

§2. Многочлены и расширения полей

Всюду в этом параграфе мы обозначаем через K произвольное коммутативное кольцо с единицей, а через $\mathbb{k}$ — произвольное поле.

2.1. Ряды и многочлены. Бесконечное выражение вида

$$f(x) = \sum_{v \geq 0} a_v x^v = a_0 + a_1 x + a_2 x^2 + \dots, \text{ где } a_i \in K, \quad (2-1)$$

называется *формальным степенным рядом* от x с коэффициентами в кольце K . Ряды

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \dots \\ g(x) &= b_0 + b_1 x + b_2 x^2 + \dots \end{aligned} \quad (2-2)$$

равны, если $a_i = b_i$ для всех i . Сложение и умножение рядов (2-2) осуществляется по стандартным правилам раскрытия скобок и приведения подобных слагаемых: коэффициенты s_m и p_m рядов $s(x) = f(x) + g(x) = s_0 + s_1 x + s_2 x^2 + \dots$ и $p(x) = f(x)g(x) = p_0 + p_1 x + p_2 x^2 + \dots$ суть¹

$$\begin{aligned} s_m &= a_m + b_m \\ p_m &= \sum_{\alpha+\beta=m} a_\alpha b_\beta = a_0 b_m + a_1 b_{m-1} + \dots + a_{m-1} b_1 + a_m b_0 \end{aligned} \quad (2-3)$$

УПРАЖНЕНИЕ 2.1. Убедитесь, что эти две операции удовлетворяют аксиомам коммутативного кольца с единицей.

Кольцо формальных степенных рядов от переменной x с коэффициентами в кольце K обозначается через $K[[x]]$. Начальный коэффициент a_0 ряда (2-1) называется *свободным членом* этого ряда. Самый левый ненулевой коэффициент в (2-1) называется *младшим коэффициентом* ряда f , а его номер — *порядком* ряда f и обозначается $\text{ord } f$. Если в кольце K нет делителей нуля, младший коэффициент произведения двух рядов равен произведению младших коэффициентов сомножителей. Поэтому кольцо формальных степенных рядов с коэффициентами из целостного кольца тоже является целостным и $\text{ord}(fg) = \text{ord}(f) + \text{ord}(g)$.

Кольцо $K[[x_1, \dots, x_n]]$ формальных степенных рядов от n переменных определяется по индукции: $K[[x_1, \dots, x_n]] \stackrel{\text{def}}{=} K[[x_1, \dots, x_{n-1}]][[x_n]]$ представляет собою множество формальных сумм вида $F(x) = \sum_{v_1, \dots, v_n \in \mathbb{Z}_{\geq 0}} a_{v_1 \dots v_n} x_1^{v_1} \dots x_n^{v_n}$.

2.1.1. Алгебраические операции над рядами. Назовём *n -арной алгебраической операцией* в $K[[x]]$ правило, сопоставляющее n рядам $f_1, \dots, f_n$ новый ряд f так, что каждый коэффициент ряда f вычисляется по коэффициентам рядов $f_1, \dots, f_n$ при помощи конечного числа² операций в K . Например, сложение и умножение рядов — это бинарные алгебраические операции, а подстановка вместо x численного значения $\alpha \in K$ алгебраической операцией обычно не является¹.

¹Говоря формально, операции, о которых тут идёт речь, являются операциями над *последовательностями* (a_v) и (b_v) элементов кольца K . Буква x служит лишь для облегчения их восприятия.

²Которое может зависеть от номера коэффициента.

¹Очевидным исключением из этого правила служит вычисление значения ряда $f(x)$ при $x = 0$, дающее в качестве результата свободный член этого ряда. Однако при произвольных α и f вычисление $f(\alpha)$ требует, вообще говоря, выполнения бесконечно большого количества сложений.

