Оглавление

§ 17. Многочлены от одной переменной

17.1. Определения и основные свойства. *Многочленом от одной переменной над кольцом* K называется выражение

$$f = f(x) = a_0 + a_1 x + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i, \quad a_i \in K,$$

где x — некоторая буква. Если $a_n \neq 0$, то a_n называется *старшим коэффициентом многочлена* f, а n — *степенью многочлена* f (обозначение: $n = \deg f$). Нулевому многочлену 0 степень не приписывается. Два многочлена *равны*, если равны коэффициенты при одинаковых степенях x. Множество всех многочленов от x над кольцом K будем обозначать символом $K[x]$. На множестве $K[x]$ определим операции сложения и умножения:

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

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{n+m} c_k x^k, \quad \text{где} \quad c_k = \sum_{i+j=k} a_i b_j.$$

При определении операции сложения мы добавляем нулевые слагаемые с тем, чтобы получить записи с одинаковыми степенями x.

Из этого определения видно, что $\langle K[x]; +, \cdot \rangle$ — алгебраическая система, которую в дальнейшем будем обозначать просто $K[x]$. Справедлива

Т е о р е м а 1. 1) *Если K — кольцо, то $K[x]$ — тоже кольцо.* 2) *Если K — коммутативное кольцо, то $K[x]$ — тоже коммутативное кольцо.* 3) *Если K содержит единицу, то $K[x]$ — тоже содержит единицу.* 4) *Если K не имеет делителей нуля, то $K[x]$ тоже не имеет делителей нуля.*

Д о к а з а т е л ь с т в о. 1) Проверим аксиомы кольца. Для этого возьмём многочлены $a, b, c \in K[x]$. Пусть a_i — коэффициенты многочлена a, b_i — коэффициенты многочлена b, c_i — коэффициенты многочлена c.

С1. Ассоциативность сложения следует из равенств

$$(a + b) + c = \sum_{i=0}^{n} \left[(a_i + b_i) + c_i \right] x^i = \sum_{i=0}^{n} \left[a_i + (b_i + c_i) \right] x^i = a + (b + c).$$

С2. Коммутативность сложения следует из равенств

$$a+b=\sum_{i=0}^{n}(a_i+b_i)x^i=\sum_{i=0}^{n}(b_i+a_i)x^i=b+a.$$

С3. Нулевым элементом является нулевой многочлен, т. е. $0\in K$.

С4. Противоположным для многочлена $a=\sum_{i=0}^{n}a_ix^i$ будет многочлен

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

У1. Надо доказать, что для любых многочленов $a,b,c\in K[x]$ справедливо равенство

$$(a\,b)\,c=a\,(b\,c).$$

Обозначим $ab=d$, $dc=f$, $bc=g$, $ag=h$. Надо проверить, что $f=h$. Пусть a_i — коэффициенты многочлена a, b_j — коэффициенты многочлена b, c_k — коэффициенты многочлена c и т. д. Тогда

$$f_i=\sum_{k+l=i}d_k\,c_l=\sum_{k+l=i}\left(\sum_{r+s=k}a_r\,b_s\right)c_l=\sum_{r+s+l=i}(a_r\,b_s)c_l.$$

С другой стороны,

$$h_i=\sum_{p+q=i}a_p\,g_q=\sum_{p+q=i}a_p\left(\sum_{u+v=q}b_u\,c_v\right)=\sum_{p+u+v=i}a_p\,(b_uc_v).$$

Учитывая, что K — кольцо, а потому операция умножения ассоциативна, получаем $f_i=h_i$.

СУ1. Надо доказать, что $(a+b)c=ac+bc$ для любых $a,b,c\in K[x]$. Обозначим $a+b=d$, $dc=f$, $ac=g$, $bc=h$, $g+h=t$. Покажем, что $f=t$. Имеем:

$$f_i=\sum_{k+l=i}d_k\,c_l=\sum_{k+l=i}(a_k+b_k)\,c_l=\sum_{k+l=i}(a_k\,c_l+b_k\,c_l)=$$

$$=\sum_{k+l=i}a_k\,c_l+\sum_{k+l=i}b_k\,c_l.$$

С другой стороны,

$$t_i=g_i+h_i=\sum_{k+l=i}a_k\,c_l+\sum_{k+l=i}b_k\,c_l.$$

Аксиома СУ2 проверяется аналогично.

2) Коммутативность умножения следует из определения операции умножения в $K[x]$.

3) Так как $K \subset K[x]$, то единицей в $K[x]$ является 1 из K. Действительно,

$$1 \cdot \sum_{i=1}^{n} a_i\, x^i = \sum_{i=1}^{n} a_i\, x^i.$$

4) Докажем, что $K[x]$ не содержит делителей нуля. Пусть

$$a = a_0 + a_1 x + \ldots + a_n x^n, \quad a_n \neq 0,$$

$$b = b_0 + b_1 x + \ldots + b_m x^m, \quad b_m \neq 0$$

— два многочлена из $K[x]$. Рассмотрим их произведение:

$$a \cdot b = (a_0 + a_1 x + \ldots + a_n x^n)(b_0 + b_1 x + \ldots + b_m x^m) = a_0 b_0 + \ldots + a_n b_m x^{n+m}.$$

Старший коэффициент $a \cdot b$ равен $a_n b_m$. Так как кольцо K без делителей нуля и $a_n \neq 0$, $b_m \neq 0$, то $a_n b_m \neq 0$. Следовательно, $ab \neq 0$. Теорема доказана.

При доказательстве последней части теоремы мы установили, что степень произведения fg равна степени f плюс степень g, т. е.

$$\deg(fg) = \deg f + \deg g, \quad f \neq 0, \quad g \neq 0.$$

Отсюда, в частности, следует, что даже если K — поле, $K[x]$ не обязано быть полем. Действительно, если $fg = 1$, то

$$\deg(fg) = \deg f + \deg g = 0.$$

Следовательно, многочлены f и g должны быть ненулевыми элементами из K. Таким образом, нами установлено

С л е д с т в и е. *Группа обратимых элементов кольца $K[x]$ совпадает с группой обратимых элементов кольца K.*

17.2. Деление с остатком. На множестве целых чисел существует операция деления с остатком, т. е. если m и n — два целых числа и при этом $n \neq 0$, то мы можем разделить m на n с остатком, т. е. представить m в виде

$$m = nq + r, \text{ где } 0 \leq r < |n|$$

для некоторого целого q и неотрицательного целого r. Для кольца многочленов тоже существует операция деления с остатком.

Т е о р е м а 2. *Пусть P — поле. Для всяких $f, g \in P[x]$, где $g \neq 0$, существуют и единственные $q, r \in P[x]$, такие, что:*

а) $f = g \cdot q + r$;

б) $r = 0$ *или* $\deg r < \deg g$.

При этом q называется *частным,* а r — *остатком* от деления f на g.

Д о к а з а т е л ь с т в о. Докажем существование. Если $\deg f < \deg g$, то можно положить $q = 0, r = f$. Если $\deg f \geq \deg g$, то построим последовательность многочленов f_i, $i = 0, 1, \ldots$, положив $f_0 = f$ и для каждого $i \geq 0$ определив

$$f_{i+1} = f_i - \frac{\text{старший коэффициент } f_i}{\text{старший коэффициент } g} \cdot g\, x^{\deg(f_i)-\deg(g)}.$$

Полагая

$$h_i = \frac{\text{старший коэффициент } f_i}{\text{старший коэффициент } g} \cdot x^{\deg(f_i)-\deg(g)},$$

запишем многочлен f_{i+1} в виде $f_{i+1} = f_i - h_i g$. Видим, что степени этих многочленов убывают:

$$\deg f_0 > \deg f_1 > \deg f_1 > \ldots$$

Следовательно, не позже чем, через $n = \deg f$ шагов, мы получим многочлен f_k, который либо равен нулю, либо его степень будет меньше степени многочлена g.

Сложим все равенства

$$\begin{aligned} f_0 &= f, \\ f_1 &= f_0 - g\, h_0, \\ f_2 &= f_1 - g\, h_1, \\ &\ldots\ldots\ldots\ldots \\ f_k &= f_{k-1} - g\, h_{k-1}, \end{aligned}$$

получим

$$(f_0+f_1+\ldots+f_{k-1})+f_k = f+(f_0+f_1+\ldots+f_{k-1})-g(h_0+h_1+\ldots+h_{k-1}).$$

Отсюда

$$f = g(h_0 + h_1 + \ldots + h_{k-1}) + f_k.$$

Положим

$$h_0 + h_1 + \ldots + h_{k-1} = q, \quad f_k = r.$$

Ясно, что r и q искомые и для них выполняются условия а) и б).

Докажем единственность. Пусть имеются две пары многочленов (q_1, r_1) и (q_2, r_2), удовлетворяющие условию теоремы, т. е.

$$f = g \cdot q_1 + r_1, \quad \text{где } r_1 = 0 \text{ или } \deg r_1 < \deg g,$$

$$f = g \cdot q_2 + r_2, \quad \text{где } r_2 = 0 \text{ или } \deg r_2 < \deg g.$$

Вычитая одно равенство из другого, получим

$$g(q_1 - q_2) = r_2 - r_1.$$

Если $r_2 - r_1 \neq 0$, то $q_1 - q_2 \neq 0$. Так как эти многочлены отличны от нуля, рассмотрим их степени. Степень левой части равна $\deg g + \deg(q_1 - q_2) \geq \deg g$, а степень правой части меньше $\deg g$. Приходим к противоречию. Значит, $r_2 - r_1 = 0$, а тогда $q_1 - q_2 = 0$ (так как кольцо $P[x]$ без делителей нуля). Теорема доказана.

17.3. Наибольший общий делитель двух многочленов. Пусть f — некоторый многочлен из кольца $K[x]$. Говорим, что многочлен $d \in K[x]$ является *делителем* многочлена f (обозначаем $d|f$), если $f = d \cdot h$ для некоторого многочлена $h \in K[x]$. Говорим, что d — *наибольший общий делитель* многочленов f и g, если:

а) $d|f$ и $d|g$;

б) если некоторый многочлен $d' \in K[x]$ является делителем f и g, то $d'|d$.

Заметим, что если d — наибольший общий делитель, то dk — тоже наибольший общий делитель для любого $k \in K^*$, т. е. наибольший общий делитель определяется неоднозначно. Символом (f, g) будем обозначать *приведённый наибольший общий делитель* многочленов f и g, т. е. наибольший общий делитель со старшим коэффициентом 1.

Т е о р е м а 3. *Пусть P — поле. Для любых ненулевых многочленов $f, g \in P[x]$ справедливы следующие утверждения.* 1) *В $P[x]$ существует наибольший общий делитель многочленов f и g.* 2) *Приведённый наибольший общий делитель многочленов f и g единственный.* 3) *Наибольший общий делитель может быть найден при помощи алгоритма Евклида и поэтому не изменится, если мы будем рассматривать многочлены над большим полем.*

Д о к а з а т е л ь с т в о. 1) Применяя алгоритм Евклида к f и g,

получим:

$$\begin{cases} f = g \cdot q_1 + r_1, & \deg r_1 < \deg g, \\ g = r_1 \cdot q_2 + r_2, & \deg r_2 < \deg r_1, \\ r_1 = r_2 \cdot q_3 + r_3, & \deg r_3 < \deg r_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ r_{k-3} = r_{k-2} \cdot q_{k-1} + r_{k-1}, & \deg r_{k-1} < \deg r_{k-2}, \\ r_{k-2} = r_{k-1} \cdot q_k + r_k, & \deg r_k < \deg r_{k-1}, \\ r_{k-1} = r_k \cdot q_{k+1}. \end{cases}$$

Тогда последний ненулевой остаток r_k и будет наибольшим общим делителем. Действительно, проверим выполнение условий из определения наибольшего общего делителя.

а) Просматривая систему равенств снизу вверх, из последнего равенства видим, что $r_k | r_{k-1}$, тогда из предпоследнего $r_k | r_{k-2}$, и т. д, наконец, из первых двух равенств заключаем, что $r_k | g$ и $r_k | f$. Следовательно, r_k делит f и g.

