§8. Многочлены и алгебраические числа.

8.1. Кольцо многочленов. Пусть K — произвольное коммутативное кольцо. Многочленом с коэффициентами из K от переменной x называется формальное бесконечное выражение вида $f(x) = a_0 + a_1x + a_2x^2 + \cdots$, в котором $a_i \in K$ и только конечное число из них отлично от нуля. Многочлены $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ и $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ равны, если $a_i = b_i\ \forall\ i$. Первый и последний ненулевые коэффициенты многочлена f называются, соответственно, его *старшим* и *младшим* коэффициентами. Номер старшего коэффициента называется *степенью* многочлена f и обозначается $\deg(f)$. Многочлен степени n обычно записывают в виде

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0\,.$$

Если старший коэффициент a_n равен единице, многочлен f называется *приведённым* или *унитарным*. Коэффициент a_0 называется *свободным членом* многочлена f. Многочлены степени ноль, состоящие из одного свободного члена, называются *константами*.

Сложение и умножение многочленов определяется по стандартным правилам раскрытия скобок и приведения подобных слагаемых. А именно, коэффициенты при x^m у суммы и произведения

$$\begin{aligned} s(x) &= f(x) + g(x) = s_0 + s_1x + s_2x^2 + \cdots \\ p(x) &= f(x)g(x) = p_0 + p_1x + p_2x^2 + \cdots \end{aligned} \tag{8-1}$$

многочленов $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ и $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ вычисляются по правилам[1]

$$\begin{aligned} s_m &= a_m + b_m\ , \\ p_m &= a_0b_m + a_1b_{m-1} + \cdots + a_{m-1}b_1 + a_mb_0 = \sum_{i+j=m} a_ib_j\ . \end{aligned} \tag{8-2}$$

Упражнение 8.1. Проверьте, что многочлены образуют коммутативное кольцо, нулевым элементом которого является нулевой многочлен (все коэффициенты которого равны нулю).

Кольцо многочленов с коэффициентами из K от переменной x обозначается $K[x]$. Кольцо K вкладывается в $K[x]$ в качестве подкольца констант. Если в K есть единица, то она же будет единицей кольца $K[x]$.

Отметим, что при вычислении старшего и младшего коэффициентов произведения сумма во второй формуле (8-2) будет состоять из единственного слагаемого, представляющего собою, соответственно, произведение старших коэффициентов и произведение младших коэффициентов многочленов-сомножителей. Поэтому если в кольце K нет делителей нуля, то кольцо $K[x]$ тоже будет целостным, и

$$\forall\ f, k \in K[x] \quad \deg(fg) = \deg(f) + \deg(g)\ .$$

Обратимыми элементами кольца многочленов являются обратимые константы и только они. В частности, если $K = \Bbbk$ является полем, то обратимыми элементы $\Bbbk[x]$ — это ненулевые константы. Отличный от обратимой константы многочлен $p \in K[x]$ называется *неприводимым*[2], если из равенства $p = fg$ вытекает, что один из сомножителей f, g является обратимой константой. Для многочлена над полем приводимость означает представимость в виде произведения двух многочленов строго меньшей степени.

8.1.1. Многочлены от многих переменных. Кольцо многочленов $K[x_1, x_2, \dots, x_n]$ от нескольких переменных определяется по индукции:

$$K[x_1, x_2, \dots, x_n] = K[x_1, x_2, \dots, x_{n-1}][x_n]$$

[1] формально говоря, эти правила задают операции на *множестве последовательностей* (a_n), (b_n); буква x служит лишь для упрощения интуитивной интерпретации формул (8-1)

[2] ср. с общим определением неприводимости из (n° 7.8)

и представляет собой множество формальных сумм вида

$$f(x_1, x_2, \ldots, x_n) = \sum_{\nu_1,\ldots,\nu_n \geqslant 0} a_{\nu_1\ldots\nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}\,,$$

где только конечное число коэффициентов $a_{\nu_1\ldots\nu_n}$ отлично от нуля. Отдельные слагаемые

$$a_{\nu_1\ldots\nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}$$

этой суммы называются *одночленами*, а произведения $x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}$ — *мономами*. Сумма степеней $\nu_1 + \nu_2 + \cdots + \nu_n$ называется *полной степенью монома*. Максимальная из полных степеней мономов, входящих в многочлен f с ненулевым коэффициентом, называется *полной степенью* f и обозначается $\deg(f)$.

8.2. Вычисление значения многочлена в точке. Значением многочлена

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

в точке $\alpha \in K$ называется число $f(\alpha) \stackrel{\text{def}}{=} a_0 + a_1\alpha + \cdots + a_n\alpha^n \in K$. Для его отыскания нет нужды отдельно вычислять все степени α^n, α^{n-1}, … Пользуясь дистрибутивностью, $f(\alpha)$ можно сосчитать за $2n$ операций сложения и умножения:

$$f(\alpha) = a_0 + \alpha \cdot \Big(a_1 + \alpha \cdot \Big(a_2 + \ \cdots\ + \alpha \cdot \big(a_{n-2} + \alpha \cdot (a_{n-1} + \alpha \cdot a_n)\big) \cdots \Big)\Big)\,. \tag{8-3}$$

8.3. Деление с остатком. Стандартная процедура «деления уголком» позволяет для любого многочлена $f(x)$ с коэффициентами в произвольном коммутативном кольце K с единицей и произвольного унитарного многочлена $u(x) = x^m + u_{m-1}x^{m-1} + \cdots + u_1 x + u_0 \in K[x]$ найти такие $q(x) \in K[x]$ (*неполное частное*) и $r(x) \in K[x]$ (*остаток*), что

$$f(x) = u(x) \cdot q(x) + r(x)\,, \quad \text{и} \quad \deg(r) < \deg(u) \quad \text{или} \quad r = 0\,. \tag{8-4}$$

Для этого полагаем $r_0 = f$, $q_0 = 0$ и далее для каждого $k = 1, 2, \ldots$ до тех пор, пока $\deg(r_{k-1}) \geqslant \deg(u)$ строим многочлены

$$q_k(x) = (\text{старший коэффициент } r_{k-1}) \cdot x^{\deg(r_{k-1}) - \deg(u)} \quad \text{и} \quad r_k = r_{k-1} - q_k u\,,$$

степень которых с каждым шагом строго уменьшается. Когда на каком-то ℓ-том шаге мы получим $\deg(r_\ell) < \deg(u)$, равенство (8-4) будет выполняться для $r = r_\ell$ и $q = q_1 + q_2 + \cdots + q_\ell$.