ПРИМЕР 2.1 (ЗАМЕНА ПЕРЕМЕННОЙ)

Подстановка в ряд (2-1) вместо x любого ряда $g(x) = b_1x + b_2x^2 + \dots$ с нулевым свободным членом является бинарной алгебраической операцией, дающей на выходе ряд

$$\begin{aligned} f(g(x)) &= a_0 + a_1(b_1x + b_2x^2 + \dots) + a_2(b_1x + b_2x^2 + \dots)^2 + a_3(b_1x + b_2x^2 + \dots)^3 + \dots = \\ &= a_0 + (a_1b_1) \cdot x + (a_1b_2 + a_2b_1^2) \cdot x^2 + (a_1b_3 + 2a_2b_1b_2 + a_3b_1^3) \cdot x^3 + \dots, \end{aligned}$$

в котором на коэффициент при x^m влияют лишь начальные члены первых m слагаемых в f .

ПРИМЕР 2.2 (ОБРАЩЕНИЕ)

Покажем, что ряд $f(x) = a_0 + a_1x + a_2x^2 + \dots \in K[[x]]$ обратим в $K[[x]]$ если и только если его свободный член a_0 обратим в K , и в этом случае обращение $f \mapsto f^{-1}$ является унарной алгебраической операцией над обратимым рядом f . Пусть

$$(a_0 + a_1x + a_2x^2 + \dots) \cdot (b_0 + b_1x + b_2x^2 + \dots) = 1.$$

Приравнивая коэффициенты при одинаковых степенях x в левой и правой части, получаем бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \dots &\dots \dots \dots \end{aligned} \tag{2-4}$$

на коэффициенты b_i . Разрешимость первого уравнения равносильна обратимости a_0 , и в этом случае $b_0 = a_0^{-1}$ и $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \dots + a_kb_0)$ при всех $k \geq 1$.

УПРАЖНЕНИЕ 2.2. Вычислите в $\mathbb{Q}[[x]]$ а) $(1-x)^{-1}$ б) $(1-x^2)^{-1}$ в) $(1-x)^{-2}$.

2.1.2. Многочлены. Ряды с конечным числом ненулевых коэффициентов называются *многочленами*. Многочлены от $x_1, \dots, x_n$ с коэффициентами в K образуют в кольце степенных рядов подкольцо, которое обозначается $K[x_1, \dots, x_n] \subset K[[x_1, \dots, x_n]]$. Многочлен от одной переменной x представляет собою формальное выражение вида $f(x) = a_0 + a_1x + \dots + a_nx^n$. Самый правый ненулевой коэффициент в нём называется *старшим*, а его номер — *степенью* многочлена f и обозначается $\deg f$. Многочлены со старшим коэффициентом 1 называются *приведёнными*, а многочлены степени нуль — *константами*.

Так как старший коэффициент произведения равен произведению старших коэффициентов сомножителей, для многочленов f_1, f_2 с коэффициентами в целостном² кольце K выполняется равенство $\deg(f_1f_2) = \deg(f_1) + \deg(f_2)$. В частности, кольцо $K[x]$ тоже целостное, и обратимыми элементами в нём являются только обратимые константы.

УПРАЖНЕНИЕ 2.3. Покажите, что $y^n - x^n$ делится в $\mathbb{Z}[x, y]$ на $y - x$ и найдите частное.

2.1.3. Дифференциальное исчисление. Заменим в $f(x) = a_0 + a_1x + a_2x^2 + \dots$ переменную x на $x + t$, где t — ещё одна переменная. Получим ряд

$$f(x+t) = a_0 + a_1(x+t) + a_2(x+t)^2 + \dots \in K[[x, t]].$$

²Т. е. с единицей и без делителей нуля.

Раскроем в нём все скобки, затем сгруппируем слагаемые по степеням переменной t и обозначим через $f_m(x) \in K[[x]]$ ряд, возникающий как коэффициент при t^m :

$$f(x+t) = f_0(x) + f_1(x) \cdot t + f_2(x) \cdot t^2 + f_3(x) \cdot t^3 + \dots = \sum_{m \geq 0} f_m(x) \cdot t^m. \quad (2-5)$$

УПРАЖНЕНИЕ 2.4. Убедитесь, что $f_0(x) = f(x)$ совпадает с исходным рядом f .