б) Пусть $d' | f$ и $d' | g$. Тогда из первого равенства следует, что d' делит r_1, из второго — что d' делит r_2 и т. д. Следовательно, d' делит r_k.

2) Пусть d_1 и d_2 — приведённые наибольшие общие делители f и g. Тогда по пункту б) $d_1 | d_2$ и $d_2 | d_1$. Отсюда $\deg d_2 \leq \deg d_1$ и $\deg d_1 \leq \deg d_2$. Следовательно, $\deg d_1 = \deg d_2$. Предположим, что $d_2 = d_1 \cdot h$, где h — многочлен нулевой степени, т. е. элемент из P, а так как d_1 и d_2 приведены, то $h = 1$, а потому $d_1 = d_2$.

3) Рассмотрим некоторое поле L, содержащее поле P. Тогда $P[x] \subset L[x]$, но если мы рассматриваем многочлены $f, g \in P[x]$ и применяем к ним алгоритм Евклида, то наибольший общий делитель над P остаётся точно таким же и для поля L. Теорема доказана.

Покажем, что с изменением поля P делители многочленов меняются.

П р и м е р. Рассмотрим поля

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Для колец многочленов имеем включения

$$\mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x].$$

Следовательно, многочлен с рациональными коэффициентами можно рассматривать как многочлен с действительными и комплексными коэффициентами, но, как видно из следующей таблицы, делители могут быть разными.

Многочлен	$\mathbb{Q}[x]$	$\mathbb{R}[x]$	$\mathbb{C}[x]$
x^2-2	$1, x^2-2$	$1, x^2-2, x\pm\sqrt{2}$	$1, x^2-2, x\pm\sqrt{2}$
x^2+1	$1, x^2+1$	$1, x^2+1$	$1, x^2+1, x\pm i$

Видим, что с увеличением поля число делителей может увеличиваться.

17.4. *Задачи на делимость многочленов.*

1) (Ф.С. 577). Определить наибольший общий делитель многочленов:

a) $x^4+x^3-3x^2-4x-1$ и x^3+x^2-x-1;
b) $x^5+x^4-x^3-2x-1$ и $3x^4+2x^3+2x-2$;
c) $x^6-7x^4+8x^3-7x+7$ и $3x^5-7x^3+3x^2-7$;
d) $x^5-2x^4+x^3+7x^2-12x+10$ и $3x^4-6x^3+5x^2+2x-2$;
e) $x^6+2x^4-4x^3-3x^2+8x-5$ и x^5+x^3-x+1.

2) (Ф.С. 578). Пользуясь алгоритмом Евклида, подобрать многочлены $M_1(x)$ и $M_2(x)$ так, чтобы $f_1(x)M_2(x)+f_2(x)M_1(x)=\delta(x)$, где $\delta(x)$ — наибольший общий делитель $f_1(x)$ и $f_2(x)$:

a) $f_1(x)=x^4+2x^3-x^2-4x-2$,
$f_2(x)=x^4+x^3-x^2-2x-2$;
b) $f_1(x)=x^5+3x^4+x^3+x^2+3x+1$,
$f_2(x)=x^4+2x^3+x+2$;
c) $f_1(x)=x^6-4x^5+11x^4-27x^3+37x^2-35x+35$,
$f_2(x)=x^5-3x^4+7x^3-20x^2+10x-25$;
d) $f_1(x)=3x^7+6x^6-3x^5+4x^4+14x^3-6x^2-4x+4$,
$f_2(x)=3x^6-3x^4+7x^3-6x+2$;
e) $f_1(x)=3x^5+5x^4-16x^3-6x^2-5x-6$,
$f_2(x)=3x^4-4x^3-x^2-x-2$;
f) $f_1(x)=4x^4-2x^3-16x^2+5x+9$,
$f_2(x)=2x^3-x^2-5x+4$.

17.5. *Задачи для любознательных.*

1) (ВМО, 1899) Доказать, что выражение

$$A=2903^n-803^n-464^n+261^n$$

при любых натуральных n делится на 1897.

2) (BMO, 1900) Пусть a, b, c, d и m — такие целые числа, что

$$am^3 + bm^2 + cm + d$$

делится на 5, причём d на 5 не делится. Доказать, что всегда можно найти такое целое число n, для которого

$$dn^3 + cn^2 + bn + a$$

также будет делиться на 5.

3) (BMO, 1901) Доказать, что сумма n–х степеней

$$1^n + 2^n + 3^n + 4^n,$$

где n — целое положительное число, делится на 5 в том и только в том случае, если показатель степени n не делится на 4.

4) (BMO, 1903) Пусть $n = 2^{p-1}(2^p - 1)$, где $2^p - 1$ — простое число. Доказать, что сумма всех делителей числа n, отличных от самого n, в точности равна n.

5) (BMO, 19022) Доказать, что многочлен четвёртой степени $x^4 + 2x^2 + 2x + 2$ нельзя разложить в произведение двух квадратных трёхчленов $x^2 + ax + b$ и $x^2 + cx + d$ с целыми коэффициентами a, b, c и d.

6) (CMO, Задача 384) Доказать, что у числа $\underbrace{11\ldots1}_{1977}$ не может быть 365 различных делителей.

7) (OK, 17-6) Сколько существует последовательностей длины n из чисел 1 и 2 таких, что их сумма делится на 3?

8) (OK, 16-1) Найти все многочлены, удовлетворяющие условию

$$f(2x) = f'(x)f''(x).$$

§ 18. Линейное уравнение от двух неизвестных

18.1. Критерий разрешимости. В кольце многочленов $P[x]$ над полем P рассмотрим уравнение

$$f \cdot u + g \cdot v = h, \quad f, g, h \in P[x] \tag{1}$$

с неизвестными $u, v \in P[x]$. Следующая теорема даёт необходимое и достаточное условие разрешимости этого уравнения.

Т е о р е м а 1. *Уравнение* (1) *имеет решение тогда и только тогда, когда наибольший общий делитель многочленов f и g делит h.*

Д о к а з а т е л ь с т в о. Предположим, что уравнение (1) имеет решение (u_0, v_0). Тогда справедливо равенство

$$f \cdot u_0 + g \cdot v_0 = h.$$

Так как приведённый наибольший общий делитель (f, g) делит f и g, то (f, g) делит и h.

Обратно. Предположим, что $(f, g) \mid h$. Применяя алгоритм Евклида, найдём (f, g):

$$\begin{cases} f = g \cdot q_1 + r_1, & \deg r_1 < \deg g, \\ g = r_1 \cdot q_2 + r_2, & \deg r_2 < \deg r_1, \\ r_1 = r_2 \cdot q_3 + r_3, & \deg r_3 < \deg r_2, \\ \ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\ r_{k-3} = r_{k-2} \cdot q_{k-1} + r_{k-1}, & \deg r_{k-1} < \deg r_{k-2}, \\ r_{k-2} = r_{k-1} \cdot q_k + r_k, & \deg r_k < \deg r_{k-1}, \\ r_{k-1} = r_k \cdot q_{k+1}. \end{cases}$$

Деля r_k на коэффициент при старшей степени получим приведённый наибольший общий делитель (f, g).

Обозначим

$$I = \{f\,a + g\,b \mid a, b \in P[x]\}.$$

Очевидно, множество I удовлетворяет следующим условиям:

1) если $h_1, h_2 \in I$, то разность $h_1 - h_2 \in I$;

2) если $h_1 \in I$, $t \in P[x]$, то произведения $h_1 \cdot t \in I$.

Следовательно, I — идеал кольца $P[x]$. Так как $f = f \cdot 1 + g \cdot 0$, $g = f \cdot 0 + g \cdot 1$, то многочлены f и g лежат в I. Отсюда по алгоритму Евклида $r_1 \in I$, $r_2 \in I$, $\ldots$, $r_k \in I$. Приведённый наибольший общий делитель (f, g) получается из r_k делением на его старший коэффициент, а потому и $(f, g) \in I$. Следовательно, $h \in I$, так как h делится на (f, g), а потому найдутся $u, v \in P[x]$, при которых $f \cdot u + g \cdot v = h$. Таким образом, уравнение (1) имеет решение. Теорема доказана.

18.2. Взаимно простые многочлены. Если $(f, g) = 1$, т. е. приведённый наибольший общий делитель многочленов f и g равен 1, то говорим, что f и g *взаимно просты.* Следующая теорема описывает свойства взаимно простых многочленов.

Т е о р е м а 2. *В кольце $P[x]$ справедливы следующие утверждения*:

а) $(f,g)=1$ *тогда и только тогда, когда существуют* u *и* v *такие, что* $f\cdot u+g\cdot v=1$;

б) *если* $(f,\varphi)=1$ *и* $(f,\psi)=1$, *то* $(f,\varphi\cdot\psi)=1$;

в) *если* $d\,|\,(fg)$ *и* $(d,f)=1$, *то* $d\,|\,g$;

г) *если* $d_1\,|\,f$, $d_2\,|f$ *и при этом* $(d_1,d_2)=1$, *то* $d_1d_2\,|\,f$.

Д о к а з а т е л ь с т в о. а) Рассмотрим уравнение

$$f\cdot u+g\cdot v=1.$$

По теореме 1 это уравнение имеет решение тогда и только тогда, когда $(f,g)=1$.

б) По пункту а) существуют u_1,v_1 такие, что

$$f\cdot u_1+\varphi\cdot v_1=1,$$

а также такие u_2,v_2, что

$$f\cdot u_2+\psi\cdot v_2=1.$$

Перемножая эти два равенства, получим

$$f\cdot(fu_1u_2+\psi u_1v_2+\varphi v_1u_2)+\varphi\psi\cdot v_1v_2=1,$$

т. е. нашлись многочлены u,v, удовлетворяющие равенству

$$f\cdot u+\varphi\psi\cdot v=1.$$

Тогда по пункту а) $(f,\varphi\psi)=1$.

в) Опять по пункту а) существуют u,v такие, что

$$d\cdot u+f\cdot v=1.$$

Умножим обе части этого равенства на g, получим

$$d\cdot ug+fg\cdot v=g.$$

Видим, что первое и второе слагаемое делятся на d. Следовательно, и сумма делится на d, а потому $d\,|\,g$.

г) Опять ввиду а) существуют u,v такие, что

$$d_1\cdot u+d_2\cdot v=1.$$

Умножая обе части на f, получим

$$d_1 \cdot uf + d_2 \cdot vf = f.$$

Так как $d_1|f$, то $f = d_1 f_1$ для некоторого многочлена f_1. Аналогично из того, что $d_2|f$, заключаем, что $f = d_2 f_2$ для некоторого многочлена f_2. Подставив эти выражения для f в левую часть предыдущего равенства, получим

$$d_1 d_2 \cdot uf_2 + d_1 d_2 \cdot vf_1 = f.$$

Видим, что первое и второе слагаемое в левой части делятся на $d_1 d_2$, следовательно, $d_1 d_2 \,|\, f$. Теорема доказана.