8.3.1. ПРЕДЛОЖЕНИЕ. *Для любого многочлена f и любого унитарного многочлена u над произвольным кольцом K с единицей существуют $q(x), r(x) \in K[x]$ со свойствами* (8-4). *Если кольцо K целостное, то такая пара многочленов единственна.*

Доказательство. Существование уже было установлено выше. Докажем, что над целостным кольцом коэффициентов многочлены r и q определяются условием (8-4) однозначно. Пусть p и s — другая пара многочленов, такая что $\deg(s) < \deg(u)$ и $f = up + s$. Из $uq + r = up + s$ вытекает, что $u(q-p) = r - s$. Поскольку в K нет делителей нуля, при $p \neq q$ будем иметь $\deg(u(q-p)) = \deg(u) + \deg(q-p) \geqslant \deg(u) > \deg(r-s)$, что противоречит равенству $u(q-p) = r - s$. Следовательно, $p - q = 0$, а значит, и $r - s = 0$. □

8.3.2. СЛЕДСТВИЕ. *Для любых многочленов f, g с коэффициентами в произвольном поле $\Bbbk$ существует единственная пара многочленов $q, r \in \Bbbk[x]$, таких что в кольце $\Bbbk[x]$ выполняется равенство $f = g \cdot q + r$ и $\deg(r) < \deg(g)$ или $r = 0$.*

Доказательство. Записывая g в виде $g = a \cdot u$, где $a \in \Bbbk$ — старший коэффициент многочлена g, а $u \in \Bbbk[x]$ унитарен, мы видим, что требуемое представление $f = g \cdot q + r$ равносильно представлению $f = u \cdot (aq) + r$ вида (8-4). □

8.3.3. Пример: значение в точке как остаток. Остаток от деления многочлена

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

на линейный двучлен $u(x) = x - \alpha$ — это константа, равная значению $f(\alpha)$ многочлена f в точке α, в чём легко убедиться, вычислив обе части равенства $f(x) = (x-\alpha)\cdot q(x) + r$ при $x = \alpha$. Поучительно, однако, увидеть это непосредственно, честно вычисляя остаток при помощи описанного выше алгоритма деления и сравнивая это вычисление с вычислением значения по формуле (8-3)

$$\begin{aligned} r_1(x) &= (a_{n-1} + \alpha a_n)x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \\ r_2(x) &= \big(a_{n-2} + \alpha(a_{n-1} + \alpha a_n)\big)x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_1x + a_0 \\ r_3(x) &= \Big(a_{n-3} + \alpha\big(a_{n-2} + \alpha(a_{n-1} + \alpha a_n)\big)\Big)x^{n-2} + a_{n-4}x^{n-4} + \cdots + a_1x + a_0 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ r_n(x) &= a_0 + \alpha\cdot\Bigg(a_1 + \alpha\cdot\Big(a_2 + \cdots + \alpha\cdot\big(a_{n-2} + \alpha\cdot(a_{n-1} + \alpha\cdot a_n)\big)\cdots\Big)\Bigg) = f(\alpha) \end{aligned} \tag{8-5}$$

Упражнение 8.2. Найдите остатки от деления многочлена $x^{179} + x^{57} + x^2 + 1$ в $\mathbb{Z}[x]$ на многочлены а) $x^2 - 1$ б) $x^2 + 1$ в) $x^2 + x + 1$.

Упражнение 8.3. Найдите частное от деления многочлена $y^n - x^n$ на $(y - x)$ в $\mathbb{Z}[x, y] = \mathbb{Z}[x][y]$ (ответ можно подглядеть в сноске ([1])).

8.3.4. Пример: разностный многочлен и производная. С каждым многочленом $f(x) \in K[x]$ можно связать многочлен от двух переменных

$$\Delta_f(t_1, t_2) \stackrel{\text{def}}{=} f(t_2) - f(t_1) \in K[t_1, t_2]\,,$$

называемый *разностным многочленом* многочлена f.

Упражнение 8.4. Проверьте, что $\forall\ f, g \in K[x]$ и $\forall\, a \in K$ выполняются равенства:

$$\begin{aligned} \Delta_{af} &= a\Delta_f \\ \Delta_{f+g} &= \Delta_f + \Delta_g \\ \Delta_{fg}(t_1,t_2) &= f(t_2)\Delta_g(t_1,t_2) + g(t_1)\Delta_f(t_1,t_2) = \\ &= g(t_2)\Delta_g(t_1,t_2) + f(t_1)\Delta_f(t_1,t_2) \end{aligned}$$

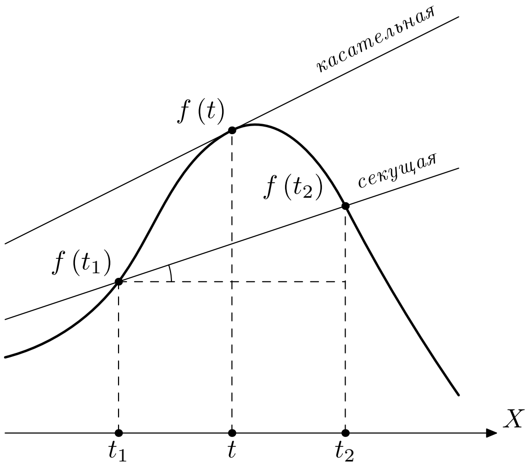

Рис. 8◇1. Касательная и секущая.