Ряд $f_1(x)$ называется *производной* от исходного ряда f и обозначается f' или $\frac{d}{dx}f$. Он однозначно определяется равенством

$$f(x+t) = f(x) + f'(x) \cdot t + (\text{члены, делящиеся на } t^2)$$

и может быть вычислен при помощи [упр. 2.3](#) как результат подстановки $t = 0$ в ряд

$$\frac{f(x+t) - f(x)}{t} = \sum_{k \geq 1} a_k \frac{(x+t)^k - x^k}{t} = \sum_{k \geq 1} a_k ((x+t)^{k-1} + (x+t)^{k-2}x + \dots + x^{k-1}),$$

что даёт

$$f'(x) = \sum_{k \geq 1} k a_k x^{k-1} = a_1 + 2a_2x + 3a_3x^2 + \dots \quad (2-6)$$

ПРИМЕР 2.3 (ряды с нулевой производной)

Из формулы (2-6) вытекает, что производная от константы равна нулю. Если³ $\text{char } K = 0$, то верно и обратное: $f' = 0$ тогда и только тогда, когда $f = a_0$. Но если $\text{char } K = p > 0$, то производная от каждого монома вида x^{kp} занулится, поскольку коэффициент m при x^{m-1} в формуле (2-6) представляет собою сумму m единиц кольца K . Мы заключаем, над целостным кольцом K характеристики $p > 0$ равенство $f'(x) = 0$ означает, что $f(x) = g(x^p)$ для некоторого $g \in K[[x]]$.

УПРАЖНЕНИЕ 2.5. Покажите, что при простом $p \in \mathbb{N}$ для любого ряда $g \in \mathbb{F}_p[[x]]$ выполняется равенство $g(x^p) = g(x)^p$.

ПРЕДЛОЖЕНИЕ 2.1 (ПРАВИЛА ДИФФЕРЕНЦИРОВАНИЯ)

Для любого $\alpha \in K$ и любых $f, g \in K[[x]]$ справедливы равенства

$$(\alpha f)' = \alpha \cdot f', \quad (f+g)' = f' + g', \quad (fg)' = f' \cdot g + f \cdot g'. \quad (2-7)$$

Кроме того, если ряд g не имеет свободного члена, то

$$(f(g(x)))' = g'(x) \cdot f'(g(x)), \quad (2-8)$$

а если ряд f обратим, то

$$\frac{d}{dx}f^{-1} = -f' / f^2. \quad (2-9)$$

Доказательство. Первые два равенства в (2-7) вытекают прямо из формулы (2-6). Для доказательства третьего перемножим ряды

$$\begin{aligned} f(x+t) &= f(x) + t \cdot f'(x) + (\text{члены, делящиеся на } t^2) \\ g(x+t) &= g(x) + t \cdot g'(x) + (\text{члены, делящиеся на } t^2). \end{aligned}$$

³См. п.° 1.5.5 на стр. 31.

С точностью до членов, делящихся на t^2 , получим

$$f(x+t)g(x+t) = f(x)g(x) + t \cdot (f'(x)g(x) + f(x)g'(x)) + (\text{члены, делящиеся на } t^2),$$