18.3. Общее решение уравнения $f \cdot u + g \cdot v = 1$. Рассмотрим уравнение

$$f \cdot u + g \cdot v = 1, \quad (f, g) = 1. \tag{2}$$

Очевидно, что, научившись решать такие уравнения, мы сможем решать и уравнения с произвольной правой частью. Справедлива

Т е о р е м а 3. 1) *Общее решение уравнения* (2) *имеет вид*

$$(u_0 + gt, v_0 - ft),$$

где (u_0, v_0) *— некоторое частное решение, а* t *— произвольный многочлен из* $P[x]$. 2) *Если степени* f *и* g *больше нуля, то существует единственное решение* (u, v) *с условием*:

$$\deg u < \deg g, \quad \deg v < \deg f.$$

Д о к а з а т е л ь с т в о. 1) То, что пара $(u_0 + gt, v_0 - ft)$ является решением уравнения (2), проверяется прямой подстановкой. Проверим, что любое наперёд заданное решение представимо в таком виде. Пусть (u_*, v_*) — некоторое решение уравнения (2). Имеем два равенства:

$$f \cdot u_* + g \cdot v_* = 1,$$
$$f \cdot u_0 + g \cdot v_0 = 1.$$

Вычитая из первого второе, получим

$$f \cdot (u_* - u_0) = g \cdot (v_0 - v_*). \tag{3}$$

Видим, что этот многочлен делится на f и на g, т. е.

$$f \,|\, g(v_0 - v_*), \quad g \,|\, f(u_* - u_0).$$

Учитывая, что $(f, g) = 1$ по пункту в) теоремы 2 имеем $f \mid (v_0 - v_*)$, т. е. $v_0 - v_* = ft$ для некоторого многочлена $t \in P[x]$. Аналогично $u_* - u_0 = gt_1$ для некоторого многочлена t_1, но, учитывая (3), заключаем, что $t = t_1$. Следовательно,

$$(u_*, v_*) = (u_0 + gt, v_0 - ft).$$

2) Пусть $\deg f > 0$, $\deg g > 0$ и (u_0, v_0) — какое-нибудь решение уравнения (2). Поделим u_0 с остатком на g, а v_0 — на f, получим:

$$u_0 = g \cdot q_1 + u_1, \quad \text{где } u_1 = 0, \text{ или } \deg u_1 < \deg g;$$

$$v_0 = f \cdot q_2 + v_1, \quad \text{где } v_1 = 0, \text{ или } \deg v_1 < \deg f.$$

Заметим, что остатки u_1 и v_1 ненулевые. Действительно, если $u_1 = 0$, то из равенства

$$f \cdot u_0 + g \cdot v_0 = 1$$

заключаем, что

$$fg \cdot q_1 + g \cdot v_0 = 1,$$

но это равенство невозможно, так как левая часть делится на многочлен g ненулевой степени, а правая — нет. Аналогично проверяется, что $v_1 \neq 0$.

Докажем, что пара (u_1, v_1) является решением уравнения (2). Имеем:

$$1 = f \cdot u_0 + g \cdot v_0 = f(gq_1 + u_1) + g(fq_2 + v_1) = fg(q_1 + q_2) + fu_1 + gv_1,$$

т. е.

$$fg(q_1 + q_2) = 1 - fu_1 - gv_1. \tag{4}$$

Предположим, что обе части равенства (4) ненулевые. Тогда степень левой части равна

$$\deg f + \deg g + \deg(q_1 + q_2) \geq \deg f + \deg g,$$

а степень правой — меньше чем

$$\deg f + \deg g.$$

Противоречие. Следовательно, обе части равенства (4) равны нулю, т. е.

$$1 - fu_1 - gv_1 = 0,$$

а потому

$$fu_1 + gv_1 = 1.$$

Заметим, что любое другое решение не удовлетворяет неравенствам из теоремы, что следует из пункта 1). Теорема доказана.

Можно заметить, что пара $(gt, -ft)$, $t \in P[x]$ является общим решением однородного уравнения

$$f \cdot u + g \cdot v = 0. \tag{5}$$

Следовательно, так же как для систем линейных уравнений, заключаем, что общее решение неоднородного уравнения (2) есть сумма частного решения (u_0, v_0) и общего решения однородного уравнения (5).

У п р а ж н е н и е. Что можно сказать про аналог уравнения Пелля

$$u^2 - f \cdot v^2 = 1, \quad f \in P[x],$$

в кольце $P[x]$?

18.4. *Задачи на решения линейного уравнения от двух неизвестных.*

3) (Ф.С. 579). Пользуясь алгоритмом Евклида, подобрать многочлены $M_1(x)$ и $M_2(x)$ так, чтобы $f_1(x)M_2(x) + f_2(x)M_1(x) = 1$:

a) $f_1(x) = 3x^3 - 2x^2 + x + 2$, $f_2(x) = x^2 - x + 1$;

b) $f_1(x) = x^4 - x^3 - 4x^2 + 4x + 1$, $f_2(x) = x^2 - x - 1$;

c) $f_1(x) = x^5 - 5x^4 - 2x^3 + 12x^2 - 2x + 12$,
$f_2(x) = x^3 - 5x^2 - 3x + 17$;

d) $f_1(x) = 2x^4 + 3x^3 - 3x^2 - 5x + 2$,
$f_2(x) = 2x^3 + x^2 - x - 1$;

e) $f_1(x) = 3x^4 - 5x^3 + 4x^2 - 2x + 1$,
$f_2(x) = 3x^3 - 2x^2 + x - 1$;

f) $f_1(x) = x^5 + 5x^4 + 9x^3 + 7x^2 + 5x + 3$,
$f_2(x) = x^4 + 2x^3 + 2x^2 + x + 1$.

4) (Ф.С. 580). Способом неопределённых коэффициентов подобрать $M_1(x)$ и $M_2(x)$ так, чтобы $f_1(x)M_2(x) + f_2(x)M_1(x) = 1$:

a) $f_1(x) = x^4 - 4x^3 + 1$, $f_2(x) = x^3 - 3x^2 + 1$;

b) $f_1(x) = x^3$, $f_2(x) = (1 - x)^2$;

c) $f_1(x) = x^4$, $f_2(x) = (1 - x)^4$.

18.5. *Задачи для любознательных.*

1) (ВМО, 1904) Доказать, что уравнение

$$x_1 + 2x_2 + \ldots + nx_n = a$$

не допускает решений в целых положительных числах тогда и только тогда, когда уравнение

$$y_1 + 2y_2 + \ldots + ny_n = a - \frac{n(n+1)}{2}$$

не допускает решений в неотрицательных целых числах (a — целое положительное число).

2) (ВМО, 1905) Каковы необходимые и достаточные условия для того, чтобы система уравнений

$$x + py = n, \quad x + y = p^z,$$

где n и p — заданные натуральные числа, допускала решения в целых положительных числах (x, y, z)? Докажите, что число таких решений не может быть больше 1.

3) (СМО, Задача 380) Доказать, что при любом целом $k > 0$ уравнение $x^2 + y^2 = z^k$ имеет решение в целых положительных числах.

18.6. *Экзамен: мифы и реальность.*

Настоящая лекция — последняя в этом семестре. Лекции и семинары заканчиваются, начинается зачётная неделя. Мне остаётся лишь поблагодарить вас за аккуратное посещение лекций, за ваше внимание и ваши вопросы, а также — пожелать удачи в зачётную неделю и поздравить с наступающим Новым годом.

Обычно, про экзамен рассказывают на консультации, когда уже не остаётся времени на подготовку и мало, что можно изменить. Возможно, эти записи будут кому–то полезными.

Экзамен — это что?

После новогодних каникул вас ожидает первая сессия и первый экзамен. Давайте обсудим: что такое экзамен, как к нему готовиться, что надо и что не надо делать во время подготовки, а также на самом экзамене.

На вопрос «Что такое экзамен?» вездесущий ИИ сразу выдаст некую банальность, вроде: «Экзамен — это проверка знаний». Отсюда мораль: думайте сами! Более интересный ответ даёт студенческий фольклор:

— Экзамен — это беседа двух умных людей.

— А если один из них дурак?

— То второй остаётся без стипендии.

Понятно, что это — шутка, которая, возможно, развеселит, но вряд ли поможет вам на экзамене. Большинство преподавателей склонны считать, что экзамен — это продолжение процесса обучения, когда студент может осмыслить прослушанный курс и проверить насколько хорошо он его усвоил. Отбросив все умные слова и глубокие теории, вы можете считать, что экзамен — это то мероприятие, на которое вы, во что бы то ни стало, обязаны прийти и убедить всех, а прежде всего себя, что вы — самый умный и талантливый. При этом вы должны *помнить, что «знания — это ваш главный оберег от двойки»!*

Подготовка к экзамену.

Как и когда надо начинать готовиться к экзамену? Если вы готовитесь к первому экзамену в Новом году, то не стоит после боя курантов и поздравлений бежать и садиться за конспекты и учебники. В первые дни Нового года отдохните и побудьте с родителями, с родственниками, друзьями. Им будет приятно ваше внимание и забота. Можете считать эти дни активного отдыха началом подготовки к экзамену.

К сожалению, отдых быстро заканчивается и надо приниматься за работу. Как правило, на подготовку даётся 4–5 дней. За это время вы вряд ли научитесь решать задачи. Поэтому сосредоточьтесь на теории. В первый день просмотреть весь лекционный материал, вспомнить или прочтите определения и формулировки основных теорем, попытайтесь представить связи между различными частями курса. Разделите число страниц ваших конспектов или число страниц в учебном пособии, где изложен лекционный материал, на количество дней, отпущенных на подготовку к экзамену и начинайте подробно разбирать весь материал. Прочитав определение или теорему, отложите учебник, возьмите листочек и попытайтесь написать всё по памяти. Еще лучше попробуйте рассказать пройденный материал кому–то из своих друзей, кто будет выступать в роли экзаменатора и задавать каверзные вопросы. Материал можно считать усвоенным если вы можете изложить его никуда не заглядывая. Пройдя таким образом весь курс, посвятите вторую часть последнего дня подготовки повторению. Теперь, представляя лекционный курс

целиком, вспомнить не только определения и формулировки теорем, но и основные идеи доказательства. *Помните, что «главный оберег от двойки — это знания»!*

Во время подготовки к экзамену постарайтесь ограничить использование своих любимых девайсов. Отдохните от них и пусть они отдохнут от вас. Не зависайте в соцсетях. Знаний это вам вряд ли прибавит, но голову забьёт ненужной информацией. Заставьте работать подсознание, думайте и постоянно держите в голове изучаемый материал. Собираясь на обед или на прогулку, прочитайте формулировку теоремы и её доказательство. По дороге обдумывайте прочитанный материал, пытайтесь понять идею доказательства. То же самое проделывайте перед сном: мысленно прокручивайте пройденный за день материал. На следующий день поймёте, что всё становится на свои места и курс прорисовывается более ясно.

Накануне экзамена стоит пораньше лечь спать, чтобы прийти на экзамен бодрым и отдохнувшим. В шутке о том, что «главное, что студент должен принести на экзамен, — это голова», как и во всякой шутке, лишь доля шутки. На экзамене вам придётся решать задачи и вспоминать доказательства теорем. Если вы что-то не доучили или забыли, то есть шанс сообразить и вспомнить, но если вы не выспались и засыпаете на ходу, то вам уже вряд ли что–то поможет. По этой же причине не стоит готовиться к экзамену по ночам. Ваш организм должен активно работать именно в утренние часы (время экзамена).

Волнение и здоровый мандраж перед экзаменом — вещи полезные. Каждый когда–то должен через это пройти, а вам ещё предстоит сдавать массу экзаменов. Поэтому, на первых курсах, как правило, автоматы не ставят. Надо учиться сдавать экзамены, справляясь со своими нервами и уметь продемонстрировать свои великолепные знания (даже если они не столь полны и идеальны). *Помните, что «главный оберег от двойки — это знания»!*

Чтобы успокоиться перед экзаменом давайте подумаем и оценим риски: наилучший и наихудший исход экзамена. Наилучший исход: вы получаете положительную оценку и идёте с друзьями отмечать свой успех. Наихудший исход: вы получаете двойку и идёте отмечать свою неудачу и успех товарищей. Понятно, что второй вариант, не очень приятен, но не стоит переживать. Сделайте соответствующие выводы и готовьтесь к следующему экзамену, успокоив себя мыслью,

что всякий студент должен получить хоть одну двойку. При этом *помните, что «главный оберег от двойки — это знания»!*

Шпоры и списывание.

Как мы уже поняли, шпаргалки надо писать. Надо ли их брать на экзамен? Решать вам. Некоторые студенты берут их для собственного успокоения, но никогда не используют. Если же вы приготовили шпаргалки для того, чтобы списать, помните, что все ваши «оригинальные» методы списывания как–то: положить шпаргалку на сидение, маленький листочек вложить в ладошку, принести листочки на которых уже написаны ответы на вопросы и остаётся лишь достать ответы на нужный билет, а также масса других — не являются столь уж оригинальными и преподаватели, большинство из которых также окончили НГУ, прекрасно всё это знают. Если вы списываете и вам не делают замечание, то это еще не значит, что никто ничего не видит. При ответе вам просто дадут дополнительные вопросы или задачи, либо более тщательно начнут «капать» написанные ответы. Следуйте правилу: не пишите то чего не понимаете. Если вы не сможете объяснить значение символов и правильно прочесть термины, написанные в ваших листочках, то ваши шансы на успех резко уменьшатся, а преподаватель поймёт, что ответы списаны, хотя он это может и не озвучивать. *Помните, что «главный оберег от двойки — это знания»!*

На экзамене.