Разностный многочлен делится в кольце $K[t_1, t_2] = K[t_1][t_2]$ на разность $(t_2 - t_1)$ без остатка, ибо последний равен значению $\Delta_f(t_1, t_2)$ при $t_2 = t_1$, что есть нуль. Частное

$$D_f \stackrel{\text{def}}{=} \frac{f(t_2) - f(t_1)}{t_2 - t_1} \in K[t_1, t_2]$$

имеет простой геометрический смысл: отношение $\big(f(t_2) - f(t_1)\big)/(t_2 - t_1)$ над полем вещественных чисел $K = \mathbb{R}$ равно наклону проходящей через точки с абсциссами t_1 и t_2 секущей графика функции $y = f(x)$ (см. рис. 8◇1). Тем самым, наклон секущей к графику многочлена также является многочленом. Когда две точки пересечения секущей с графиком сливаются в одну точку с абсциссой t, секущая превращается в касательную, наклон которой будет равен значению многочлена $D_f(t_1, t_2)$ при $t_1 = t_2 = t$. Итак, наклон касательной, восстановленной к графику многочлена в точке с абсциссой x, тоже является многочленом. Этот многочлен обозначается

$$f'(x) \stackrel{\text{def}}{=} D_f(x, x) \in K[x] \tag{8-6}$$

и называется *производным многочленом* (или *производной*) от f. Подчеркнём, что формула (8-6) определяет производную для многочлена с коэффициентами в *любом кольце* K. Отображение

$$\frac{\partial}{\partial x} : K[x] \xrightarrow{f \mapsto f'} K[x]\,, \tag{8-7}$$

[1] ответ: $\dfrac{y^n - x^n}{y - x} = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \cdots + yx^{n-2} + x^{n-1}$ (что является одним из вариантов формулы для суммирования геометрической прогрессии)

сопоставляющее многочлену его производную, называется *дифференцированием по переменной* x.

Упражнение 8.5. Выведите из упр. 8.4, что $\forall\, f,g \in K[x]\,,\ \forall\, a \in K$ справедливы формулы:
а) $(af)' = a\cdot f'$ б) $(f+g)' = f' + g'$ в) (правило Лейбница) $(fg)' = f'\cdot g + f\cdot g'$

Согласно упр. 8.3, $D_{x^n}(t_1,t_2) = \frac{t_2^n - t_1^n}{t_2 - t_1} = t_2^{n-1} + t_2^{n-2}t_1 + t_2^{n-3}t_1^2 + \cdots + t_2 t_1^{n-2} + t_1^{n-1}$. Поэтому производная одночлена x^n равна $D_{x^n}(x,x) = nx^{n-1}$, а для произвольного $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1\ .$$

Обратите внимание, что коэффициент n в формуле $(x^n)' = nx^{n-1}$ — это *сумма* n *единиц кольца* K. В частности, если в качестве кольца коэффициентов взять конечное поле из p элементов

$$K = \mathbb{F}_p = \mathbb{Z}/(p)$$

(см. n° 7.9), то производная от любого одночлена вида x^{pk}, будет нулевым многочленом.

Упражнение 8.6. Покажите, что в кольце многочленов $\mathbb{F}_p[x]$ равенство $f'(x) = 0$ равносильно тому, что $f(x) = g(x^p)$ для некоторого $g \in \mathbb{F}_p[x]$.

8.3.5. Пример: НОД и алгоритм Евклида. В кольце $\Bbbk[x]$ многочленов с коэффициентами в произвольном поле $\Bbbk$ у любого набора элементов $f_1, f_2, \dots, f_n$ имеется наибольший общий делитель[1], причём его можно представить в виде

$$\text{нод}(f_1, f_2, \dots, f_n) = f_1 h_1 + f_2 h_2 + \cdots + f_n h_n \tag{8-8}$$

с подходящими $h_i \in \Bbbk[x]$. Доказывается это точно также, как и для целых чисел. А именно, обозначим через

$$(f_1, f_2, \dots, f_n) \overset{\text{def}}{=} \{ f_1 h_1 + f_2 h_2 + \cdots + f_n h_n \mid h_i \in \Bbbk[x] \} \tag{8-9}$$

множество всех многочленов, представимых в виде (8-8) с фиксированными $f_1, f_2, \dots, f_n$ и произвольными $h_1, h_2, \dots, h_n \in \Bbbk[x]$, и обозначим через $d(x) \in (f_1, f_2, \dots, f_n)$ любой ненулевой многочлен минимальной встречающейся в $(f_1, f_2, \dots, f_n)$ степени.

Упражнение 8.7. Покажите, что подмножество $(f_1, f_2, \dots, f_n) \subset \Bbbk[x]$ обладает следующими свойствами:
а) любой многочлен из $(f_1, f_2, \dots, f_n)$ делится на каждый общий делитель многочленов $f_1, f_2, \dots, f_n$
б) $f_1, f_2, \dots, f_n \in (f_1, f_2, \dots, f_n)$ в) $g_1, g_2 \in (f_1, f_2, \dots, f_n) \Rightarrow g_1 \pm g_2 \in (f_1, f_2, \dots, f_n)$
г) $g \in (f_1, f_2, \dots, f_n) \Rightarrow gh \in (f_1, f_2, \dots, f_n)\ \forall\, h \in \Bbbk[x]$
д) любой многочлен из $(f_1, f_2, \dots, f_n)$ делится на $d(x)$

Из последнего утверждения задачи вытекает, что, $(f_1, f_2, \dots, f_n) = (d)$ совпадает с множеством всех многочленов, кратных d. В частности $d = \text{нод}(f_1, f_2, \dots, f_n)$ и представляется в виде (8-8).

Отметим, что из этого вытекает, что отсутствие у пары многочленов $f, g \in \Bbbk[x]$ нетривиальных[2] общих делителей равносильна их *взаимной простоте*, т. е. возможности представления единицы кольца в виде $1 = fh_1 + gh_2$ с подходящими $h_1, h_2 \in \Bbbk[x]$.

