 1$;

b) $2x^3 - 3x^2 - x + 2,\ x^4 - 2x^2 - 3x + 4$;

c) $2x^4 - x^3 + 3,\ 3x^3 - x^2 + 4$;

d) $\Phi_n,\ \Phi_m$ (круговые многочлены).

8. Исключить $x$ из системы уравнений:

a) $x^2 - xy + y^2 = 3,\ x^2y + xy^2 = 6$;

b) $y^2 - 7xy + 4x^2 + 13x - 2y - 3 = 0,\ y^2 - 14xy + 9x^2 + 28x - 4y - 5 = 0$;

c) $5y^2 - 6xy + 5x^2 - 16 = 0,\ y^2 - xy + 2x^2 - y - x - 4 = 0$.

9. Найти все значения $\lambda$, при которых следующие многочлены имеют кратный корень:

a) $x^4 - 4x + \lambda$; b) $x^3 - 8x^2 + (13-\lambda)x - (6+2\lambda)$; c) $x^4 - 4x^3 + (2-\lambda)x^2 + 2x - 2$.

10. Пусть $f, g$ — многочлены. Доказать, что $D(fg) = D(f)D(g)R^2(f,g)$.

11. Вычислить дискриминант следующих многочленов:

a) $x^n + x^{n-1} + \ldots + 1$; b) $\Phi_n(x)$; c) $1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}$; d) $x^n + a$; e) $H_n(x) = (-1)^n \exp(\frac{x^2}{2})\frac{d^n}{dx^n}\exp(-\frac{x^2}{2})$ (многочлен Эрмита); f) $L_n(x) = (-1)^n \exp(x)\frac{d^n}{dx^n}(x^n \exp(-x))$ (многочлен Лагерра); g) $P_n(x) = 2\cos(n \arccos \frac{x}{2})$ (многочлен Чебышева).

### Задачи по алгебре к 4 ноября 1997

1. Пусть $d \in \mathbf{Z}$. Найти кольцо целых чисел и дискриминант поля $\mathbf{Q}(\sqrt{d})$.

2. Пусть $d$ — целое отрицательное число свободное от квадратов. Пусть $R$ — кольцо целых мнимого квадратичного поля $\mathbf{Q}(\sqrt{d})$. Доказать, что

a) алгоритм деления с остатком по норме $\|\alpha\| = \alpha \cdot \overline{\alpha}$ имеет место в $R$ (т.е. $\forall\ \alpha, \beta\ \exists\ \gamma, \delta \mid \alpha = \gamma\beta + \delta,\ \|\delta\| < \|\beta\|$) тогда и только тогда, когда сдвиги единичного круга (без границы) на все векторы решетки $R$ покрывают всю плоскость $\mathbf{C}$;

b) это происходит тогда и только тогда, когда $d$ принимает следующие значения: -1,-2,-3,-7,-11;

c) если $d$ не входит в этот список, а $\alpha \in R,\ \alpha \neq 0, \pm 1$, то $\|\alpha\| \geq 3$;

d) если $d$ не входит в этот список, то кольцо $R$ не евклидово, т.е. ни для какой нормы не работает алгоритм деления с остатком.

3. Доказать, что кольцо целых $\mathbf{Q}(\sqrt{2})$ евклидово.

4. Используя однозначность разложения на множители в кольце целых чисел поля $\mathbf{Q}(\sqrt{-2})$, доказать, что уравнение $x^2 + 2y^4 = 17z^4$ в поле рациональных чисел имеет только нулевое решение $x = y = z = 0$.

5. Пусть $R$ — кольцо, целозамкнутое в своем поле частных. Доказать, что кольцо $R[t]$ тоже целозамкнуто в своем поле частных.

6. Пусть $R$ — кольцо целых чисел числового поля, а $I \subset R$ — идеал. Доказать, что $I$ порожден не более чем двумя элементами.

7. Пусть $R$ — кольцо целых чисел числового поля, а $I, J, K \subset R$ — идеалы. Докажите, что $I \cap (J + K) = (I \cap J) + (I \cap K)$; $I + (J \cap K) = (I + J) \cap (I + K)$.