Взяв счастливый (или не очень счастливый) билет, садитесь и начинайте готовиться. Не стоит паниковать и волноваться если билет вы знаете не очень хорошо. Посидите и успокойтесь. Затем запишите то, что знаете: определения, формулировки. Пишите всё, что знаете по этому билету. Попробуйте решить задачу. Даже если не можете решить её целиком, разберите частные случаи, сформулируйте гипотезу. Затем попробуйте вспомнить и записать доказательства теорем. Если вы всё это сделали и у вас есть время, прорепетируйте ваш ответ, проговорив его мысленно, стараясь предугадать возможные вопросы экзаменатора.

Студент и преподаватель: коллеги или ... ?

Получить на первом курсе, в первую сессию, да еще и на первом экзамене двойку — почти невозможно. Но, разумеется, если вы сильно захотите, то сможете этого добиться: преподаватель не сможет вам отказать и, наверняка, пойдёт навстречу. Вместе с тем, помните, что

преподаватели доброжелательно относятся к студентам и склонны скорее завысить оценку, нежели занизить, а тем более завалить вас. Ни один из уважающих себя преподавателей не станет сводить с вами счеты на экзамене, даже если вы в течение семестра 7 раз наступили ему на любимую мозоль. Все понимают, что у студента и преподавателя слишком разные весовые категории и преподаватель легко может завалить студента, дав трудную задачу или спрашивая те вещи, которые, обычно, плохо усваиваются. Кроме того, есть негласное правило: не принимать экзамен у своих студентов, а учитывая, что экзамен принимают несколько преподавателей, вы можете выбрать любого понравившегося. Только помните: *«главный оберег от двойки — это знания»!*

Приметы.

Существует масса примет, связанных с экзаменом. Например, идя на экзамен, надо подложить пятак под левую пятку; нельзя стричься во время сессии и бриться перед экзаменом, в день экзамена надо вставать с кровати и входить в аудиторию с левой ноги, в ночь перед экзаменом надо положить под подушку конспекты лекций, призвать на помощь Халяву, заговорить зачётную книжку и т. д. Конечно, вы прекрасно понимаете, что всё это суеверия чистой воды, в которые ни один здравомыслящий человек, а тем более студент НГУ, не поверит. Хотя бытует мнение, что приметы помогают даже тем кто в них не верит.

Настоящей науке известны лишь две приметы, которые действительно работают. Первая: вечером перед экзаменом надо прогуляться до Пруда с уточками, погладить Ёжика и обнять Земной шар. Вторая примета: если во время экзамена кто-то думает о вас, переживает и держит кулачки, то это наверняка вам поможет.

Через несколько лет, с теплотой вспоминая первую сессию, будете улыбаясь недоумевать: почему так сильно волновались, стоило ли оно того? Но это придёт лишь потом, а пока: *Помните, ...*

§ 19. Корни и значения многочлена

19.1. Теорема Безу. До сих пор мы смотрели на многочлены как на формальные выражения, которые можно складывать и умножать. Существует и другая точка зрения, рассматривающая много-

член $f(x) \in P[x]$ как функцию $f\colon P \longrightarrow P$. Если

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \in P[x],$$

то для всякого $c \in P$ *значением многочлена в точке* c назовём элемент

$$f(c) = a_0 + a_1c + \ldots + a_nc^n \in P.$$

Если $f(c) = 0$, то c называется *корнем многочлена* $f(x)$.

Следующая теорема показывает, что задача нахождения корней многочлена равносильна задаче нахождения его линейных делителей.

Т е о р е м а (Безу, 1779). *Элемент $c \in P$ является корнем многочлена $f(x) \in P[x]$ тогда и только тогда, когда $(x - c) \mid f(x)$.*

Д о к а з а т е л ь с т в о. Разделим $f(x)$ с остатком на $x - c$, получим

$$f(x) = (x - c)q(x) + r, \quad q(x) \in P[x], \quad r \in P.$$

Отсюда при $x = c$ получим $f(c) = r$. Из этого равенства и следует нужное утверждение.

19.2. Формула Тейлора. Дадим вначале

О п р е д е л е н и е. Если

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \in P[x]$$

— некоторый многочлен, то его *производной* (*первой производной*) называется многочлен

$$f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}.$$

Производная от производной называется *второй производной* и обозначается $f''(x)$. Вообще для произвольного натурального $i > 1$ i–я производная определяется правилом

$$f^{(i)}(x) = (f^{(i-1)}(x))'.$$

При этом мы считаем, что $f^{(0)}(x) = f(x)$.

Мы дали формальное определение производной многочлена, не привлекая понятие предела и других прелестей математического анализа. Тем не менее, можно показать, что привычные формулы для производных справедливы и в нашем случае.

У п р а ж н е н и е. Проверьте следующие равенства:
1) $(f+g)' = f' + g'$;
2) $(f \cdot g)' = f'g + g'f$;
3) $(cf)' = cf'$, $c \in P$.

Т е о р е м а 1. *Пусть P — поле нулевой характеристики. Если f — многочлен степени n из $P[x]$, то для всякого элемента $c \in P$ справедливо равенство*

$$f(x) = \sum_{i=0}^{n} \frac{f^{(i)}(c)}{i!}(x-c)^i.$$

Эта формула называется *формулой Тейлора.*

Д о к а з а т е л ь с т в о. Положим

$$f(x) = b_0 + b_1(x-c) + \ldots + b_n(x-c)^n.$$

Тогда

$$\begin{aligned}
&f'(x) = b_1 + 2b_2(x-c) + \ldots + nb_n(x-c)^{n-1},\\
&f''(x) = 2b_2 + 3\cdot 2b_3(x-c) + \ldots + n(n-1)b_n(x-c)^{n-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&f^{(i)}(x) = i!b_i + \ldots + n(n-1)\ldots(n-i+1)b_n(x-c)^{n-i},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&f^{(n)}(x) = n!b_n.
\end{aligned}$$

При $x = c$ в этих формулах остаются только свободные члены:

$$f^{(i)}(c) = i!\, b_i, \quad i = 0, 1, \ldots, n.$$

Значит,

$$b_i = \frac{f^{(i)}(c)}{i!}, \quad i = 0, 1, \ldots, n.$$

Теорема доказана.

19.3. Интерполяционная формула Лагранжа.

З а д а ч а и н т е р п о л я ц и и. Пусть задано $n+1$ попарно различных элементов $x_0, x_1, \ldots, x_n$ поля P и $n+1$ элементов $y_0, y_1, \ldots, y_n$ из P. Требуется найти такую функцию $f(x)$: $P \longrightarrow P$, для которой выполняются равенства $y_i = f(x_i)$, $i = 0, 1, \ldots, n$. Наглядно это можно представить в виде следующей таблицы.

x	x_0	x_1	$\ldots$	x_i	$\ldots$	x_n
$f(x)$	y_0	y_1	$\ldots$	y_i	$\ldots$	y_n

Понятно, что при такой постановке задача имеет множество решений. Если же искать функцию в виде многочлена, то можно показать, что существует единственный многочлен степени не выше n, удовлетворяющий условиям этой задачи. Действительно, будем искать $f(x)$ в виде многочлена

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in P[x]$$

с неизвестными коэффициентами a_i. Подставляя в него x_j, $j = 0, 1, \ldots, n$, получим систему $n+1$ уравнения с $n+1$ неизвестным:

$$\begin{cases} a_0 + a_1 x_0 + \ldots + a_n x_0^n = y_0, \\ a_0 + a_1 x_1 + \ldots + a_n x_1^n = y_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + a_1 x_n + \ldots + a_n x_n^n = y_n. \end{cases}$$

Определитель этой системы:

$$\begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{vmatrix}$$

— знаменитый определитель Вандермонда, который равен

$$\prod_{0 \le i < j \le n} (x_i - x_j)$$

и по условию отличен от нуля. Следовательно, система имеет единственное решение.

Существует готовая формула (*формула Лагранжа*), позволяющая сразу написать этот многочлен:

$$f(x) = \sum_{i=0}^{n} y_i \cdot \frac{(x - x_0)(x - x_1)\ldots(x - x_{i-1})(x - x_{i+1})\ldots(x - x_n)}{(x_i - x_0)(x_i - x_1)\ldots(x_i - x_{i-1})(x_i - x_{i+1})\ldots(x_i - x_n)}.$$

Легко проверить, что $y_i = f(x_i)$, $i = 0, 1, \ldots, n$.

19.4. Кратные корни. Как следует из теоремы Безу, если c является корнем многочлена, то он делится на $x - c$. Может случиться, что многочлен делится не только на $x - c$, но и на некоторую его степень.

О п р е д е л е н и е. Если

$$f(x) = (x-c)^k g(x)$$

и $g(c) \neq 0$, то c называется *k–кратным корнем многочлена* или корнем кратности k многчлена $f(x)$. Если $k = 1$, то говорят, что c — *простой корень.*

Т е о р е м а 2. *Над полем нулевой характеристики корень кратности $k > 1$ многочлена является корнем кратности $k-1$ его производной.*

Д о к а з а т е л ь с т в о. Пусть

$$f(x) = (x-c)^k g(x), \quad g(c) \neq 0.$$

Тогда

$$f'(x) = k(x-c)^{k-1}g(x) + (x-c)^k g'(x) = (x-c)^{k-1}[kg(x) + (x-c)g'(x)].$$

Нетрудно проверить, что выражение в квадратных скобках не обращается в нуль при $x = c$.

У п р а ж н е н и е. Для полей ненулевой характеристики теорема неверна.

19.5. *Задачи на корни уравнения и задачу интерполяции.*

1) (Ф.С. 549). Выполнить деление с остатком:

a) $x^4 - 2x^3 + 4x^2 - 6x + 8$ на $x - 1$;
b) $2x^5 - 5x^3 - 8x$ на $x + 3$;
c) $4x^3 + x^2$ на $x + 1 + i$;
d) $x^3 - x^2 - x$ на $x - 1 + 2i$.

2) (Ф.С. 550). Пользуясь схемой Горнера, вычислить $f(x_0)$:

a) $f(x) = x^4 - 3x^3 + 6x^2 - 10x + 16, \quad x_0 = 4$;
b) $f(x) = x^5 + (1+2i)x^4 - (1+3i)x^2 + 7, \quad x_0 = -2 - i$.

3) (Ф.С. 551). Пользуясь схемой Горнера, разложить полином $f(x)$ по степеням $x - x_0$:

a) $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$, $x_0 = -1$;
b) $f(x) = x^5$, $x_0 = 1$;
c) $f(x) = x^4 - 8x^3 + 24x^2 - 50x + 90$, $x_0 = 2$;
d) $f(x) = x^4 + 2ix^3 - (1+i)x^2 - 3x + 7 + i$, $x_0 = -i$.

4) (Ф.С. 552). Пользуясь схемой Горнера, разложить на простейшие дроби:

a) $\dfrac{x^3 - x + 1}{(x-2)^5}$; b) $\dfrac{x^4 - 2x^3 + 3}{(x+1)^5}$.

5) (Ф.С. 555). Чему равен показатель кратности корня:
a) 2 для полинома $x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$;
b) -2 для полинома $x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16$?

5) (Ф.С. 631). Пользуясь способом Ньютона, построить полином наименьшей степени по данной таблице значений:

a)
x	0	1	2	3	4
$f(x)$	1	2	3	4	6

; b)
x	-1	0	1	2	3
$f(x)$	6	5	0	3	2

;

c)
x	1	$\frac{9}{4}$	4	$\frac{25}{4}$
$f(x)$	1	$\frac{3}{2}$	2	$\frac{5}{2}$

, найти $f(2)$; d)
x	1	2	3	4	6
$f(x)$	5	6	1	-4	10

.

