Глава 3

КОЛЬЦА МНОГОЧЛЕНОВ

§ 18. Многочлены от одной переменной

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

$$f = f(x) = a_0 + a_1x + \ldots + a_nx^n = \sum_{i=0}^{n} a_ix^i, \quad a_i \in K,$$

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:

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

$$\sum_{i=0}^{n} a_ix^i \cdot \sum_{j=0}^{m} b_jx^j = \sum_{k=0}^{n+m} c_kx^k, \quad \text{где} \quad c_k = \sum_{i+j=k} a_ib_j,$$

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 $K[x]$. Более того, справедлива

Теорема 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.

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 $f=\sum_{i=0}^{n}a_ix^i$ будет многочлен

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

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, 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
$$a = a_0 + a_1 x + \ldots + a_n x^n, a_n \neq 0,$$
$$b = b_0 + b_1 x + \ldots + b_m x^m, b_m \neq 0,$$
– 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.*

18.2. Деление с остатком. На множестве целых чисел существует операция деления с остатком, т. е., если m и $n \neq 0$ – два целых числа, то мы можем разделить m на n с остатком, т. е. представить m в виде
$$m = nq + r, \text{ где } r = 0 \text{ или } r < n,$$

для некоторых целых чисел q и 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

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

получим

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

Отсюда

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

Положим $(h_0 + h_1 + \ldots + h_{k-1}) = q, f_k = r$. Ясно, что r и q искомые и для них выполняются условия а) и б).

Докажем единственность. Пусть имеется 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.

18.3. 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 kd – тоже наибольший общий делитель для любого $k \in K^*$, т. е. наибольший общий делитель определяется неоднозначно. Символом (f, g) будем обозначать *приведенный 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) *Приведенный 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

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

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, 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 делит r_2 и т. д. Следовательно, d' делит r_k.

2) Пусть d_1 и d_2 – приведенные 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 остается 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	$\mathbb{Q}[x]$	$\mathbb{R}[x]$	$\mathbb{C}[x]$
$x^2 - 2$	$1, x^2 - 2$	$1, x^2 - 2, x \pm \sqrt{2}$	$1, x^2 - 2, x \pm \sqrt{2}$
$x^2 + 1$	$1, x^2 + 1$	$1, x^2 + 1$	$1, x^2 + 1, x \pm i$

С увеличением поля число делителей увеличивается.

§ 19. Линейное уравнение первой степени с двумя неизвестными

19.1. Критерий разрешимости. В кольце $P[x]$ рассмотрим уравнение

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

с неизвестными u, v. Следующая теорема дает 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 приведенный наибольший общий делитель (f, g) делит f и g, то (f, g) делит и правую часть предыдущего равенства. Следовательно, $(f, g)|h$.

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

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

Деля r_k на коэффициент при старшей степени, получим (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 $h \in I$, $t \in P[x]$, то произведения $h \cdot t \in I$, $t \cdot h \in I$.

Подмножество кольца, удовлетворяющее условиям 1) – 2) называется *идеалом.* 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, $r_1 \in I$, $r_2 \in I$, ..., $r_k \in I$. Приведенный 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.

19.2. Взаимно простые многочлены. Если $(f, g) = 1$, т. е приведенный 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. *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* $d \mid (fg)$ *и* $(d, f) = 1$, *то* $d \mid g$;

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

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

$$f \cdot (f u_1 u_2 + \psi u_1 v_2 + \varphi v_1 u_2) + \varphi\psi \cdot v_1 v_2 = 1,$$

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 предыдущее равенство, получим

$$d_1 d_2 \cdot u f_1 + d_1 d_2 \cdot v_2 = f.$$

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

19.3. 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: степень* u *меньше степени* g*, а степень* v *меньше степени* 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 наперед 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.