Для практического отыскания наибольшего общего делителя и наименьшего общего кратного пары многочленов с коэффициентами в произвольном поле $\Bbbk$ применяется дословно тот же самый алгоритм Евклида, что и для целых чисел (ср. с n° 7.4). А именно, для пары многочленов $f_1(x)$ и $f_2(x)$ с $\deg(f_1) \geqslant \deg(f_2)$ положим $E_0 = f_1$, $E_1 = f_2$, и $E_k =$ остатку от деления E_{k-2} на E_{k-1} при $k \geqslant 1$. Степени многочленов E_k будут строго убывать до тех пор, пока какой-то E_r не разделит нацело предыдущий E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой многочлен E_r будет равен $\text{нод}(f_1, f_2)$, причём если при вычислении каждого E_k мы будем представлять его в виде $E_k = h_1^{(k)} f_1 + h_2^{(k)} f_2$, то $E_r = \text{нод}(f_1, f_2)$ и $E_{r+1} = 0$ тоже получатся представленными в таком виде. Отметим, что в выражении $E_{r+1} = 0 = h_1^{(r+1)} f_1 + h_2^{(r+1)} f_2$ многочлены $h_1^{(r+1)}$ и $h_2^{(r+1)}$ будут взаимно простыми множителями, дополняющими f_1 и f_2 до их наименьшего общего кратного $\text{нок}(f_1, f_2) = h_1^{(r+1)} f_1 = -h_2^{(r+1)} f_2$.

Упражнение 8.8. Докажите все эти утверждения.

Например, для $f_1 = x^7 + 3\,x^6 + 4\,x^5 + x^4 + 5\,x^2 + 3\,x^3 + 3\,x + 4\,,\ f_2 = x^5 + 5\,x^4 + 11\,x^3 + 12\,x^2 + 7\,x + 4$ первый шаг алгоритма Евклида приводит к

$$\begin{aligned}
E_0 &= x^7 + 3\,x^6 + 4\,x^5 + x^4 + 5\,x^2 + 3\,x^3 + 3\,x + 4\\
E_1 &= x^5 + 5\,x^4 + 11\,x^3 + 12\,x^2 + 7\,x + 4\\
E_2 &= -4\,x^4 - 13\,x^3 - 21\,x^2 - 10\,x - 8 = E_0 - \left(x^2 - 2\,x + 3\right) E_1
\end{aligned}$$

[1]напомним, что общий делитель называется *наибольшим*, если он делится на любой другой общий делитель
[2]т. е. отличных от констант и не кратных самим этим многочленам

дальше удобнее делить на E_2 не E_1, а $16E_1$, а затем умножить результат на 1/16:

$$E_3 = \frac{1}{16}\left(x^3+5\,x^2+10\,x+8\right) = \frac{1}{16}\left(16E_1+(4\,x+7)\;E_2\right) = \frac{4\,x+7}{16}\,E_0 - \frac{4\,x^3-x^2-2\,x+5}{16}\,E_1$$

следующий шаг уже даёт наибольший общий делитель

$$E_4 = -16\,(x^2+3\,x+4) = E_2 + 16\;(4\,x-7)\;E_3 = 16\left(x^2-3\right)\,E_0 - 16\left(x^4-2\,x^3+2\,x-2\right)\,E_1$$

поскольку

$$E_5 = E_3 + \frac{x+2}{256}\,E_4 = 0 = \frac{x^3+2\,x^2+x+1}{16}\,E_0 - \frac{x^5+x^2+1}{16}\,E_1\;.$$

Таким образом,

$$\begin{aligned}
\text{нод}(f_1,f_2) &= x^2+3\,x+4 = -\left(x^2-3\right)\,f_1(x) + \left(x^4-2\,x^3+2\,x-2\right)\,f_2(x)\\
\text{нок}(f_1,f_2) &= \left(x^3+2\,x^2+x+1\right)\,f_1(x) = \left(x^5+x^2+1\right)\,f_2(x)\;.
\end{aligned}$$

8.3.6. ПРЕДЛОЖЕНИЕ. *Всякий многочлен f с коэффициентами в произвольном поле $\Bbbk$ является произведением конечного числа неприводимых многочленов, причём любые два таких представления $p_1p_2\cdots p_k = f = q_1q_2\cdots q_m$ имеют одинаковое число сомножителей $k=m$, и эти сомножители можно перенумеровать так, чтобы $\forall\, i\;\; p_i = s_iq_i$, где $s_i\in\Bbbk$ — некоторые константы.*

Доказательство. Годятся дословно те же аргументы, что и для целых чисел (ср. с n° 7.8.1). Первое утверждение очевидно: если f неприводим, то он сам и будет своим разложением, если f приводим, то он является произведением многочленов строго меньшей степени, которые в свою очередь или неприводимы или являются произведениями многочленов строго меньшей степени и т. д. Поскольку степень не может бесконечно уменьшаться, мы в конце концов получим требуемое разложение. Для доказательства его единственности рассмотрим равенство

$$p_1p_2\cdots p_k = q_1q_2\cdots q_m\;, \tag{8-10}$$

в котором все сомножители неприводимы. Поскольку p_1 неприводим, он делится только на константы и на многочлены вида $s\cdot p_1$ с $s\in\Bbbk$. Если таких многочленов среди q_i нет, то $\forall\, i$ нод$(p_1,q_i)=1$, а значит p_1 взаимно прост с каждым из q_i, а следовательно, и с их произведением. Но равенство $h_1p_1+h_2q_1\cdots q_m=1$ невозможно, поскольку его левая часть в силу (8-10) делится на p_1. Итак, один из q_i — назовём его q_1 — имеет вид $q_1 = s_1p_1$ с $s_1\in\Bbbk$. Тогда (8-10) можно переписать в виде $p_1(p_2\cdots p_k + s_1\cdot q_2\cdots q_m)=0$, откуда следует более короткое равенство $p_2p_3\cdots p_k = (s_1q_2)q_3\cdots q_m$ (в котором s_1q_2 тоже неприводим), к которому применимо то же рассуждение. □

8.4. Корни многочленов. Элемент $\alpha\in K$, называется *корнем* многочлена $f\in K[x]$, если значение $f(\alpha)=0$ или , что равносильно, если $f(x)$ делится в $K[x]$ на $(x-\alpha)$.