6) (Ф.С. 632). Построить полином по заданной таблице значений, пользуясь формулой Лагранжа:

a)
x	1	2	3	4
y	2	1	4	3

; b)
x	1	i	-1	$-i$
y	1	2	3	4

.

7) (Ф.С. 585). Отделить кратные множители полиномов:
a) $x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$;
b) $x^5 - 10x^3 - 20x^2 - 15x - 4$;
c) $x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27$;
d) $x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8$.

19.6. *Задачи для любознательных.*
1) (ВМО, 1899) Пусть x_1 и x_2 — корни уравнения

$$x^2 - (a + d)x + ad - bc = 0.$$

Доказать, что тогда x_1^3 и x_2^3 — корни уравнения

$$y^2 - (a^3 + d^3 + 3abc + 3bcd)y + (ad - bc)^3 = 0.$$

2) (ВМО, 1902) Доказать, что: a) всякий квадратный трёхчлен

$$Ax^2 + Bx + C$$

с известными числовыми коэффициентами можно представить в виде

$$k\frac{x(x-1)}{1 \cdot 2} + lx + m,$$

где коэффициенты k, l и m имеют вполне определённые числовые значения;

б) квадратный трёхчлен

$$Ax^2 + Bx + C$$

принимает целочисленные значения при всех целых x в том и только в том случае, если при записи его в виде

$$k\frac{x(x-1)}{1\cdot 2} + lx + m$$

клэффициенты k, l и m — целые числа.

3) (BMO, 1907) Пусть p и q — два целых нечётных числа. Доказать, что уравнение

$$x^2 + 2px + 2q = 0$$

не может иметь рациональных корней.

4) (СМО, задача 16) Каким условиям должны удовлетворять числа p, q, чтобы многочлен $x^3 + px + q$ обращался в нуль при трёх различных действительных значениях аргумента x?

5) (СМО, задача 19) Доказать, что ни для одного многочлена $p(x)$ с целыми коэффициентами не могут выполняться равенства $p(7) = 5$; $p(15) = 9$.

6) (ОК, 02-4) Многочлен $f(x)$ не имеет вещественных корней. Доказать, что многочлен

$$f(x) + \frac{f''(x)}{2!} + \frac{f^{(4)}(x)}{4!} + \dots$$

также не имеет вещественных корней.

7) (ОК, 03-1) Докажите, что если все корни многочлена

$$x^n + a_2x^{n-2} + \dots + a_{n-1}x + a_n$$

вещественны, то $a_2 \le 0$.

§ 20. Кольца с однозначным разложением

20.1. Определения и примеры. Из основной теоремы арифметики следует, что всякое целое число a единственным способом представимо в виде произведения простых чисел:

$$a = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \quad \varepsilon = \pm 1, \alpha_i \in \mathbb{N},$$

где p_i — простые числа. Возникает естественный вопрос: верно ли аналогичное утверждение для кольца многочленов $P[x]$? В настоящем параграфе даётся утвердительный ответ на этот вопрос.

Будем называть кольцо K *целостным*, если оно коммутативн и не имеет делителей нуля. Далее в этом параграфе будем считать, что K — целостное кольцо с единицей. Очевидно, что этим условиям удовлетворяет, в частности, кольцо целых чисел и кольцо многочленов над полем.

О п р е д е л е н и е. Элементы a и b из K называются *ассоциированными,* если $a = b \cdot \varepsilon$, где ε — обратимый элемент кольца K.

О п р е д е л е н и е. Ненулевой необратимый элемент a из K называется *неразложимым,* если из равенства $a = b \cdot c$ следует, что либо b обратимый, либо c обратимый.

О п р е д е л е н и е. Целостное кольцо K с единицей называется *кольцом с однозначным разложением*, если:

а) всякий ненулевой необратимый элемент из K разлагается в произведение неразложимых множителей;

б) если $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ — два разложения на неразложимые множители, то $r = s$ и, возможно после перенумерации сомножителей, p_1 ассоциирован с q_1, p_2 ассоциирован с q_2 и т. д., наконец, p_r ассоциирован с q_r.

П р и м е р ы. 1) В кольце $\mathbb{Z}$ обратимыми являются элементы $-1, 1$, ассоциированные элементы: a и $-a$; неразложимые элементы: $\pm p$, где p — простое число.

2) В кольце $P[x]$ обратимыми являются элементы $\alpha \in P$, $\alpha \neq 0$, ассоциированные элементы: $f, \alpha f$, $\alpha \neq 0$; неразложимые элементы: неразложимые элементы кольца многочленов $P[x]$. Как мы видели ранее, множество неразложимых элементов зависит от поля P.

Оба кольца $\mathbb{Z}$ и $P[x]$ являются кольцами с однозначным разложением. Для кольца $\mathbb{Z}$ это следует из основной теоремы арифметики, а для кольца $P[x]$ мы докажем это ниже.

20.2. Кольцо многочленов как кольцо с однозначным разложением. Для доказательства основного утверждения настоящего пункта нам потребуется

Л е м м а 1. *Если $f \in P[x]$, p — неразложим в $P[x]$, то либо $p \mid f$, либо $(p, f) = 1$.*

Д о к а з а т е л ь с т в о. Пусть $d = (p, f)$, т. е. $p = d \cdot h$ для некоторого многочлена $h \in P[x]$. Так как p неразложим, то либо $d \in$

P^*, либо $h \in P^*$. Если $d \in P^*$, то $d = 1$, так как (p, f) — приведённый наибольший общий делитель. Если $h \in P^*$, то $d = \frac{1}{h}p$, т. е. $p \mid f$. Лемма доказана.

Теперь мы готовы доказать следующее утверждение.

Т е о р е м а. *Если P — поле, то $P[x]$ — кольцо с однозначным разложением.*

Д о к а з а т е л ь с т в о. Для доказательства надо проверить условия а) и б) из определения кольца с однозначным разложением. Пусть f — ненулевой необратимый элемент из $P[x]$.

а) Если f неразложим, то доказывать нечего, в противном случае разлагаем f в произведение двух многочленов: $f = f_1 \cdot f_2$, где $\deg f_1 < \deg f$, $\deg f_2 < \deg f$. Если какой–то многочлен f_i разложим, то разлагаем его: $f_i = f_{i1} \cdot f_{i2}$, где $\deg f_{i1} < \deg f_i$, $\deg f_{i2} < \deg f_i$ и т. д. Видим, что на каждом шаге мы получаем многочлен меньшей степени, а потому процесс оборвётся, т. е. на некотором шаге получим разложение f в произведение неразложимых множителей.

б) Пусть

$$f = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

— два разложения в произведение неразложимых множителей. Надо доказать, что $r = s$ и после перенумерации $p_i = q_i \cdot \varepsilon_i$, $i = 1, 2, \dots, r$, где ε_i — обратимый элемент. Доказательство проведем индукцией по r. При $r = 1$ нужное утверждение следует из определения неразложимого элемента.

Предположим, что утверждение доказано для $r-1$ и надо установить его для r. Имеем $p_1 \mid q_1 q_2 \dots q_s$. Покажем, что p_1 делит некоторый q_i. Действительно, по лемме 1 либо $p_1 \mid q_1$, либо $(p_1, q_1) = 1$. Если p_1 делит q_1, то это нас устраивает. Если $(p_1, q_1) = 1$, то $p_1 \mid q_2 \dots q_s$ (по теореме о взаимной простоте). Опять по лемме 1 либо $p_1 \mid q_2$, либо $p_1 \mid q_3 \dots q_s$ и т. д. Через несколько шагов получим, что $p_1 \mid q_i$ для некоторого i. Выполняя перенумерацию сомножителей, будем считать, что $p_1 \mid q_1$, т. е. $q_1 = p_1 \varepsilon_1$, где $\varepsilon_1 \in P^*$, а это значит, что p_1 и q_1 ассоциированы. Так как $P[x]$ без делителей нуля, то, сокращая обе части нашего равенства на p_1, приходим к равенству

$$p_2 \dots p_r = \varepsilon_1 q_2 \dots q_s.$$

По индукционному предположению $r = s$ и p_2 ассоциирован с $\varepsilon_1 q_2$, который ассоциирован с q_2, p_3 ассоциирован с q_3 и т. д., наконец, p_r ассоциирован с q_r. Теорема доказана.

П р и м е р. Если рассматривать многочлен x^2-2 как многочлен из $\mathbb{Q}[x]$, то он неразложим. Если рассматривать его как многочлен из $\mathbb{R}[x]$, то он разложим и является произведением двух неразложимых многочленов:

$$x^2-2=(x+\sqrt{2})(x-\sqrt{2}).$$

При этом по–другому его можно представить в виде

$$x^2-2=[r(x+\sqrt{2})][r^{-1}(x-\sqrt{2})],\quad r\in\mathbb{R}$$

и легко заметить, что $x+\sqrt{2}$ ассоциирован с $r(x+\sqrt{2})$, а $x-\sqrt{2}$ ассоциирован с $r^{-1}(x-\sqrt{2})$.

20.3. Примеры целостных колец, не являющихся кольцами с однозначным разложением.

П р и м е р 1. В этом примере разложение на неразложимые сомножители не обрывается (не выполняется условие а) определения кольца с однозначным разложением).

Пусть $K=\mathbb{Z}[2^{\frac{1}{2}},2^{\frac{1}{4}},2^{\frac{1}{8}},\dots,2^{\frac{1}{2^i}},\dots]$ — подкольцо поля $\mathbb{R}$, порождённое множеством целых чисел $\mathbb{Z}$ и числами $2^{\frac{1}{2}},2^{\frac{1}{4}},2^{\frac{1}{8}},\dots,2^{\frac{1}{2^i}},\dots$ То, что K является целостным кольцом следует из включения $K\subseteq\mathbb{R}$. Также очевидно, что K содержит единицу.

Чтобы понять, как устроены элементы из K, определим кольца

$$K_r=\mathbb{Z}[2^{\frac{1}{2}},2^{\frac{1}{4}},2^{\frac{1}{8}},\dots,2^{\frac{1}{2^r}}],\quad r=1,2,\dots$$

Очевидно,

$$K=\bigcup_{r=1}^{\infty}K_r.$$

Кроме того, легко заметить, что

$$K_r=\mathbb{Z}[2^{\frac{1}{2^r}}].$$

Если рассмотреть произвольный элемент a из K, то он лежит в некотором K_r, а потому найдется многочлен $g\in\mathbb{Z}[x]$ такой, что $a=g(\theta)$, где $\theta=2^{\frac{1}{2^r}}$.

Покажем, что процесс разложения на неразложимые множители в K не обрывается:

$$2=2^{\frac{1}{2}}\cdot 2^{\frac{1}{2}}=2^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}=2^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot 2^{\frac{1}{8}}\cdot 2^{\frac{1}{8}}=\dots,$$

как видно, этот процесс не оборвется. Но надо показать, что в этих разложениях нет обратимых элементов.

Л е м м а 2. *Все элементы* $2^{\frac{1}{2^m}}$, $m = 0, 1, 2, \ldots$ *необратимы в кольце* K.

Д о к а з а т е л ь с т в о. Пусть некоторый элемент $2^{\frac{1}{2^m}}$ обратим, т. е. найдется многочлен $g(x) \in \mathbb{Z}[x]$ и элемент $\theta = 2^{\frac{1}{2^r}}$ такие, что

$$2^{\frac{1}{2^m}} \cdot g(\theta) = 1.$$

Можно считать, что $r \geq m$. Тогда $f(\theta) = 1$ для многочлена $f(x) = x^{2^{r-m}} g(x)$ из $\mathbb{Z}[x]$. При этом $f(x)$ — многочлен без свободного члена. С другой стороны, $\theta^{2^r} = 2$.