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

Учитывая, что $(f, g) = 1$ по теореме 2 в) 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 $\deg f > 0$, $\deg g > 0$. Пусть (u_0, v_0) – какое-нибудь решение уравнения (2). Поделим u_0 с остатком на g, а v_0 – на f, получим

$$u_0 = g \cdot u_1 + u_2, \quad \text{где } u_2 = 0, \text{ или } \deg u_2 < \deg g;$$

$$v_0 = f \cdot v_1 + v_2, \quad \text{где } v_2 = 0, \text{ или } \deg v_2 < \deg f.$$

Заметим, что остатки u_2 и v_2 ненулевые. Действительно, если $u_2 = 0$, то из равенства

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

заключаем, что

$$fg \cdot u_1 + g \cdot v_0 = 1,$$

но это равенство невозможно так как левая часть делится на многочлен g ненулевой степени, а правая – нет. Аналогично проверяется, что $v_2 \neq 0$.

Докажем, что пара (u_2, v_2) является решением уравнения (2). Имеем,

$$1 = f \cdot u_0 + g \cdot v_0 = f(gu_1 + u_2) + g(fv_1 + v_2) = fg(u_1 + v_1) + fu_2 + gv_2,$$

т. е.

$$fg(u_1 + v_1) = 1 - fu_2 - gv_2. \tag{4}$$

Хотим доказать, что $1 - fu_2 - gv_2 = 0$. Предположим, что обе части равенства (4) ненулевые. Тогда степень левой части равна

$$\deg f + \deg g + \deg(u_1 + v_1) \geq \deg f + \deg g,$$

а степень правой части меньше чем

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

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

$$1 - fu_2 - gv_2 = 0,$$

а потому

$$fu_2 + gv_2 = 1.$$

Заметим, что любое другое решение не годится, что следует из пункта 1). Теорема доказана.

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 $P[x]$?

§ 20. Корни и значения многочлена

20.1. Теорема Безу. До сих пор мы смотрели на многочлены как на чисто формальные выражения, которые можно складывать и умножать. Существует и другая точка зрения, рассматривающая многочлен $f(x) \in P[x]$ как функцию $f : P \longrightarrow P$. Если

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

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

$$f(c) = a_0 + a_1 c + \ldots + a_n c^n \in P.$$

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

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

Т е о р е м а (Безу). *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.

20.2. Формула Тейлора. Дадим вначале

О п р е д е л е н и е. Если

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

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

$$f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}.$$

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

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

Мы даем чисто 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

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

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.

20.3. Интерполяционная формула Лагранжа.

З а д а ч а   и н т е р п о л я ц и и. Пусть задано $n+1$ различных элементов $x_0, x_1, \ldots, x_n$ поля P и заданы $n+1$ 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

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

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

$$\begin{cases}
a_0 + a_1x_0 + \ldots + a_nx_0^n = y_0,\\
a_0 + a_1x_1 + \ldots + a_nx_1^n = y_1,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_0 + a_1x_n + \ldots + a_nx_n^n = y_n.
\end{cases}$$

Решая эту систему, найдем искомый многочлен. Существует готовая формула (*формула Лагранжа*), позволяющая сразу написать этот многочлен:

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

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

20.4. Кратные корни. Как следует из теорему 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* $f(x)$. Если $k = 1$, то говорят, что c – *простой корень.*

Т е о р е м а 2. *Над полем характеристики нуль k-кратный корень многочлена является $k-1$-кратным корнем 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.

§ 21. Кольца с однозначным разложением

21.1. 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 дается утвердительный ответ на этот вопрос.

Пусть K – *целостное кольцо*, т. е. коммутативное кольцо без делителей нуля. Предположим также, что K содержит единицу. Очевидно, что этим условиям удовлетворяет, в частности, кольцо целых чисел и кольцо многочленов над полем. Далее в этом параграфе будем считать, что K – целостное кольцо с единицей.

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 q_1, p_2 ассоциирован q_2 и т. д., и наконец, p_r ассоциирован 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.