откуда $(fg)' = f' \cdot g + f \cdot g'$. Формула (2-8) доказывается похожим образом: подставляя в $f(x)$ вместо x ряд $g(x+t)$, получаем $f(g(x+t)) = f(g(x) + t \cdot g'(x) + (\text{члены, делящиеся на } t^2))$. Полагая $\tau(x, t) \stackrel{\text{def}}{=} g(x+t) - g(x) = t \cdot g'(x) + (\text{члены, делящиеся на } t^2)$ и переписывая правую часть предыдущего ряда как

$$\begin{aligned} f(g(x+t)) &= f(g(x) + \tau(x, t)) = \\ &= f(g(x)) + \tau(x, t) \cdot f'(g(x)) + (\text{члены, делящиеся на } \tau(x, t)^2) = \\ &= f(g(x)) + t \cdot g'(x) \cdot f'(g(x)) + (\text{члены, делящиеся на } t^2), \end{aligned}$$

закключаем, что $(f(g(x)))' = g'(x) \cdot f'(g(x))$. Для доказательства формулы (2-9) достаточно продифференцировать обе части равенства $f \cdot f^{-1} = 1$. $\square$

УПРАЖНЕНИЕ 2.6. Покажите, что при $\text{char } \mathbb{k} = 0$ в разложении (2-5) каждый ряд $f_m(x)$ равен $\frac{1}{m!} \left(\frac{d}{dx}\right)^m f(x)$, где $\left(\frac{d}{dx}\right)^m$ означает m -кратное применение операции $\frac{d}{dx}$.

2.2. Делимость в кольце многочленов. Школьный алгоритм «деления уголком» работает для многочленов с коэффициентами в произвольном коммутативном кольце с единицей при условии, что многочлен-делитель имеет обратимый старший коэффициент.

Предложение 2.2 (деление с остатком)

Пусть K — произвольное коммутативное кольцо с единицей, и старший коэффициент многочлена $u \in K[x]$ обратим. Тогда для любого $f \in K[x]$ существуют такие $q, r \in K[x]$, что $f = uq + r$ и $\deg(r) < \deg(u)$ или $r = 0$. Если кольцо K целостное, то q и r однозначно определяются этими свойствами по f и u .

Доказательство. Пусть $f = a_n x^n + \dots + a_1 x + a_0$ и $u = b_k x^k + \dots + b_1 x + b_0$, где b_k обратим. Если $n < k$, можно взять $q = 0$ и $r = f$. Если $k = 0$, т.е. $u = b_0$, можно взять $r = 0$, $q = b_0^{-1} f$. Пусть $n \geq k > 0$ и предположение справедливо для всех многочленов f с $\deg f < n$. Тогда многочлен $f - a_n b_k^{-1} x^{n-k} u$ имеет степень, строго меньшую чем n , и по индукции представляется в виде $qu + r$, где $\deg r < \deg u$ или $r = 0$. Тем самым, $f = (q + a_n b_k^{-1} x^{n-k}) \cdot u + r$, как и утверждалось. Если кольцо K целостное и $p, s \in K[x]$ таковы, что $\deg(s) < \deg(u)$ и $up + s = f = uq + r$, то $u(q - p) = r - s$. При $p - q \neq 0$ степень левой части не менее $\deg u$, что строго больше степени правой. Поэтому, $p - q = 0$, откуда и $r - s = 0$. $\square$

Определение 2.1

Многочлены q и r , удовлетворяющие условиям предл. 2.2 называются *неполным частным* и *остатком* от деления f на u в $K[x]$.

Следствие 2.1

Для любых многочленов f, g с коэффициентами в любом поле $\mathbb{k}$ существует единственная такая пара многочленов $q, r \in \mathbb{k}[x]$, что $f = g \cdot q + r$ и $\deg(r) < \deg(g)$ или $r = 0$. $\square$

Пример 2.4 (вычисление значения многочлена в точке)

Остаток от деления многочлена $f(x) = a_n x^n + \dots + a_1 x + a_0$ на линейный двучлен $x - \alpha$ имеет степень нуль и равен значению $f(\alpha)$ многочлена f при $x = \alpha$, в чём легко убедиться, подставляя

$x = \alpha$ в равенство $f(x) = (x - \alpha) \cdot q(x) + r$. При «делении уголком» значение $f(\alpha)$ вычисляется в виде

$$f(\alpha) = \alpha \left(\dots \alpha (\alpha(a_n a_n + a_{n-1}) + a_{n-2}) + \dots \right) + a_0,$$

что гораздо эффективнее «лобовой подстановки» значения $x = \alpha$ в $a_n x^n + \dots + a_1 x + a_0$.