Рассмотрим многочлены $f(x) - 1$ и $x^{2^r} - 2$. Для них θ является корнем. Поэтому по теореме Безу

$$(x - \theta) \mid (f(x) - 1) \quad \text{и} \quad (x - \theta) \mid (x^{2^r} - 2),$$

а потому они не взаимно просты, т. е. $(f(x) - 1, x^{2^r} - 2) \neq 1$. Покажем, что $x^{2^r} - 2$ неразложим в $\mathbb{Z}[x]$. Пусть, напротив,

$$x^{2^r} - 2 = g_1 \cdot g_2, \quad g_i \in \mathbb{Z}[x], \quad \deg g_i > 0.$$

Определим отображение $\mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$, где $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ — поле, состоящее из двух элементов, как отображение, переводящее многочлен

$$a = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in \mathbb{Z}[x]$$

в многочлен

$$\overline{a} = \overline{a}_0 + \overline{a}_1 x + \overline{a}_2 x^2 + \ldots + \overline{a}_n x^n \in \mathbb{Z}_2[x],$$

где $\overline{a}_i$ — остаток от деления a_i на 2. Можно заметить, что это отображение является гомоморфизмом колец, а потому равенство

$$x^{2^r} - 2 = g_1 \cdot g_2$$

перейдет в равенство

$$x^{2^r} = \overline{g_1} \cdot \overline{g_2}.$$

П р и м е р. Равенство

$$(x^2 - 3\,x + 2)(x^4 - 1) = x^6 - 3\,x^5 + 2\,x^4 - x^2 + 3\,x - 2$$

переходит в равенство

$$(x^2+x)(x^4+\overline{1}) = x^6+x^5+x^2+x.$$

Нетрудно показать, что $\overline{g_1} = x^s$ и $\overline{g_2} = x^{2^r-s}$ для некоторого натурального s. Значит, в g_1 и g_2 все коэффициенты, кроме старших, чётные. В частности, свободные члены многочленов g_i чётные. При перемножении многочленов свободные члены перемножаются и свободный член произведения $g_1 \cdot g_2$ делится на 4, а в левой части нашего равенства

$$x^{2^r} - 2 = g_1 \cdot g_2$$

свободный член не делится на 4. Противоречие. Следовательно, $x^{2^r} - 2$ неразложим в $\mathbb{Z}[x]$.

Теперь мы хотим воспользоваться леммой 1, но в ней требуется, чтобы многочлен был неразложим в $P[x]$, где P — поле.

Следующее утверждение будет доказано позже (см. следствие леммы 5 из § 29).

Л е м м а 3. *Многочлен из $\mathbb{Z}[x]$ неразложим в $\mathbb{Q}[x]$ тогда и только тогда, когда он неразложим в $\mathbb{Z}[x]$.*

По этой лемме $x^{2^r} - 2$ неразложим в $\mathbb{Q}[x]$, а потому ввиду леммы 1

$$(x^{2^r} - 2) \mid (f(x) - 1),$$

т. е.

$$f(x) - 1 = (x^{2^r} - 2) \cdot h(x),$$

для некоторого $h(x) \in \mathbb{Z}[x]$. Следовательно, свободный член многочлена $f(x) - 1$ равен свободному члену многочлена $(x^{2^r} - 2) \cdot h(x)$, но это невозможно, так как свободный член первого равен -1, а свободный член второго делится на 2. Следовательно, все элементы в нашем разложении необратимы и процесс разложения на неразложимые множители не обрывается.

П р и м е р 2. В этом примере существует разложение на неразложимые множители, но оно неоднозначно. Рассмотрим кольцо $K = \mathbb{Z}[\sqrt{-3}]$. Это подкольцо поля $\mathbb{C}$, порожденное $\mathbb{Z}$ и $\sqrt{-3}$. Нетрудно проверить, что

$$K = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

Так как $K \subseteq \mathbb{C}$, то K — целостное кольцо и, очевидно, содержит единицу.

Покажем, что каждый элемент из K разлагается на неразложимые множители. Для всякого элемента $\alpha = a+b\sqrt{-3}$ из K определим норму $N\colon K \longrightarrow \mathbb{N} \cup \{0\}$, полагая $N(\alpha) = a^2 + 3\,b^2$. Нетрудно проверить, что норма удовлетворяет следующему равенству:

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta).$$

Действительно, если $\beta = c + d\sqrt{-3}$ — другой элемент из K, то

$$\alpha \cdot \beta = (a\,c - 3\,b\,d) + (a\,d + b\,c)\sqrt{-3},$$

и для нормы произведения справедливо равенство

$$N(\alpha \cdot \beta) = (a\,c - 3\,b\,d)^2 + 3\,(a\,d + b\,c)^2 = a^2\,c^2 + 9b^2\,d^2 + 3a^2\,d^2 + 3b^2\,c^2.$$

С другой стороны,

$$N(\alpha) \cdot N(\beta) = (a^2 + 3\,b^2)(c^2 + 3\,d^2) = a^2\,c^2 + 3a^2\,d^2 + 3b^2\,c^2 + 9b^2\,d^2,$$

т. е. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

Используя установленное равенство, дадим описание обратимых элементов кольца K.

Л е м м а 4. *В кольце K обратимыми являются только элементы* 1 *и* -1.

Д о к а з а т е л ь с т в о. Предположим, что $\alpha = a + b\sqrt{-3} \in K$ обратим. Тогда для него найдётся $\beta \in K$ такой, что $\alpha\beta = 1$. По свойству нормы из этого равенства получим $N(\alpha) \cdot N(\beta) = 1$. Следовательно, $N(\alpha) = N(\beta) = 1$, но это означает, что $a^2 + 3\,b^2 = 1$, а это равенство выполняется лишь при условии $a = \pm 1$, $b = 0$. Лемма доказана.

Рассмотрим некоторый ненулевой необратимый элемент α из K и будем разлагать его в произведение:

$$\alpha = \alpha_1 \cdot \alpha_2 = \alpha_{11} \cdot \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{22} = \ldots$$

Этому разложению соответствует разложение для норм:

$$N(\alpha) = N(\alpha_1) \cdot N(\alpha_2) = N(\alpha_{11}) \cdot N(\alpha_{12}) \cdot N(\alpha_{21}) \cdot N(\alpha_{22}) = \ldots$$

Как мы знаем, $N(\alpha) = 1$ тогда и только тогда, когда $\alpha = \pm 1$, т. е. является обратимым элементом в K. Учитывая, что норма принимает целые неотрицательные значения, видим, что для норм этот процесс

оборвётся. Таким образом, всякий элемент $\alpha \in K$ разлагается на неразложимые сомножители.

Покажем, что это разложение неединственно. Действительно,

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}),$$

т. е. 4 имеет два разложения на множители. Ясно, что 2 не ассоциировано с $1 \pm \sqrt{-3}$. Покажем, что 2 неразложим. Предположим, что $2 = \alpha \cdot \beta$, $\alpha, \beta \in K$. Тогда $N(2) = N(\alpha) \cdot N(\beta)$. Так как $N(2) = 4$ имеет единственное нетривиальное разложение $4 = 2 \cdot 2$ в $\mathbb{Z}$, то достаточно заметить, что 2 не является нормой никакого числа из K. Если бы $N(\alpha) = a^2 + 3\,b^2 = 2$, то отсюда следовало бы, что $b = 0$, а так как a — целое число, то это равенство невозможно.

Аналогично устанавливается, что и $1 \pm \sqrt{-3}$ неразложим (заметим, что $N(1 \pm \sqrt{-3}) = 4$).

20.4. *Задачи для любознательных.*

1) (СМО, Задача 385) Доказать, что любое целое число можно представить в виде суммы пяти кубов целых чисел.

§ 21. Идеалы в кольце многочленов

21.1. Кольцо многочленов как кольцо главных идеалов. Напомним (см. § 3), что подмножество I кольца K называется идеалом (пишем: $I \lhd K$), если выполнены следующие два условия:

а) если $a, b \in I$, то $a - b \in I$;

б) если $a \in I$, $c \in K$, то $a \cdot c \in I$, $c \cdot a \in I$.

П р и м е р. Пусть $K = P[x]$, а f — некоторый многочлен из K. Тогда идеалом является множество всех многочленов, которые делятся на f, т. е.

$$I = \{f \cdot g \mid g \in K\}.$$

Такой идеал называется главным.

Напомним (см. § 3), что если M — некоторое подмножество кольца K, то символом (M) обозначается пересечение всех идеалов в K, содержащих M, иными словами, (M) — наименьший идеал, содержащий множество M. Если $I = (M)$, то говорим, что I порождается множеством M или что M является базой идеала I.

Более конструктивное описание идеала (M) было дано в лемме 7, в которой было доказано, что если K — коммутативное кольцо с единицей и $M \subseteq K$, то

$$(M) = \left\{ \sum m_i b_i \mid m_i \in M, \quad b_i \in K \right\},$$

где в каждой сумме лишь конечное число коэффициентов b_i отлично от нуля.

Как мы знаем, в кольце $\mathbb{Z}$ всякий идеал является главным. Аналогичным свойством обладает и кольцо $P[x]$.

Т е о р е м а 1. *В кольце $P[x]$ каждый идеал является главным, т. е. имеет вид*

$$(f) = \{f \cdot g \mid g \in P[x]\}$$

для некоторого f из $P[x]$.

Д о к а з а т е л ь с т в о. Пусть I — некоторый идеал в $P[x]$. Если $I = \{0\}$, то $I = (0)$. Предположим, что $I \neq (0)$, и выберем многочлен f наименьшей степени, лежащий в I. Покажем, что $I = (f)$. Действительно, включение $I \supseteq (f)$ очевидно. Пусть g — произвольный многочлен из I. Разделим g с остатком на f, получим:

$$g = fq + r, \quad \text{где } r = 0 \text{ или } \deg r < \deg f.$$

Если при этом $r \neq 0$, то $r = g - fq \in I$, что противоречит тому, что f — многочлен наименьшей степени в I. Следовательно, $g = fq$, т. е. $g \in (f)$, а потому $I = (f)$.

Кольцо, в котором каждый идеал является главным называется *кольцом главных идеалов*.

У п р а ж н е н и е. Укажите в кольце $P[x, y]$ идеал, который не является главным.

У к а з а н и е. Рассмотрите идеал (x, y), состоящий из многочленов без свободного члена.

21.2. Кольца с условием максимальности. Следующая теорема является и определением.

Т е о р е м а 2. *Для всякого кольца K следующие условия равносильны*:

а) *всякий идеал кольца K порождается конечным множеством элементов*;

б) *всякая возрастающая цепочка идеалов*

$$I_1 \leq I_2 \leq \ldots$$

стабилизируется на некотором номере n, т. е. $I_n = I_{n+1} = \ldots$

При любом из этих условий K называется *кольцом с условием максимальности.* Класс всех таких колец обозначается Max.

Д о к а з а т е л ь с т в о. а) $\Rightarrow$ б). Предположим противное: существует цепочка идеалов, которая неограниченно растёт:

$$I_1 < I_2 < \ldots < I_n < I_{n+1} < \ldots$$

Возьмём множество

$$I = \bigcup_{k=1}^{\infty} I_k.$$

Покажем, что I — идеал в K. Действительно, если $a, b \in I$, то $a \in I_n$, $b \in I_m$ для некоторых натуральных n и m. Следовательно, $a, b \in I_s$ при $s = \max\{n, m\}$. Так как I_s — идеал, то $a - b \in I_s$, а потому $a - b \in I$. Пусть теперь $a \in I$, $c \in K$. Следовательно, $a \in I_n$ для некоторого n. Следовательно, $ac \in I_n$, а потому $ac \in I$. Таким образом, I действительно является идеалом.

Допустим, что $I = (a_1, a_2, \ldots, a_m)$, т. е. I порождается конечным множеством элементов. Пусть $a_1 \in I_{n_1}$, $a_2 \in I_{n_2}$, $\ldots$, $a_m \in I_{n_m}$. Положим $n = \max\{n_1, n_2, \ldots, n_m\}$. Тогда идеал I_n содержит элементы $a_1, a_2, \ldots, a_m$, но тогда I_n содержит и I. Значит, $I_n = I$, и, следовательно,

$$I_n = I_{n+1} = \ldots$$

Противоречие.

б) $\Rightarrow$ а). От противного. Пусть идеал I не конечно порождённый. Выберем элемент $a_1 \in I$, тогда $(a_1) < I$; выберем $a_2 \in I \setminus (a_1)$, тогда $(a_1, a_2) < I$; выберем $a_3 \in I \setminus (a_1, a_2)$, тогда $(a_1, a_2, a_3) < I$, и так как идеал I не является конечно порождённым, то этот процесс можно продолжать до бесконечности. Получаем цепочку идеалов

$$(a_1) < (a_1, a_2) < (a_1, a_2, a_3) < \ldots,$$

которая не стабилизируется. Противоречие. Теорема доказана.