21.2. 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 $h \in P[x]$, но так как p – неразложим, то либо $d \in P^*$, либо $h \in P^*$. Если $d \in P^*$, то $d = 1$, так как (p, f) – приведенный 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 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 имеем многочлены меньших степеней, а потому процесс оборвется. На каком-то 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 $p_1 \,|\, q_1 q_2 \dots q_s$. Покажем, что p_1 делит некоторый q_i. Действительно, по лемме 1 либо $p_1 \,|\, q_1$, либо $(p_1, q_1) = 1$. Если p_1 делит q_1, то это нас устраивает. Если $(p_1, q_1) = 1$, то $p_1 \,|\, q_2 \dots q_s$ (по теореме о взаимной простоте). Опять по лемме 1, либо $p_1 \,|\, q_2$, либо $p_1 \,|\, q_3 \dots q_s$ и т. д. Через несколько шагов получим, что $p_1 \,|\, q_i$ для некоторого i. Выполняя перенумерацию сомножителей, будем считать, что $p_1 \,|\, q_1$. 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. и, 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 $r(x + \sqrt{2})$, а $x - \sqrt{2}$ ассоциирован $r^{-1}(x - \sqrt{2})$.

21.3. 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 $\mathbb{R}$, порожденное 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, т. е. коммутативным кольцом без делителей нуля 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,

$$K = \bigcup_{i=1}^{\infty} K_i.$$

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. Именно,

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

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

Л е м м а 2. *Все элементы* $2^{\frac{1}{2^m}}$, $m = 0, 1, 2, \dots$ *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 некоторого $f(x)$ 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

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

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

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

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. Тогда 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

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

Таким образом, $\overline{g_1} = x^s$ и $\overline{g_2} = x^{2^r - s}$ для некоторого натурального s. Значит в g_1 и g_2 все коэффициенты кроме старших – четные. В частности, свободные члены многочленов g_i четные. 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 (в начале второго семестра).

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.

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

где $h(x) \in \mathbb{Z}[x]$. 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: $N : K \longrightarrow \mathbb{N} \cup \{0\}$, 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 найдется $\beta \in K$ такой, что $\alpha\beta = 1$. По свойству нормы из этого равенства получим $N(\alpha) \cdot N(\beta) = 1$. Следовательно, $N(\alpha) = N(\alpha^{-1}) = 1$, но это означает, что $a^2 + 3\,b^2 = 1$, а это равенство выполняется лишь при условии $a = \pm 1$, $b = 0$.

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

Покажем, что это разложение не единственно. 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 (заметьте, что $N(1 \pm \sqrt{-3}) = 4$).

§ 22. Идеалы. Фактор-кольца

22.1. Определения и примеры. С идеалом мы фактически уже встречались, когда доказывали критерий разрешимости линейного уравнения с двумя неизвестными. Введенное там множество I являлось идеалом. Дадим формальное определение.

О п р е д е л е н и е. Подмножество I кольца K называется *идеалом* (обозначение: $I \lhd K$), 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 $a \cdot c \in I$, $c \cdot a \in I$.

Из этого определения, в частности, следует, что идеал является подкольцом. С другой стороны, кольцо целых чисел является подкольцом поля рациональных чисел, но не является идеалом.

П р и м е р 1. Пусть $\mathbb{Z}$ – кольцо целых чисел. Тогда множество

$$n\mathbb{Z} = \{\text{целые числа, делящиеся на } n\}$$

является идеалом для любого целого неотрицательного n.

У п р а ж н е н и е. Докажите, что идеалы $n\mathbb{Z}$ исчерпывают все идеалы в $\mathbb{Z}$.

П р и м е р 2. Пусть $K = P[x]$, а f – некоторый многочлен из K. Тогда идеалом является множество всех многочленов, которые делятся на f, т. е.

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

Ниже мы покажем, что такими идеалами исчерпываются все идеалы кольца K.