8.4.1. ПРЕДЛОЖЕНИЕ. *Если в K нет делителей нуля, то всякий многочлен $f\in K[x]$, имеющий несколько попарно различных корней $\alpha_1,\alpha_2,\dots,\alpha_s\in K$, делится в $K[x]$ на произведение*

$$\prod_{i=1}^{s}(x-\alpha_i)\;.$$

В частности, если $f\neq 0$, то $\deg(f)\geqslant s$.

Доказательство. Запишем f в виде $f(x)=(x-\alpha_1)\cdot f_1(x)$. Поскольку в K нет делителей нуля и $(\alpha_i-\alpha_1)\neq 0$ при $i\neq 1$, вычисляя обе части при $x=\alpha_2,\alpha_3,\,\dots\,,\alpha_s$, мы заключаем, что $\alpha_2,\alpha_3,\,\dots\,,\alpha_s$ являются корнями многочлена $f_1(x)$, и можем применить к ним то же самое рассуждение. □

Упражнение 8.9. Пусть $\Bbbk$ — поле. Проверьте, что многочлен второй степени неприводим в $\Bbbk[x]$ тогда и только тогда, когда у него нет корней в поле $\Bbbk$

8.4.2. СЛЕДСТВИЕ. *Ненулевой многочлен f с коэффициентами из целостного кольца не может иметь в этом кольце более $\deg(f)$ различных корней.* □

8.4.3. СЛЕДСТВИЕ. *Пусть кольцо K целостное, и $f, g \in K[x]$ имеют степени, не превосходящие n. Если $f(\alpha_i) = g(\alpha_i)$ для более, чем n попарно разных $\alpha_i \in K$, то $f = g$ в $K[x]$.*

Доказательство. Многочлен $f - g$ нулевой, поскольку имеет степень $\leqslant n$ и больше, чем n корней. □

8.4.4. Пример: общие корни нескольких многочленов. Число α тогда и только тогда является общим корнем нескольких многочленов $f_1, f_2, \dots, f_m \in \Bbbk[x]$, где $\Bbbk$ — поле, когда α является корнем их наибольшего общего делителя. В самом деле, если $(x - \alpha)$ делит каждый из f_i, то $(x - \alpha)$ делит $\text{нод}(f_1, f_2, \dots, f_m)$, и наоборот. Таким образом, отыскание общих корней набора многочленов — это отыскание корней их наибольшего общего делителя, что часто бывает проще, чем отыскание корней любого из f_i в отдельности, т. к. $\deg \text{нод}(f_1, f_2, \dots, f_m)$ обычно бывает меньше $\min\big(\deg(f_i)\big)$.

В частности, если $\text{нод}(f_1, f_2, \dots, f_m) = 1$, то у многочленов f_i нет общих корней, причём не только в поле $\Bbbk$, над которым заданы эти многочлены, но и ни в каком большем кольце $K \supset \Bbbk$. Действительно, $f_i(\alpha)$ никак не могут одновременно обратиться в нуль, поскольку $\exists\, h_1, h_2, \dots, h_m \in \Bbbk[x]$, такие что

$$f_1h_1 + f_2h_2 + \dots + f_mh_m = \text{нод}(f_1, f_2, \dots, f_m) = 1$$

никогда не обращается в нуль.

8.4.5. Пример: кратные корни. Корень $\alpha \in K$ многочлена $f \in K[x]$ называется *кратным*, если $f(x)$ делится в $K[x]$ на $(x - \alpha)^2$. В этом случае $f(x) = (x - \alpha)^2 g(x)$ для некоторого $g \in K[x]$, и стало быть, $f'(x) = (x - a)\,(2g(x) - (x - \alpha)g'(x))$ делится на $(x - \alpha)$. Таким образом, все кратные корни многочлена f являются общими корнями f и f', а значит, являются корнями $\text{нод}(f, f')$.

Упражнение 8.10. Может ли неприводимый многочлен $f \in \mathbb{Q}[x]$ иметь кратный корень в поле $\mathbb{C}$?

8.5. Кольца вычетов $\Bbbk[x]/(f)$, где $\Bbbk$ — поле, определяются аналогично кольцам $\mathbb{Z}/(n)$. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$, обозначим через

$$(f) = \{fh \mid h \in \Bbbk[x]\}$$

множество всех многочленов, делящихся на f и рассмотрим смежные классы

$$[g]_f = g \,(\mathrm{mod}\ f) = g + (f) \stackrel{\text{def}}{=} \{g + fh \mid h \in \Bbbk[x]\}\,. \tag{8-11}$$

Два многочлена g_1 и g_2 лежат в одном и том же смежном классе $[g_1]_f = [g_2]_f$, если и только если разность $g_1 - g_2$ делится на f.

Упражнение 8.11. Убедитесь, что любые два смежных класса $[g_1]_f$, $[g_2]_f$ либо не пересекаются, либо совпадают.

Сложение и умножение смежных классов задаётся теми же самыми формулами (7-1), что и сложение целочисленных вычетов:

$$[g] + [h] \stackrel{\text{def}}{=} [g + h]\,, \quad [g] \cdot [h] \stackrel{\text{def}}{=} [gh]\,. \tag{8-12}$$

Упражнение 8.12. Проверьте корректность этого определения (т. е. независимость классов $[g+h]$ и $[gh]$ от выбора представителей $g \in [g]$ и $h \in [h]$), а также выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулевым элементом кольца $\Bbbk[x]/(f)$ является класс $[0]_f = (f)$, единицей является класс $[1]_f = 1 + (f)$. Поскольку никакая константа не может делиться на многочлен положительной степени, классы всех констант $c \in \Bbbk$ будут различны. Иначе говоря, поле $\Bbbk$ *вкладывается* в кольцо $\Bbbk[x]/(f)$ в качестве классов констант, и далее мы будем писать c вместо $[c]_f$ для $c \in \Bbbk$.