Предложение 2.3

Над произвольным полем $\mathbb{k}$ для любого набора многочленов $f_1, \dots, f_n \in \mathbb{k}[x]$ существует единственный приведённый многочлен $d \in \mathbb{k}[x]$, который делит каждый из многочленов f_i и делится на любой многочлен, делящий каждый из многочленов f_i . Он представляется в виде

$$d = f_1 h_1 + \dots + f_n h_n, \quad \text{где } h_i \in \mathbb{k}[x]. \quad (2-10)$$

Произвольный многочлен $g \in \mathbb{k}[x]$ представим в виде (2-10) если и только если $d|g$.

Доказательство. Единственность очевидна: два многочлена, каждый из которых делится на другой, имеют равные степени и могут различаться лишь постоянным множителем, который равен единице, коль скоро оба многочлена приведены. Существование доказывается тем же рассуждением, что и в п° 1.4.2 на стр. 27. Обозначим множество всех многочленов $g \in \mathbb{k}[x]$, представимых в виде (2-10), через $(f_1, \dots, f_n) \stackrel{\text{def}}{=} \{f_1 h_1 + \dots + f_n h_n \mid h_i \in \mathbb{k}[x]\}$. Это подкольцо в $\mathbb{k}[x]$, содержащее вместе с каждым многочленом g и все кратные ему многочлены hg с любым $h \in \mathbb{k}[x]$. Кроме того, $(f_1, \dots, f_n)$ содержит каждый из многочленов f_i , и все многочлены из $(f_1, \dots, f_n)$ делятся на любой общий делитель всех многочленов f_i . Возьмём в качестве d приведённый многочлен наименьшей степени в $(f_1, \dots, f_n)$. Для любого $g \in (f_1, \dots, f_n)$ остаток $r = g - qd$ от деления g на d лежит в $(f_1, \dots, f_n)$, и так как неравенство $\deg r < \deg d$ невозможно, мы заключаем, что $r = 0$, т. е. все $g \in (f_1, \dots, f_n)$ делятся на d . $\square$

Определение 2.2

Многочлен d из предл. 2.3 называется *наибольшим общим делителем*⁴ многочленов f_i и обозначается $\text{нод}(f_1, \dots, f_n)$.

2.2.1. Взаимная простота. Из предл. 2.3 вытекает, что для любого поля $\mathbb{k}$ взаимная простота¹ многочленов $f_1, \dots, f_m \in \mathbb{k}[x]$, т. е. наличие таких $h_1, \dots, h_m \in \mathbb{k}[x]$, что $h_1 f_1 + \dots + h_m f_m = 1$, равносильна отсутствию у многочленов $f_1, \dots, f_n$ общих делителей положительной степени — точно также, как это происходит в кольце целых чисел $\mathbb{Z}$.

Определение 2.3

Необратимый многочлен $f \in K[x]$ с коэффициентами в целостном¹ кольце K называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

Упражнение 2.7. Пусть $\mathbb{k}$ — любое поле. Пользуясь лем. 1.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\mathbb{k}[x]$: каждый многочлен f положительной степени является произведением конечного числа неприводимых многочленов, причём в любых двух таких представлениях $p_1 \dots p_k = f = q_1 \dots q_m$ одинаковое количество множителей $k = m$, и их можно перенумеровать так, чтобы $p_i = \lambda_i q_i$ при всех i для некоторых ненулевых констант $\lambda_i \in \mathbb{k}$.

⁴Ср. с зам. 1.3. на стр. 26.

¹См. опр. 1.2 на стр. 26.

¹Т. е. с единицей и без делителей нуля.