### Задачи по алгебре к 11 ноября 1997

1. Разложить в прямую сумму циклических групп факторгруппу $A/B$, где $A$ — свободная абелева группа с базисом $x_1, x_2, x_3$, а $B$ — ее подргуппа, порожденная $y_1, y_2, y_3$:

a) $y_1 = 7x_1 + 2x_2 + 3x_3,\ y_2 = 21x_1 + 8x_2 + 9x_3,\ y_3 = 5x_1 - 4x_2 + 3x_3$;

b) $y_1 = 4x_1 + 5x_2 + 3x_3,\ y_2 = 5x_1 + 6x_2 + 5x_3,\ y_3 = 8x_1 + 7x_2 + 9x_3$;

c) $y_1 = 2x_1 + 6x_2 - 2x_3,\ y_2 = 2x_1 + 8x_2 - 4x_3,\ y_3 = 4x_1 + 12x_2 - 2x_3$.

2. Сколько подгрупп a) порядков 3 и 6 в нециклической абелевой группе порядка 18; b) порядков 5 и 15 в нециклической абелевой группе порядка 75?

3. Пусть $A$ — свободная абелева группа с базисом $x_1, \ldots, x_n$, а $B$ — ее подгруппа с порождающими элементами $y_i = \sum_{i=1}^{n} a_{ij} x_j,\ j = 1, \ldots, n$. Доказать, что факторгруппа $A/B$ конечна тогда и только тогда, когда $\det(a_{ij}) \neq 0$, и при этом $\sharp A/B = |\det(a_{ij})|$.

4. Найти жорданову форму матрицы:

$$a) \begin{pmatrix} 1 & -3 & 4 \\ 4 & -7 & 8 \\ 6 & -7 & 7 \end{pmatrix};\ b) \begin{pmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{pmatrix};\ c) \begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix};$$

$$d) \begin{pmatrix} n & n-1 & n-2 & \ldots & 1 \\ 0 & n & n-1 & \ldots & 2 \\ 0 & 0 & n & \ldots & 3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & n \end{pmatrix};\ e) \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

5. Решить уравнения a) $X^2 = \begin{pmatrix} 3 & 1 \\ -1 & 5 \end{pmatrix}$; b) $X^2 = \begin{pmatrix} 6 & 2 \\ 3 & 7 \end{pmatrix}$.

6. Вычислить a) $\begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}^{50}$; b) $\begin{pmatrix} 7 & -4 \\ 4 & -8 \end{pmatrix}^{64}$.

7. Найти жорданову форму следующих операторов: a) $A:\ f(x,y) \mapsto f(x+1, y+1)$ в 9-мерном пространстве комплексных многочленов степени не выше 2 по $x$ и $y$; b) $B = \frac{\partial}{\partial x} + \frac{\partial}{\partial y}$ в $\frac{n(n+1)}{2}$-мерном пространстве комплексных многочленов от $x$ и $y$ степени не выше $n-1$; c) $L_C(X) = CX$ в 4-мерном пространстве $2 \times 2$-матриц, где $C$ — фиксированная $2 \times 2$-матрица известной жордановой формы.

**Задачи по алгебре к 18 ноября 1997**

1. Вычислить $D(\mathbf{Q}(\sqrt{2} + \sqrt{5}))$.

2. Доказать, что дискриминант любого числового поля сравним либо с 0, либо с 1 по модулю 4.

3. Пусть $A$ — кольцо целых числового поля $F$. Предположим, число классов идеалов $A$ равно 2. Доказать, что

a) если $\mathbf{p} \in A$ — неразложимый элемент, но идеал $(\mathbf{p}) \subset A$ не является простым, то $(\mathbf{p}) = \mathbf{P}_1\mathbf{P}_2$, где $\mathbf{P}_1, \mathbf{P}_2$ — простые идеалы (не обязательно различные);

b) если $A \ni a = \mathbf{p}_1 \ldots \mathbf{p}_k = \mathbf{q}_1 \ldots \mathbf{q}_m$ — два разложения $a \in A$ на неразложимые множители, то $k = m$.

4. Пусть $A$ — кольцо целых числового поля $F$. Пусть $\mathbf{P}_1, \mathbf{P}_2 \subset A$ — различные простые идеалы. Доказать, что для любых натуральных $a, b$ идеал $\mathbf{P}_1^a + \mathbf{P}_2^b$ равен $A$.