Поскольку любой многочлен $g \in \Bbbk[x]$ единственным образом записывается в виде $g = fh + r$, где $\deg(r) < \deg(f)$, в каждом классе $[g]_f$ имеется единственный представитель $r \in [g]_f$ степени $\deg(r) < \deg(f)$. Таким образом, каждый класс *единственным образом* записывается в виде

$$[a_0 + a_1x + \dots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}\,, \quad \text{где } \vartheta = [x]_f\,, \text{ а } a_i \in \Bbbk\,.$$

Заметим, что класс $\vartheta = [x]_f$ удовлетворяет в кольце $\Bbbk[x]/(f)$ уравнению $f(\vartheta) = 0$, т.к. $f(\vartheta) = f([x]_f) = [f(x)]_f = [0]_f$. Таким образом, сложение и умножение классов по правилам (8-12) можно интерпретировать как формальное сложение и умножение записей

$$a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1}, \tag{8-13}$$

по стандартным правилам раскрытия скобок и приведения подобных, но с учётом того, что символ ϑ удовлетворяет соотношению $f(\vartheta) = 0$. Поэтому кольцо $\Bbbk[x]/(f)$ иначе обозначают через $\Bbbk[\vartheta] : f(\vartheta) = 0$ и называют *расширением* поля $\Bbbk$ при помощи *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$. Выражения (8-13) в таком контексте называются (обобщёнными[1]) *алгебраическими числами*.

Например, кольцо $\mathbb{Q}[x]/(x^2-2)$ можно воспринимать как множество формальных записей вида $a + b\sqrt{2}$, где символ $\sqrt{2} \in \mathbb{Q}[x]/(x^2-2)$ обозначает класс $x \pmod{x^2-2}$. Сложение и умножение таких записей происходит по стандартным правилам раскрытия скобок с учётом того, что $\left(\sqrt{2}\right)^2 = 2$:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2\,bd) + (cb + ad)\sqrt{2}$$

Упражнение 8.13. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых ϑ удовлетворяет соотношению: а) $\vartheta^3 + 1 = 0$ б) $\vartheta^3 + 2 = 0$?

8.5.1. Пример: «алгебраическое» определение комплексных чисел. Поле комплексных чисел можно *определить* как расширение поля $\mathbb{R}$ при помощи корня квадратного уравнения $x^2 + 1 = 0$, т.е. как кольцо

$$\mathbb{R}[x]/(x^2+1) = \mathbb{R}\left[\sqrt{-1}\right] : \left(\sqrt{-1}\right)^2 = -1\,,$$

состоящее из чисел вида $a + b\sqrt{-1}$, где $a, b \in \mathbb{R}$, а символ $\sqrt{-1}$ обозначает класс одночлена x по модулю (x^2+1). Сложение и умножение таких чисел происходит по правилам

$$(a + b\sqrt{-1}) + (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1}$$
$$(a + b\sqrt{-1})(c + d\sqrt{-1}) = (ac - bd) + (cb + ad)\sqrt{-1}\,.$$

Кольцо $\mathbb{R}\left[\sqrt{-1}\right]$ является полем, поскольку каждый ненулевой класс $a + b\sqrt{-1}$ обладает обратным

$$\frac{1}{a + b\sqrt{-1}} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\sqrt{-1}\,.$$

Отображение $\mathbb{R}\left[\sqrt{-1}\right] \xrightarrow{\gamma} \mathbb{C}$ из этого поля в поле комплексных чисел $\mathbb{C}$, определённое в §6, сопоставляющее числу $a + b\sqrt{-1} \in \mathbb{R}\left[\sqrt{-1}\right]$ вектор $\gamma\left(a + b\sqrt{-1}\right) = a + bi \in \mathbb{C}$, является изоморфизмом полей.

8.5.2. ПРЕДЛОЖЕНИЕ. *Кольцо $\Bbbk[x]/(f)$ является полем тогда и только тогда, когда многочлен f неприводим в $\Bbbk[x]$.*

Доказательство. Если $f = gh$, где оба многочлена f, g имеют строго меньшую, чем f степень, то ненулевые классы $[g], [h]$ будут делителями нуля в $\Bbbk[x]/(f)$, что невозможно в поле. Если же f неприводим, то он будет взаимно прост с любым многочленом $g \notin (f)$, т.е. для некоторых $h, q \in \Bbbk[x]$ будет выполняться равенство $fh + gq = 1$, и стало быть $[q]\cdot[g] = [1]$ в $\Bbbk[x]/(f)$, т.е. любой ненулевой класс $[g]_f \in \Bbbk[x]/(f)$ будет обратим. □

Упражнение 8.14. Покажите, что поле $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Упражнение 8.15. Напишите явную формулу для вычисления обратного элемента

а) к числу $a_0 + a_1\vartheta$ в поле $\mathbb{Q}[\vartheta] : \vartheta^2 + \vartheta + 1 = 0$;

[1] *алгебраическим числом* в классическом смысле называется элемент поля $\mathbb{Q}[x]/(f)$, где $f \in \mathbb{Q}[x]$ — неприводимый многочлен (см. предложение (n° 8.5.2) ниже); наша обобщённая трактовка отличается от классической тем, что во-первых, вместо $\mathbb{Q}$ разрешается произвольное поле $\Bbbk$, а во-вторых, не требуется, чтобы соотношение на ϑ было неприводимо

б) к числу $a_0 + a_1\vartheta + a_2\vartheta^2$ в поле $\mathbb{Q}[\vartheta] : \vartheta^3 + \vartheta^2 + \vartheta + 1 = 0$.