У п р а ж н е н и е. *Во всяком поле P только два идеала: нулевой и само P.*

Р е ш е н и е. Действительно, пусть I – идеал в P и $I \neq 0$. Возьмем элемент $a \in I$, $a \neq 0$. Тогда $1 = a \cdot a^{-1} \in I$, но по определению идеала отсюда следует, что $1 \cdot b$ для любого элемента $b \in P$. Следовательно, $I = P$.

22.2. Порождающее множество идеала. Так же, как и в случае колец доказывается

Л е м м а 1. *Пересечение любого семейства идеалов является идеалом.*

Если M – некоторое подмножество кольца K, то символом ид(M) или просто (M) обозначим 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. Если множество M конечно, то говорят, что идеал I *конечно порожден.*

Более конструктивное описание идеала (M) дает

Л е м м а 2. *Пусть K – коммутативное кольцо с единицей и $M \subseteq K$. Тогда*

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

В частности, если $M = \{a_1, a_2, \ldots, a_n\}$, то

$$(a_1, a_2, \ldots, a_n) = \left\{ \sum_{i=1}^{n} a_i\, b_i \mid b_i \in K \right\}.$$

Д о к а з а т е л ь с т в о. Включение справа налево очевидно. Проверим, что множество сумм, стоящих в правой части действительно образуют идеал:

а) так как $\sum a_i\, b_i - \sum a_i\, b_i' = \sum a_i\,(b_i - b_i')$, то разность является такой же суммой;

б) так как $(\sum a_i\, b_i) \cdot c = \sum a_i\,(b_i c)$, то умножение на c переводит сумму в аналогичную сумму.

Таким образом, мы установили, что множество $\{\sum a_i\, b_i \mid a_i \in M, b_i \in K\}$ является наименьшим идеалом, содержащим M.

О п р е д е л е н и е. Идеал, порожденный одним элементом называется *главным.*

П р и м е р. Очевидно, $n\mathbb{Z} = (n)$, n – порождающий идеала $n\mathbb{Z}$. При этом

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}.$$

22.3. Фактор-кольца. Пусть K – кольцо, I – идеал в K и a, b – два элемента из K. Говорим, что *a сравним с b по модулю идеала I* и пишем: $a \equiv b \,(\mathrm{mod}\ I)$ или просто $a \equiv b$, если $a - b \in I$. Заметим, что отношение $\equiv$ является отношением эквивалентности. Действительно,

1) так как I – подкольцо, то $0 = a - a \in I$, т. е $a \equiv a$;

2) если $a - b \in I$, то и $-(a - b) = b - a \in I$, т. е. из того, что $a \equiv b$ следует, что $b \equiv a$;

3) если $a - b \in I$ и $b - c \in I$, то $(a - b) + (b - c) = a - c \in I$, т. е. из того, что $a \equiv b$ и $b \equiv c$ следует, что $a \equiv c$.

Заметим, что при доказательстве этих пунктов мы использовали лишь то, что I подкольцо.

Как мы знаем, множество с определенным на нем отношением эквивалентности разбивается на классы эквивалентности. Множество K распадается на смежные классы:

$$K/I = \{\text{смежные классы кольца } K \text{ по идеалу } I\}.$$

Легко видеть, что всякий смежный класс

$$K_a = \{x \in K \mid x \equiv a (\mathrm{mod}\ I)\}$$

имеет вид

$$K_a = a + I,$$

где мы обозначаем

$$a + I = \{a + i \mid i \in I\}.$$

На множестве всех смежных классов можно ввести операции сложения и умножения.