2.2.2. Алгоритм Евклида–Гаусса из п° 1.2.2 также применим к многочленам с коэффициентами из любого поля $\mathbb{K}$. Покажем, как он работает, вычислив $\text{НОД}(f, g)$ для

$$f = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x + 4 \text{ и } g = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4.$$

Как и в п° 1.2.2 на стр. 24, составляем таблицу

$$\begin{pmatrix} f & 1 & 0 \\ g & 0 & 1 \end{pmatrix} = \begin{pmatrix} x^7 + 3x^6 + 4x^5 + x^4 + 3x^3 + 5x^2 + 3x + 4 & 1 & 0 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix}.$$

и преобразуем её строки, умножая какую-нибудь из них на ненулевую константу и прибавляя к результату другую строку, умноженную на подходящий многочлен, так, чтобы степень одного из многочленов в левом столбце строго уменьшалась, пока один из них не обнулится:

$$\begin{aligned} (1) &\mapsto (1) - x^2(2): \begin{pmatrix} -2x^6 - 7x^5 - 11x^4 - 4x^3 + x^2 + 3x + 4 & 1 & -x^2 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\ (1) &\mapsto (1) + 2x(2): \begin{pmatrix} 3x^5 + 11x^4 + 20x^3 + 15x^2 + 11x + 4 & 1 & -x^2 + 2x \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\ (1) &\mapsto (1) - 3(2): \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\ (2) &\mapsto 4(2) + x(1): \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ 7x^4 + 23x^3 + 38x^2 + 20x + 16 & x & -x^3 + 2x^2 - 3x + 4 \end{pmatrix} \\ (2) &\mapsto 4(2) + 7(1): \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\ (1) &\mapsto (1) + 4x(2): \begin{pmatrix} 7x^3 + 19x^2 + 22x - 8 & 16x^2 + 28x + 1 & -16x^4 + 4x^3 + 7x^2 - 18x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\ (1) &\mapsto (1) - 7(2): \begin{pmatrix} -16x^2 - 48x - 64 & 16x^2 - 48 & -16x^4 + 32x^3 - 32x + 32 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\ (2) &\mapsto (2) + x(1)/16: \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 2x^2 + 6x + 8 & x^3 + x + 7 & -x^5 + 2x^4 - 4x^3 - x^2 + 4x - 5 \end{pmatrix} \\ (2) &\mapsto (2) - 2(1): \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 0 & x^3 + 2x^2 + x + 1 & -x^5 - x^2 - 1 \end{pmatrix} \end{aligned}$$

Полученный результат означает, что $\text{НОД}(f, g) = x^2 + 3x + 4 = -(x^2 - 3) \cdot f + (x^4 - 2x^3 + 2x - 2) \cdot g$, а $\text{НОК}(f, g) = (x^3 + 2x^2 + x + 1) \cdot f = (x^5 + x^2 + 1) \cdot g$.

УПРАЖНЕНИЕ 2.8. Убедитесь, что в каждой возникающей по ходу вычисления таблице

$$\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$$

выполняются равенства $p = rf + sg$, $q = uf + wg$, а многочлен $rw - us$ является ненулевой константой, и выведите из них, что в итоговой таблице вида

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & m_1 & m_2 \\ d' & h_1 & h_2 \end{pmatrix}$$

многочлен $d' = fh_1 + gh_2$ делит f и g , а многочлен $c' = fm_1 = -gm_2$ делит любое общее кратное f и g .

2.3. Корни многочленов. Число $\alpha \in K$ называется *корнем* многочлена $f \in K[x]$, если $f(\alpha) = 0$. Как мы видели в [прим. 2.4](#) на стр. 39, это равносильно тому, что $f(x)$ делится в $K[x]$ на $x - \alpha$.

УПРАЖНЕНИЕ 2.9. Пусть $\mathbb{k}$ — поле. Проверьте, что многочлен степени 2 или 3 неприводим в $\mathbb{k}[x]$ если и только если у него нет корней в поле $\mathbb{k}$.