21.3. Теорема Гильберта о базах. Если рассмотреть бесконечную систему линейных уравнений от переменных $x_1, x_2, \ldots, x_n$, то она эквивалентна некоторой конечной подсистеме. Если мы рассмотрим произвольную систему полиномиальных уравнений

$$f_\alpha(x_1, \ldots, x_n) = 0, \quad \alpha \in A,$$

то возникает естественный вопрос: будет ли она равносильна некоторой своей конечной подсистеме

$$g_1(x_1,\dots,x_n)=0,\quad g_2(x_1,\dots,x_n)=0,\dots,g_s(x_1,\dots,x_n)=0?$$

Положительный ответ на этот вопрос следует из теоремы Гильберта о базах.

Т е о р е м а (Д. Гильберт, 1890). *Пусть K — коммутативное кольцо с единицей. Если $K\in\mathrm{Max}$, то $K[x]\in\mathrm{Max}$.*

Д о к а з а т е л ь с т в о теоремы проведем от противного. Допустим, что K — коммутативное кольцо с единицей, удовлетворяющее условию максимальности ($K\in\mathrm{Max}$), но $K[x]\notin\mathrm{Max}$. Следовательно, найдётся цепочка идеалов, которая не стабилизируется, или, что то же самое, I — идеал в $K[x]$, который не конечно порождён. Выберем в I множество многочленов, полагая $f_0=0$, и для каждого $i=0,1,\dots$ выберем многочлен f_{i+1} наименьшей степени, который не лежит в идеале $(f_0,f_1,\dots,f_i)$, т. е. $f_{i+1}\in I\setminus(f_0,f_1,\dots,f_i)$. Пусть n_i — степень многочлена f_i, а a_i — его старший коэффициент, $i=1,2,\dots$ Очевидно,

$$n_1\le n_2\le\dots$$

Рассмотрим цепочку идеалов в кольце K:

$$(a_1)\le(a_1,a_2)\le\dots\le(a_1,a_2,\dots,a_i)\le(a_1,a_2,\dots,a_i,a_{i+1})\le\dots.$$

Так как $K\in\mathrm{Max}$, заключаем, что для некоторого номера i справедливо равенство

$$(a_1,a_2,\dots,a_i)=(a_1,a_2,\dots,a_i,a_{i+1}).$$

Тогда

$$a_{i+1}=\sum_{k=1}^{i}a_k\,b_k \text{ при подходящих } b_k\in K.$$

Рассмотрим многочлен

$$g(x)=f_{i+1}(x)-\sum_{k=1}^{i}f_k(x)b_k\,x^{n_{i+1}-n_k}.$$

Если $g\in(f_0,f_1,\dots,f_i)$, то и $f_{i+1}\in(f_0,f_1,\dots,f_i)$, что противоречит построению последовательности многочленов. Если

$$g\in I\setminus(f_0,f_1,\dots,f_i),$$

то, замечая, что степень g меньше степени f_{i+1}, приходим к противоречию, с тем, что f_{i+1} — многочлен наименьшей степени из разности $I \setminus (f_0, f_1, \ldots, f_i)$. Теорема доказана.

У п р а ж н е н и е. Где используется наличие единицы в кольце K?

Как мы знаем, кольцо целых чисел является кольцом с условием максимальности, так как каждый идеал порождается одним элементом. Заметим также, что поле является кольцом с условием максимальности. Действительно, мы знаем, что каждый идеал поля либо нулевой, либо совпадает со всем полем. В первом случае он порождается нулём, а во втором — единицей. Замечая, что $K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$, индукцией по n из теоремы Гильберта получаем

С л е д с т в и е 1. *Если K — поле или кольцо $\mathbb{Z}$, то $K[x_1, \ldots, x_n] \in$* Max.

С л е д с т в и е 2. *Всякая система полиномиальных уравнений от n неизвестных над любым полем или кольцом $\mathbb{Z}$ равносильна некоторой конечной подсистеме.*

Д о к а з а т е л ь с т в о. Пусть K — поле или кольцо $\mathbb{Z}$. Пусть $M \subseteq K^n$ — это множество всех решений нашей системы:

$$f_\alpha(x_1, \ldots, x_n) = 0, \quad \alpha \in A. \tag{1}$$

Символом I обозначим множество

$$\{f \in K[x_1, \ldots, x_n] \mid f(x_1^0, x_2^0, \ldots, x_n^0) = 0 \text{ при всех } (x_1^0, x_2^0, \ldots, x_n^0) \in M\}$$

— множество всех многочленов, корни которых лежат в M. Легко проверить, что I — идеал в кольце $K[x_1, \ldots, x_n]$ и этот идеал содержит все многочлены f_α, $\alpha \in A$. По следствию 1 идеал I конечно порождён. Следовательно, найдутся многочлены g_1, g_2, …, g_s из $K[x_1, \ldots, x_n]$ такие, что $I = (g_1, g_2, \ldots, g_s)$. Покажем, что система (1) равносильна системе

$$g_1(x_1, \ldots, x_n) = 0, \quad g_2(x_1, \ldots, x_n) = 0, \ldots, g_s(x_1, \ldots, x_n) = 0, \tag{2}$$

т. е.

$$\{\text{решение системы (1)}\} = \{\text{решение системы(2)}\}.$$

Действительно, для всякого многочлена f_α найдутся многочлены h_{α_1}, h_{α_2}, …, h_{α_s} из $K[x_1, \ldots, x_n]$ такие, что

$$f_\alpha = g_1 h_{\alpha_1} + g_2 h_{\alpha_2} + \ldots + g_s h_{\alpha_s},$$

а потому если какая–то n–ка является решением системы (2), то она является решением системы (1). Обратное включение очевидно.

Теорема Гильберта о базах даёт решение знаменитой проблемы конечной базируемости системы инвариантов, поставленной Гордоном в 1870 году, причём на фоне изощрённых вычислительных работ XIX века логически безупречные и исключительно простые рассуждения Гильберта выглядели столь необычно, что Линдеман назвал их «страшными», а Гордон заявил: «Это не математика. Это теология». Лишь когда в 1893 году, опираясь на эту свою теорему «чистого существования» конечной базы, Гильберт указал метод, позволяющий за конечное число шагов построить явную конечную базу системы инвариантов, недоверие сменилось восхищением и Гордон любезно признал: «Я убедился, что у теологии есть свои преимущества».

21.4. *Задачи на идеалы и фактор–кольца.*

1) (П. 1781). Будут ли следующие множества подгруппами аддитивной группы, подкольцами или идеалами указанных ниже колец:

а) множество $n\mathbb{Z}$ чисел, кратных числу $n > 1$, в кольце целых чисел $\mathbb{Z}$;

б) множество $\mathbb{Z}$ целых чисел в кольце $\mathbb{Z}[x]$ целочисленных многочленов;

в) множество $n\mathbb{Z}[x]$ многочленов, коэффициенты которых кратны числу $n > 1$, в кольце $\mathbb{Z}[x]$ целочисленных многочленов;

г) множество $\mathbb{N}$ натуральных чисел в кольце целых чисел $\mathbb{Z}$;

д) множество $\mathbb{Z}$ целых чисел в кольце A целых гауссовых чисел, т. е. чисел вида $a + bi$ с целыми рациональными a, b;

е) множество B чисел $a+bi$, где $a = b$, в кольце A целых гауссовых чисел;

ж) множество C чисел вида $x(1 + i)$ в кольце A целых гауссовых чисел, где x пробегает всё кольцо A;

з) множество $\mathbb{Z}[x]$ целочисленных многочленов в кольце $\mathbb{Q}[x]$ многочленов над полем $\mathbb{Q}$ рациональных чисел;

и) множество I многочленов, не содержащих членов с x^k для всех $k < n$, где $n > 1$, в кольце $\mathbb{Z}[x]$ целочисленных многочленов;

к) множество I многочленов с чётными свободными членами в кольце $\mathbb{Z}[x]$ целочисленных многочленов;

л) множество I многочленов с чётными старшими коэффициентами в кольце $\mathbb{Z}[x]$ целочисленных многочленов.

2) (П. 1785*). *Кольцом главных идеалов* называется коммутативное кольцо с единицей и без делителей нуля, в котором каждый идеал — главный (см. задачу 1783). Доказать, что каждое из следующих колец является кольцом главных идеалов:

а) кольцо $\mathbb{Z}$ целых чисел;

б) кольцо $P[x]$ многочленов от одного неизвестного x над полем P;

в) кольцо A целых гауссовых чисел.

3) (П. 1796). Пусть $I = (x, 2)$ — идеал, порождённый множеством из двух элементов x и 2, в кольце целочисленных многочленов $\mathbb{Z}[x]$. Доказать, что:

а) идеал I состоит из всех многочленов с чётными свободными членами;

б) идеал I не является главным;

в) факторкольцо $\mathbb{Z}[x]/I$ изоморфно полю вычетов по модулю 2.

4) (П. 1799). Пусть $\mathbb{Z}_p$ — поле вычетов по простому модулю p, $f(x)$ — многочлен степени n из кольца $\mathbb{Z}_p[x]$, неприводимый над полем $\mathbb{Z}_p$ (из теории полей известно, что такой многочлен существует для любого простого p и любого натурального n), I — главный идеал, порождённый многочленом $f(x)$ в кольце $\mathbb{Z}_p[x]$. Доказать, что факторкольцо $\mathbb{Z}_p[x]/I$ есть конечное поле, и найти число его элементов.

§ 22. Теорема о существовании корня

22.1. Постановка задачи. Сформулируем следующую задачу. Пусть P — поле, f — многочлен степени ≥ 1 из $P[x]$. Построить поле L, удовлетворяющее следующим условиям:

1) L содержит P как подполе;

2) в L существует элемент α такой, что $f(\alpha) = 0$, т. е. α — корень многочлена f.

Учитывая, что многочлен f можно представить в виде произведения $f = f_1 f_2 \dots f_m$ неразложимых многочленов, можно считать, что f неразложим, так как если α — корень многочлена f_i, то α — корень и многочлена f.

Т е о р е м а о с у щ е с т в о в а н и и к о р н я. *Для всякого поля P и всякого неразложимого многочлена $f \in P[x]$ степени*

$n > 0$ существует поле L со свойствами 1)–2). *Если, кроме того, выполнено условие*

3) *подполе в L, порождённое P и α, совпадает с L,*

то L единственное с точностью до изоморфизма, т. е. любые два поля со свойствами 1)–3) *изоморфны.*

Доказательство теоремы разобьём на две части. Вначале покажем, что такое поле L действительно существует, а затем докажем единственность.

22.2. Существование. Рассмотрим фактор–кольцо $L' = P[x]/(f)$, где (f) — главный идеал, порождённый многочленом f. Проверим, что L' — поле. Так как операции сложения и умножения определены на представителях, то все аксиомы кольца выполняются. Проверяем оставшиеся аксиомы.

У2) $(g + (f)) \cdot (h + (f)) = (h + (f)) \cdot (g + (f))$.

Эта аксиома выполнена в силу определения умножения смежных классов и коммутативности умножения в $P[x]$.

У3) Легко заметить, что смежный класс $1+(f)$ является единицей в L'.

У4) Пусть $g + (f) \neq (f)$, т. е. $g \notin (f)$, а потому g не делится на f. Так как f неразложим, то по лемме 1 из § 21 $(f, g) = 1$, а значит существуют $u, v \in P[x]$ такие, что

$$fu + gv = 1.$$

Тогда обратным к классу $g+(f)$ будет $(g+(f))^{-1} = v+(f)$. Действительно,

$$(g + (f)) \cdot (v + (f)) = gv + (f) = 1 - fu + (f) = 1 + (f).$$

Таким образом, L' — поле.