8.5.3. Пример: китайская теорема об остатках. Если многочлен $f \in \Bbbk[x]$ является произведением m попарно взаимно простых сомножителей $f = f_1 f_2 \cdots f_m$, кольцо $\Bbbk[x]/(f)$ изоморфно прямому произведению колец вычетов $\Bbbk[x]/(f_i)$. Изоморфизм

$$\Bbbk[x]/(f) \xrightarrow{\varphi} (\Bbbk[x]/(f_1)) \times (\Bbbk[x]/(f_2)) \times \cdots \times (\Bbbk[x]/(f_m)) ,$$

как и в примере (n° 7.6.1), переводит класс $[g]_f \in \Bbbk[x]/(f)$ в набор классов

$$\varphi([g]_f) \stackrel{\text{def}}{=} ([g]_{f_1}, [g]_{f_2}, \dots, [g]_{f_m}) \qquad \forall g \in \Bbbk[x] .$$

Упражнение 8.16. Проверьте, что это правило корректно (не зависит от выбора представителя $g \in \Bbbk[x]$ в классе $[g]_f \subset \Bbbk[x]$) и является *гомоморфизмом* (т. е. переводит суммы и произведения, соответственно, в суммы и произведения).

Точно также, как в примере (n° 7.6.1), проверяется, что φ, рассматриваемый как гомоморфизм аддитивных групп, имеет нулевое ядро: если $\forall\ i\ [g]_{f_i} = 0$, то g делится на каждое f_i, а в силу их попарной взаимно просты — и на произведение $f_1 f_2 \cdots f_m = f$, откуда $[g]_f = 0$. Следовательно, по теореме о строении гомоморфизма групп, φ является вложением.

Сюрьективность φ устанавливается явным построением для заданного набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f)$ такого многочлена $g \in \Bbbk[x]$, что $g \equiv r_i \pmod{f_i}$ сразу для всех i. Как и в примере (n° 7.6.1), для каждого i обозначим через

$$F_i = \prod_{\nu \neq i} f_\nu$$

произведение всех сомножителей f_ν кроме f_i и построим многочлен

$$g_i = F_i \cdot h_i \equiv 1 \pmod{f_i} .$$

В качестве h_i в этой формуле можно взять любой многочлен[1], класс которого по модулю f_i обратен классу $F_i \pmod{f_i}$ (который взаимно прост с f_i и потому обратим). Тогда

$$\varphi(g_i) = \left([0]_{f_1}, \dots, [0]_{f_{i-1}}, [1]_{f_i}, [0]_{f_{i+1}}, \dots, [0]_{f_m}\right) ,$$

и в качестве многочлена g, отображающегося в заданные классы $[r_i]_{f_i}$ при всех i, можно взять $g = r_1 g_1 + r_2 g_2 + \cdots + r_m g_m$.

8.5.4. Пример: конечные поля $\mathbb{F}_p[\vartheta]$. Если взять в качестве $\Bbbk$ конечное поле $\mathbb{F}_p = \mathbb{Z}/(p)$ из p элементов, а в качестве $f \in \mathbb{F}_p[x]$ неприводимый многочлен степени n, то $\mathbb{F}_p[x]/(f)$ будет конечным полем, состоящим из p^n элементов вида $a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1}$ со всевозможными $a_i \in \mathbb{F}_p$. Например, $x^2 + x + 1 \in \mathbb{F}_2[x]$ неприводим согласно упр. 8.9, т. к. у него нет корней в $\mathbb{F}_2$. Поле $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1) = \mathbb{F}_2[\omega]$, где $\omega^2 + \omega + 1 = 0$ состоит из четырёх элементов: $0,\ 1,\ \omega = x \pmod{(x^2 + x + 1)}$ и $1 + \omega = \omega^2 = \omega^{-1}$ (обратите внимание, что в следствие равенства $-1 = 1$ в поле $\mathbb{F}_2$ можно обходиться без «минусов»).

Упражнение 8.17. Решите в поле $\mathbb{F}_4$ уравнение $x^2 + x + 1 = 0$.

Отметим, что мультипликативная группа $\mathbb{F}_4^*$ поля $\mathbb{F}_4$ изоморфна циклической группе $\boldsymbol{\mu}_3$.

Точно также, $x^2 + 1 \in \mathbb{F}_3[x]$ не имеет корней в $\mathbb{F}_3$, и значит, неприводим. Соответствующее поле $\mathbb{F}_9 = \mathbb{F}_3\left[\sqrt{-1}\right]$ состоит из девяти элементов $a + b\sqrt{-1}$ где $a, b \in \{-1, 0, 1\} = \mathbb{F}_3$.

Упражнение 8.18. Составьте для поля $\mathbb{F}_9$ таблицу умножения, таблицу обратных элементов, таблицу квадратов и таблицу кубов. Изоморфна ли мультипликативная группа $\mathbb{F}_9^*$ циклической группе $\mathbb{Z}/(8)$?

На самом деле, для каждого $n \in \mathbb{N}$ и любого простого $p \in \mathbb{N}$ существует единственное с точностью до изоморфизма поле $\mathbb{F}_q$, состоящее из $q = p^n$ элементов, и всякое конечное поле изоморфно одному из этих полей $\mathbb{F}_q$. Этот факт (а также неприводимые многочлены над полями $\mathbb{F}_p$) обсуждается в задачах из (необязательного) листка $6\frac{1}{2}$. Здесь же мы ограничимся всего одним результатом в этом направлении — покажем, что мультипликативная группа конечного поля, состоящего из q элементов является циклической группой порядка $q - 1$ (и тем самым, зависит только от q). Это следует из следующего более общего предложения.