О п р е д е л е н и е. Для смежных классов $a + I$ и $b + I$ из K/I положим

$$(a + I) + (b + I) = a + b + I,$$

$$(a + I) \cdot (b + I) = a \cdot b + I.$$

Справедлива

Т е о р е м а 1. 1) *Сложение и умножение смежных классов не зависят от случайного выбора представителей в смежных классах.* 2) *Множество K/I с операциями сложения и умножения является кольцом.* Оно называется *фактор-кольцом кольца K по идеалу I.*

Д о к а з а т е л ь с т в о. 1) Пусть $a + I = a' + I$ и $b + I = b' + I$. Надо доказать, что

$$a + b + I = a' + b' + I,$$

$$a \cdot b + I = a' \cdot b' + I.$$

Иными словами, из того, что $a - a' \in I$ и $b - b' \in I$ надо доказать, что

$$(a + b) - (a' + b') \in I,$$

$$a \cdot b - a' \cdot b' \in I.$$

Так как сумма элементов из идеала лежит в идеале, то

$$(a - a') + (b - b') = (a + b) - (a' + b') \in I,$$

и первое включение установлено.

Рассмотрим далее

$$a \cdot b - a' \cdot b' = a \cdot b - a' \cdot b + a' \cdot b - a' \cdot b' = (a' - a) \cdot b + a' \cdot (b - b'),$$

ввиду того, что $(a' - a) \cdot b \in I$ и $a' \cdot (b - b') \in I$, заключаем, что и вся сумма в правой части лежит в идеале I. Заметим, что здесь мы использовали полное определение идеала.

2) Надо проверить аксиомы кольца. Они следуют из соответствующих аксиом для K. Например, аксиома ассоциативности сложения:

$$[(a + I) + (b + I)] + (c + I) = (a + I) + [(b + I) + (c + I)]$$

следует из равенства

$$(a + b) + c + I = a + (b + c) + I.$$

Аналогично проверяется коммутативность сложения, ассоциативность умножения, дистрибутивность.

Нулевым классов является класс $0 + I = I$.

Противоположным к классу $a+I$ будет класс $-(a+I) = -a+I$. Теорема доказана.

П р и м е р. Пусть $\mathbb{Z}$ – кольцо целых чисел, а $I = (5)$ – множество всех чисел кратных 5. Тогда $\mathbb{Z}/I \simeq \mathbb{Z}_5$ – кольцо вычетов по модулю 5.

22.4. Кольцо многочленов как кольцо главных идеалов. 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 2. *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 $I = (f)$.

Упражнение. Укажите в кольце $P[x, y]$ идеал, который не является главным.

Указание: рассмотрите идеал (x, y), состоящий из многочленов без свободного члена.

§ 23. Теорема о существовании корня

23.1. Постановка задачи. Сформулируем следующую задачу. Пусть P – поле, $f \in P[x]$. 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.

Теорема о существовании корня. *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 порожденное 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 разобьем на две части. Вначале покажем, что такое поле L действительно существует, а затем докажем единственность.

23.2. Существование. Рассмотрим фактор-кольцо $L' = P[x]/(f)$, где (f) – главный идеал, порожденный многочленом f. Проверим, что L' поле. Проверяем аксиомы поля.

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 $P[x]$ 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 $\omega : P \longrightarrow P'$ определяется следующим образом: $a \longmapsto a + (f)$, $a \in P$. Покажем, что ω – изоморфизм P на P', т. е.

1) ω – однозначно;

2) ω – унивалентно;

3) ω – отображение *на*;

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

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

1) То, что отображение ω однозначно – очевидно. 2) Если $a \neq b$, то надо показать, что $a + (f) \neq b + (f)$. Пусть $a + (f) = b + (f)$, тогда $a - b \in (f)$ и $f \mid (a - b)$, тогда $a - b = f \cdot g$ и, следовательно, $a - b = 0$ (учесть, что a и b – элементы из поля, а потому имеют нулевую степень), т. е $a = b$. 3) Очевидно. 4) Левая часть: $(a+b)\omega = a+b+(f)$; правая часть: $a\omega + b\omega = (a+(f)) + (b+(f)) = a+b+(f)$. 5) Проверяется аналогично. Таким образом, ω – изоморфизм.

Теперь возьмем $L = (L' \setminus P') \cup P$ с перенесенными 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). Возьмем $\alpha = x+(f)$ 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?