5. Пусть $A$ — кольцо целых числового поля $F$. Предположим, $(p) = I\mathbf{P}^2$ для некоторого простого числа $p \in \mathbf{Z}$, простого идеала $\mathbf{P} \subset A$, и произвольного идеала $I \subset A$ (т.е. $(p)$ делится на $\mathbf{P}^2$). Доказать, что a) $\exists\ \alpha \in I\mathbf{P} \mid \alpha \notin I\mathbf{P}^2$; b) $\forall\ \beta \in A\ (\alpha\beta)^p \in (p)$; c) $Tr^p_{F/\mathbf{Q}}(\alpha\beta) \equiv Tr_{F/\mathbf{Q}}(\alpha^p\beta^p)$ $(\mathrm{mod}\ (p))$; d) $p | Tr_{F/\mathbf{Q}}(\alpha\beta)$; e) $p | D(A)$.

6. "Идеальные числа". Пусть $A$ — кольцо целых числового поля $F$. Пусть $K \supset F$ — произвольное числовое поле с кольцом целых $B$, и $I, J \subset A$ — такие идеалы, что $IB$ делит $JB$. Доказать, что a) $I$ делит $J$; b) $IB \cap A = I$;

c) Пусть $I \subset A$ — некоторый идеал. Доказать, что найдется числовое поле $K \supset F$ с кольцом целых $B$ такое, что $IB \subset B$ — главный идеал.

**Задачи по алгебре к 25 ноября 1997**

1. a) Доказать, что всякий идеал кольца $\mathbf{Z}[\sqrt{-5}]$ эквивалентен некоторому идеалу, содержащему главный идеал $(2)$;

b) Определить кольцо вычетов $\mathbf{Z}[\sqrt{-5}]/(2)$;

c) Доказать, что число классов идеалов кольца $\mathbf{Z}[\sqrt{-5}]$ равно 2;

d) Разложить идеал $(6) \subset \mathbf{Z}[\sqrt{-5}]$ в произведение простых идеалов.

2. Доказать, что дискриминант поля $\mathbf{Q}(\sqrt[p]{1})$ ($p$ — простое число) равен $(-1)^{\frac{p-1}{2}} p^{p-2}$.

3. Пусть $I \subset A \subset F$ — идеал кольца целых числового поля. Наибольший общий делитель чисел вида $|N_{F/\mathbf{Q}}(\alpha)|$, $\alpha \in I$, называется *нормой* идеала $I$ и обозначается $N_{F/\mathbf{Q}}(I) = N(I)$. Пусть $[F : \mathbf{Q}] = n$. Доказать, что число $\psi(a)$ идеалов с данной нормой $a$ не превосходит числа $\tau_n(a)$ всех решений уравнения $x_1 x_2 \ldots x_n = a$ в натуральных числах.

4. Пусть $J \subset I \subset A \subset F$ — идеалы кольца целых числового поля. Как мы знаем, $J$ делится на $I$, т.е. существует идеал $K$ такой, что $KI = J$. Доказать, что $\sharp I/J = N(K)$.

5. Доказать, что в любых двух различных классах идеалов содержатся взаимно простые идеалы, т.е. такие идеалы $I, J$, что $I + J = A$.

6. Для идеала $I \subset A$ обозначим через $\varphi(I)$ число классов вычетов $\overline{\alpha} \in A/I$ взаимно простых с $I$ (т.е. таких что $I + (\alpha) = A$) — это обобщение функции Эйлера. Доказать, что

a) если идеалы $I, J$ взаимно просты, то $\varphi(IJ) = \varphi(I)\varphi(J)$;

b) $\varphi(I) = N(I)\prod_{\mathbf{P}}(1 - \frac{1}{N(\mathbf{P})})$, где $\mathbf{P}$ пробегает все простые идеалы, делящие $I$.

c) если $\alpha \in A$ взаимно просто с $I$, то $\alpha^{\varphi(I)} - 1 \in I$ (обобщение теоремы Эйлера);

d) если $\mathbf{P}$ — простой идеал, $\alpha \in A$, то $\alpha^{N(\mathbf{P})} - \alpha \in \mathbf{P}$ (обобщение малой теоремы Ферма);

e) $\sum_{I \subset J \subset A} \varphi(J) = N(I)$.

7. Пусть $\mathbf{P} \subset A$ — простой идеал, и $A \ni \alpha_1, \ldots, \alpha_s,\ s = N(\mathbf{P}) - 1$ — полная система представителей $A/\mathbf{P} - 0$. Доказать, что $\alpha_1 \ldots \alpha_s + 1 \in \mathbf{P}$ (обобщение теоремы Вильсона).