---

[1] чтобы найти его явно, можно, например, взять остаток R_i от деления F_i на f_i и применить к паре $E_0 = f_i$, $E_1 = R_i$ алгоритм Евклида, что даст на выходе представление $1 = \text{нод}(F_i, f_i) = \text{нод}(R_i, f_i)$ в виде $1 = R_i h_i + f_i \tilde{h}_i$, из которого вытекает, что класс $[h_i]_{f_i} = [R_i]_{f_i}^{-1} = [F_i]_{f_i}^{-1}$ обладает нужным свойством

8.5.5. ПРЕДЛОЖЕНИЕ. *Любая конечная подгруппа в мультипликативной группе произвольного поля $\Bbbk$ является циклической.*

Доказательство. Пусть подгруппа $G \subset \Bbbk^*$ состоит из n элементов. Обозначим через m максимальный из порядков элементов группы G. Мы должны показать, что $m \geqslant n$. Для этого достаточно убедиться, что порядок любого элемента группы G является делителем числа m. В самом деле, если это верно, то все n элементов группы G будут корнями многочлена $x^m - 1 = 0$, откуда и следует нужное неравенство.

Чтобы доказать, что порядки всех элементов группы являются делителями максимального порядка, достаточно для любых двух элементов $b_1, b_2 \in G$, имеющих порядки m_1, m_2, построить элемент $b \in G$, порядок которого равен $\text{НОК}(m_1, m_2)$.

Упражнение 8.19. Покажите, что при $\text{НОД}(m_1, m_2) = 1$ в качестве такого элемента подойдёт $b = b_1 b_2$.

Если m_1 и m_2 не взаимно просты, то, раскладывая их в произведение простых чисел, мы можем представить $\text{НОК}(m_1, m_2)$ в виде произведения $\ell_1 \ell_2$ так, что[1] $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ и $\text{НОД}(\ell_1, \ell_2) = 1$. Тогда элементы $b_1' = b_1^{k_1}$ и $b_2' = b_2^{k_2}$ будут иметь взаимно простые порядки ℓ_1 и ℓ_2, а их произведение $b_1' b_2'$ по упр. 8.19 будет иметь порядок $\ell_1 \ell_2 = \text{НОК}(n_1, n_2)$. □

8.5.6. Пример: квадратичные вычеты. Зафиксируем целое простое $p > 2$. Ненулевые элементы поля $\mathbb{F}_p$, которые являются квадратами, называются *квадратичными вычетами* по модулю p. Иными словами, квадратичные вычеты составляют образ отображения возведения в квадрат $\mathbb{F}_p^* \xrightarrow{x \mapsto x^2} \mathbb{F}_p^*$. Поскольку это отображение является гомоморфизмом мультипликативных групп, и его ядро состоит из двух элементов[2] ± 1, квадратичных вычетов имеется ровно $(p-1)/2$ и они образуют в $\mathbb{F}_p^*$ мультипликативную подгруппу индекса 2.

Судить о том, является ли данный элемент $a \in \mathbb{F}_p^*$ квадратом или нет, можно при помощи малой теоремы Ферма. А именно, если $a = b^2$, то $a^{\frac{p-1}{2}} = b^{p-1} = 1$. Возведение в $\frac{p-1}{2}$-тую степень

$$\mathbb{F}_p^* \xrightarrow{x \mapsto x^{\frac{p-1}{2}}} \mathbb{F}_p^* \tag{8-14}$$

также является гомоморфизмом мультипликативных групп, причём его образ содержится среди корней всё того же уравнения $x^2 = 1$. Отметим, что -1 лежит в этом образе, поскольку $\mathbb{F}_p^*$ — это циклическая группа, и при $p > 2$ в ней есть элемент порядка $(p-1) > (p-1)/2$. Следовательно, ядро гомоморфизма (8-14) совпадает с подгруппой квадратичных вычетов, и $a \in \mathbb{F}_p^*$ является квадратом тогда и только тогда, когда $a^{\frac{p-1}{2}} = 1$ (для $p = 2$ это, формально, тоже так).

Например, -1 является квадратом в $\mathbb{F}_p$ в точности тогда, когда $(p-1)/2$ чётно.

Вместо того, чтобы вычислять $a^{\frac{p-1}{2}}$, можно воспользоваться следующим соображением, восходящим к Гауссу. Запишем элементы поля $\mathbb{F}_p$ в виде

$$-(p-1)/2\,,\ \dots\,,\ -1\,,\ 0\,,\ 1\,,\ \dots\,,\ (p-1)/2 \tag{8-15}$$

и умножим все «положительные» числа на a. Произведение всех полученных чисел будет отличаться от произведения всех «положительных» чисел в точности на множитель $a^{\frac{p-1}{2}}$. С другой стороны, каждое из произведений ac будет числом вида $\pm b$, где b «положительно», причём для каждого b ровно одно из чисел $\pm b$ будет представлено среди этих произведений, поскольку равенство $ab = \pm ac$ возможно только при $b = \pm c$. Таким образом, произведение всех чисел ac, где c «положительно», будет отличаться от произведения всех c знаком, равным $(-1)^s$, где s — количество «положительных» чисел, ставших после умножения на a «отрицательными». Таким образом, a является квадратичным вычетом тогда и только тогда, когда при умножении на a меняет знак чётное число «положительных» элементов записи (8-15).

Например, 2 является квадратичным вычетом по модулю p тогда и только тогда, когда $p \equiv \pm 1 \pmod 8$.

Упражнение 8.20. Покажите, что $a^{\frac{p-1}{2}}$ равно знаку перестановки элементов поля $\mathbb{F}_p$, происходящей при их умножении на a.

В задачах упражнений (дополнительный листок $5\frac{1}{2}$) доказывается *квадратичный закон взаимности* Гаусса, который позволяет выяснить, является ли заданное a квадратичным вычетом по модулю p, примерно за столько же действий, за сколько отыскивается $\text{НОД}(a, p)$.

[1] в ℓ_1 надо отправить все простые делители m_1, которые входят в m_1 в бо́льшей степени, чем в m_2, причём взять их нужно ровно с теми степенями, которые они имеют в m_1

[2] ибо уравнение $x^2 = 1$ имеет в любом целостном кольце с единицей ровно два корня