В L' укажем подполе, изоморфное полю P. Положим

$$P' = \{a + (f) \mid a \in P\}.$$

Пусть $\omega\colon P \longrightarrow P'$ определяется следующим образом: $a \longmapsto a + (f)$, $a \in P$. Покажем, что ω — изоморфизм P на P', т. е.

а) ω — однозначно;

б) ω — унивалентно;

в) ω — отображение *на*;

г) $\omega(a + b) = \omega(a) + \omega(b)$;

д) $\omega(a \cdot b) = \omega(a) \cdot \omega(b)$.

а) То, что отображение ω однозначно — очевидно. б) Если $a \neq b$, то надо показать, что $a+(f) \neq b+(f)$. Пусть $a+(f) = b+(f)$, тогда $a-b \in (f)$ и $f \mid (a-b)$, т. е. $a-b = f \cdot g$ и, следовательно, $a-b=0$ (учесть, что a и b — элементы из поля, а потому имеют нулевую степень), а потому $a = b$. в) Очевидно. г) Левая часть: $\omega(a+b) = a+b+(f)$; правая часть: $\omega(a)+\omega(b) = (a+(f))+(b+(f)) = a+b+(f)$. д) Проверяется аналогично. Таким образом, ω — изоморфизм.

Теперь возьмём $L = (L' \backslash P') \cup P$ с перенесёнными из L' операциями:

$$A+B = \begin{cases} a+b & \text{при } A=a\in P, \quad B=b\in P; \\ g+b+(f) & \text{при } A=g+(f)\notin P', \quad B=b\in P; \\ a+h+(f) & \text{при } A=a\in P, \quad B=h+(f)\notin P'; \\ g+h+(f) & \text{при } A=g+(f)\notin P', \quad B=h+(f)\notin P', \\ & \quad A+B\notin P'; \\ c & \text{при } A=g+(f)\notin P', \quad B=h+(f)\notin P', \\ & \quad A+B=c+(f)\in P'; \end{cases}$$

$$A\cdot B = \begin{cases} ab & \text{при } A=a\in P, \quad B=b\in P; \\ gb+(f) & \text{при } A=g+(f)\notin P', \quad B=b\in P; \\ ah+(f) & \text{при } A=a\in P, \quad B=h+(f)\notin P'; \\ gh+(f) & \text{при } A=g+(f)\notin P', \quad B=h+(f)\notin P', \\ & \quad A\cdot B\notin P'; \\ c & \text{при } A=g+(f)\notin P', \quad B=h+(f)\notin P', \\ & \quad A\cdot B=c+(f)\in P'. \end{cases}$$

Проверим, что L — искомое. То, что для него выполняется свойство 1), очевидно. Покажем, что выполняется свойство 2). Возьмём $\alpha = x+(f)$ и покажем, что $f(\alpha)=0$. Пусть

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad a_i \in P,$$

тогда

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = a_0 + a_1(x+(f)) + \ldots + a_n(x+(f))^n =$$

$$= a_0 + a_1 x + \ldots + a_n x^n + (f) = f + (f) = 0.$$

У п р а ж н е н и е. Что будет, если многочлен f разложим?

22.3. Единственность. Докажем, что построенное поле единственно. Воспользуемся тем, что если два поля изоморфны одному

и тому же полю, то они изоморфны между собой. Пусть M — поле, удовлетворяющее условиям 1)–3), т. е.

1) $M \supseteq P$;

2) найдётся элемент $\beta \in M$ такой, что $f(\beta) = 0$;

3) подполе поля M, порождённое P и β, совпадает с M.

Надо доказать, что $M \simeq L'$. Предварительно заметим, что

$$M = \{g(\beta) \mid g \in P[x]\}.$$

Понятно, что

$$M \supseteq \{g(\beta) \mid g \in P[x]\},$$

т. е. всякий элемент $b_0 + b_1\,\beta + \ldots + a_m\,\beta^m$ лежит в M. Покажем, что множество

$$\{g(\beta) \mid g \in P[x]\}$$

является подполем, содержащим P и β. Обозначим

$$M_1 = \{g(\beta) \mid g \in P[x]\}.$$

Заметим, что если $g_1(\beta), g_2(\beta) \in M_1$, то и элементы

$$g_1(\beta) - g_2(\beta) = (g_1 - g_2)(\beta), \quad g_1(\beta) \cdot g_2(\beta) = (g_1 \cdot g_2)(\beta)$$

лежат в M_1. Пусть теперь $g(\beta) \neq 0$. Тогда $f \nmid g$ (иначе $g = f \cdot h$ и $g(\beta) = f(\beta) \cdot h(\beta) = 0$). Так как f неразложим, то опять по лемме 1 из § 21 $(f, g) = 1$. Значит, существуют u, v такие, что $fu + gv = 1$. При $x = \beta$ имеем

$$f(\beta) \cdot u(\beta) + g(\beta) \cdot v(\beta) = 1.$$

Так как $f(\beta) \cdot u(\beta) = 0$, то $v(\beta) = g(\beta)^{-1}$. Следовательно, мы установили, что множество M_1 является полем, а так как оно содержит P и β, то оно содержит и M.

Докажем, что M и L' изоморфны. Рассмотрим отображение

$$\varphi\colon L' \longrightarrow M,$$

определённое правилом

$$g + (f) \longmapsto g(\beta),$$

т. е. смежному классу $g + (f)$ сопоставим элемент $g(\beta)$ из M. Проверим, что φ — изоморфизм L' на M. Для этого надо проверить следующие условия:

а) φ — однозначно;
б) φ — унивалентно;
в) φ — отображение *на*;
г) $\varphi(A+B)=\varphi(A)+\varphi(B)$;
д) $\varphi(A\cdot B)=\varphi(A)\cdot\varphi(B)$.

а) Покажем, что от выбора представителя наше определение не зависит. Пусть $g+(f)=g_1+(f)$. Тогда $f\mid(g-g_1)$, т. е. $g-g_1=f\cdot f_1$, отсюда $g(\beta)-g_1(\beta)=0$ и $g(\beta)=g_1(\beta)$.

б) Пусть $g+(f)\neq h+(f)$. Надо доказать, что $g(\beta)\neq h(\beta)$. Пусть, напротив, $g(\beta)=h(\beta)$. Тогда β — корень $g-h$ и f. По теореме Безу

$$(x-\beta)\mid(g(x)-h(x))\text{ и }(x-\beta)\mid f(x).$$

Значит, $(g-h,f)\neq 1$, а так как f неразложим, то опять по лемме 1 из § 21 имеем: $f\mid(g-h)$, откуда $g+(f)=h+(f)$. Противоречие.

в) Следует из установленного равенства:

$$M=\{g(\beta)\mid g\in P[x]\}.$$

г) Пусть $A=g+(f)$, $B=h+(f)$, тогда левая часть

$$\varphi(A+B)=\varphi(g+h+(f))=g(\beta)+h(\beta),$$

правая часть

$$\varphi(A)+\varphi(B)=g(\beta)+h(\beta).$$

д) Устанавливается аналогично.

Теорема доказана.

Как установлено в доказательстве теоремы, наименьшее поле, содержащее P и некоторый элемент β, единственно. Оно называется *расширением поля P при помощи элемента β* и обозначается $P(\beta)$. Также из доказательства следует, что

$$P(\beta)=\{g(\beta)\mid g\in P[x]\}.$$

У п р а ж н е н и е. Возьмите в качестве поля P поле вещественных чисел $\mathbb{R}$, в качестве многочлена f многочлен x^2+1 и постройте наименьшее поле, в котором этот многочлен имеет корень.

22.4. *Задачи на решения уравнений 3-й и 4-й степени.*

1) (Ф.С. 167). Решить по формуле Кардано уравнения:

а) $x^3-6x+9=0$; b) $x^3+12x+63=0$;

c) $x^3+9x^2+18x+28=0$; d) $x^3+6x^2+30x+25=0$;
e) $x^3-6x+4=0$; f) $x^3+6x+2=0$.

2) (Ф.С. 172). Вывести формулу для алгебраического решения уравнения

$$x^5-5ax^3+5a^2x-2b=0.$$

3) (Ф.С. 173). Решить уравнения:
a) $x^4-2x^3+2x^2+4x-8=0$;
b) $x^4+2x^3-2x^2+6x-15=0$;
c) $x^4-x^3-x^2+2x-2=0$;
d) $x^4-4x^3+3x^2+2x-1=0$.

4) (Ф.С. 174). Способ Феррари для решения уравнения четвёртой степени $x^4+ax^3+bx^2+cx+d$ состоит в том, что левая часть представляется в виде

$$\left(x^2+\frac{a}{2}x+\frac{\lambda}{2}\right)^2-\left[\left(\frac{a^2}{4}+\lambda-b\right)x^2+\left(\frac{a\lambda}{2}-c\right)x+\left(\frac{\lambda^2}{4}-d\right)\right]$$

и затем λ подбирается так, чтобы выражение в квадратных скобках было квадратом двучлена первой степени. Для этого необходимо и достаточно, чтобы было

$$\left(\frac{a\lambda}{2}-c\right)^2-4\left(\frac{a^2}{4}+\lambda-b\right)\left(\frac{\lambda^2}{4}-d\right)=0,$$

т. е. λ должно быть корнем некоторого вспомогательного кубического уравнения. Найдя λ, раскладываем левую часть на множители.

Выразить корни вспомогательного уравнения через корни уравнения четвёртой степени.

5) (Ф.С. 175). Написать корни из единицы степени:
a) 2; b) 3; c) 4; d) 6; e) 8; f) 12; g) 24.

6) (Ф.С. 176). Выписать первообразные корни из единицы степени:
a) 2; b) 3; c) 4; d) 6; e) 8; f) 12; g) 24.

22.5. *Задачи на теорему Штурма.*
Составить ряд Штурма и отделить корни полиномов:

1) (Ф.С. 773). a) $x^3 - 3x - 1$; b) $x^3 + x^2 - 2x - 1$;
c) $x^3 - 7x + 7$; d) $x^3 - x + 5$; e) $x^3 + 3x - 5$.

2) (Ф.С. 775). a) $x^4 - 2x^3 - 4x^2 + 5x + 5$;
b) $x^4 - 2x^3 + x^2 - 2x + 1$;
c) $x^4 - 2x^3 - 3x^2 + 2x + 1$;
d) $x^4 - x^3 + x^2 - x - 1$;
e) $x^4 - 4x^3 - 4x^2 + 4x + 1$.

3) (Ф.С. 780). Пользуясь теоремой Штурма, определить число вещественных корней уравнения $x^3 + px + q = 0$ при вещественных p и q.

4) (Ф.С. *781). Определить число вещественных корней уравнения

$$x^n + px + q = 0.$$

5) (Ф.С. 782). Определить число вещественных корней уравнения

$$x^5 - 5ax^3 + 5a^2x - 2b = 0.$$

Это уравнение вы уже встречали в задаче (Ф.С. 172).

22.6. *Задачи для любознательных.*
1) (СМО, Задача 470) Доказать, что уравнение $x^5+ax^4+bx^3+c = 0$, где a, b, c — действительные числа и $c \neq 0$, имеет по крайней мере два комплексных, не действительных корня.
2) (СМО, Задача 473) Пусть $p(z)$ и $q(z)$ — многочлены ненулевой степени с комплексными коэффициентами. Доказать, что если для любого комплексного w многочлен $p(w) = 0$ тогда и только тогда, когда $q(w) = 0$, и $p(w) = 1$ тогда и только тогда, когда $q(w) = 1$, то многочлены $p(z)$ и $q(z)$ равны.
3) (СМО, Задача 484) Сколько существует многочленов вида $x^3 + ax^2 + bx + c = 0$ таких, что множество их корней есть $\{a, b, c\}$?
4) (ОК, 11-2) Сколько вещественных корней у многочлена

$$f(x) = nx^n - x^{n-1} - x^{n-2} - \ldots - 1?$$

5) (ОК, 15-1) Дан многочлен $f(x) = x^3 - ax - b$, где a и b — положительные числа. Доказать, что а) ровно один корень многочлена $f(x)$ является вещественным положительным числом; б) этот корень лежит в интервале $(max\{\sqrt{a}, \sqrt[3]{b}\}, \sqrt{a} + \sqrt[3]{b})$.