23.3. 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) найдется элемент $\beta \in M$ такой, что $f(\beta) = 0$;

3) подполе поля M, порожденное 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 $b_0 + b_1\,\beta + \ldots + a_n\,\beta^n$ лежит в M. Надо доказать, что других элементов там нет, т. е.

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

– подполе в M, порожденное P и β.

Заметим, что если $g_1, g_2 \in P[x]$, то и элементы $g_1(\beta) + g_2(\beta)$, $g_1(\beta) \cdot g_2(\beta)$, $-g_1(\beta)$ лежат в нашем множестве. 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

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

является полем, а так как оно содержит P и β, то оно содержит и M.

Докажем, что M и L' изоморфны. Рассмотрим отображение $\varphi : L' \longrightarrow M$, определенное 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:

1) φ – однозначно;

2) φ – унивалентно;

3) φ – отображение *на*;

4) $(A + B)\varphi = A\varphi + B\varphi$;

5) $(A \cdot B)\varphi = A\varphi \cdot B\varphi$.

1) 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 $g(\beta) = g_1(\beta)$.

2) 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 $f \mid (g-h)$, откуда $g+(f) = h+(f)$. Противоречие.

3) Следует из установленного равенства:

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

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

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

правая часть

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

5) устанавливается аналогично.

Теорема доказана.

Как установлено в доказательстве, 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.

§ 24. Идеалы в кольце многочленов

24.1. Кольца с условием максимальности.

Т е о р е м а 1. *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 растет:

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

Возьмем 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 $a_1 \in I_{n_1}$, $a_2 \in I_{n_2}$, ..., $a_m \in I_{n_m}$. 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 порожденный. Пусть $a_1 \in I$, тогда $(a_1) < I$. Пусть $a_2 \in I \setminus (a_1)$, тогда $(a_1, a_2) < I$. Пусть $a_3 \in I \setminus (a_1, a_2)$, тогда $(a_1, a_2, a_3) < I$, и так до бесконечности. Получаем цепочку идеалов

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

которая не стабилизируется. Противоречие. Теорема доказана.

24.2. 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

$$f_i(x_1, \ldots, x_n) = 0, \quad i \in A,$$

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

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

или, что равносильно, идеал, порожденный множеством $\{f_i \mid i \in A\}$ равен идеалу, порожденному $g_1, g_2, \ldots, g_s$?

Положительный ответ на этот вопрос следует из теоремы Гильберта.

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, найдется цепочка идеалов, которая не стабилизируется или, что равносильно, I – идеал в $K[x]$, который не конечно порожден. Выберем в I множество многочленов, полагая $f_0 = 0$, и для каждого $i = 0, 1, \ldots$ выберем многочлен f_{i+1} наименьшей степени, который не лежит в идеале $(f_0, f_1, \ldots, f_i)$, т. е. $f_{i+1} \in J \setminus (f_0, f_1, \ldots, f_i)$. Пусть n_i – степень многочлена f_i, а a_i – его старший коэффициент. Очевидно,

$$n_1 \leq n_2 \leq \ldots.$$

Достаточно доказать, что цепочка идеалов

$$(a_1) < (a_1, a_2) < \ldots < (a_1, a_2, \ldots, a_i) < (a_1, a_2, \ldots, a_i, a_{i+1}) < \ldots$$

не стабилизируется. Пусть напротив, $(a_1, a_2, \ldots, a_i) = (a_1, a_2, \ldots, a_i, a_{i+1})$ при некотором i, тогда

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

Рассмотрим

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

Ясно, что

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

Если бы $g \in (f_0, f_1, \ldots, f_i)$, то и $f_{i+1} \in (f_0, f_1, \ldots, f_i)$ и степень g была бы меньше степени f_{i+1}. Противоречие. Теорема доказана.

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 нулем, 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. *Если K – поле или кольцо $\mathbb{Z}$, то* $K[x_1, \ldots, x_n] \in \mathrm{Max}$.