Предложение 2.4

Пусть K — целостное кольцо и $f \in K[x]$ имеет s различных корней $\alpha_1, \dots, \alpha_s \in K$. Тогда f делится в $K[x]$ на произведение $\prod_i (x - \alpha_i)$. В частности, $\deg(f) \geq s$ или $f = 0$.

Доказательство. Так как в K нет делителей нуля и $(\alpha_i - \alpha_1) \neq 0$ при $i \neq 1$, подставляя в равенство $f(x) = (x - \alpha_1) \cdot q(x)$ значения $x = \alpha_2, \dots, \alpha_s$, убеждаемся, что они являются корнями многочлена $q(x)$, и применяем индукцию. $\square$

Следствие 2.2

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. Так как $\deg(f - g) \leq n$, и у $f - g$ больше n корней, $f - g = 0$. $\square$

Пример 2.5 (интерполяционный многочлен Лагранжа)

Пусть $\mathbb{k}$ — поле. По [сл. 2.2](#) для любых наборов из $n + 1$ различных чисел $a_0, a_1, \dots, a_n \in \mathbb{k}$ и произвольных значений $b_0, b_1, \dots, b_n \in \mathbb{k}$ имеется не более одного многочлена $f \in \mathbb{k}[x]$ степени $\leq n$ со значениями $f(a_i) = b_i$ при всех i . Единственный такой многочлен всегда существует и называется *интерполяционным многочленом Лагранжа*. Чтобы выписать его явно заметим, что произведение $\prod_{v \neq i} (x - a_v)$ зануляется во всех точках a_v кроме i -той, где его значение отлично от нуля. Деля на него, получаем многочлен $f_i(x) = \prod_{v \neq i} (x - a_v) / \prod_{v \neq i} (a_i - a_v)$ со значениями $f_i(a_v) = 0$ при $v \neq i$ и $f_i(a_i) = 1$. Искомый многочлен Лагранжа имеет вид

$$\sum_{i=0}^n b_i f_i(x) = \sum_{i=0}^n b_i \prod_{v \neq i} \frac{x - a_v}{a_i - a_v}.$$

2.3.1. Присоединение корней. Зафиксируем произвольный отличный от константы многочлен $f \in \mathbb{k}[x]$. Кольцо вычетов $\mathbb{k}[x]/(f)$ определяется аналогично кольцу¹ $\mathbb{Z}/(n)$. А именно, обозначим через $(f) = \{fh \mid h \in \mathbb{k}[x]\}$ подкольцо в $\mathbb{k}[x]$, состоящее из всех многочленов, делящихся на f . Сдвиги этого подкольца на всевозможные элементы $g \in \mathbb{k}[x]$ обозначаются

$$[g]_f = g + (f) = \{g + fh \mid h \in \mathbb{k}[x]\}$$

и называются *классами вычетов* по модулю f . Два таких класса $[g_1]_f$ и $[g_2]_f$ либо не пересекаются, либо совпадают, причём последнее означает, что $g_1 - g_2 \in (f)$.

УПРАЖНЕНИЕ 2.10. Убедитесь, что отношение $g_1 \equiv g_2 \pmod{f}$, означающее, что $g_1 - g_2 \in (f)$, является эквивалентностью².

Множество классов вычетов обозначается через $\mathbb{k}[x]/(f)$. Сложение и умножение в нём задаётся формулами $[g]_f + [h]_f \stackrel{\text{def}}{=} [g + h]_f$, $[g]_f \cdot [h]_f \stackrel{\text{def}}{=} [gh]_f$.

¹См. п. 1.4 на стр. 27.

²См. [опр. 0.1](#) на стр. 9.

УПРАЖНЕНИЕ 2.11. Проверьте корректность³ этого определения и выполнение в $\mathbb{K}[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулём кольца $\mathbb{K}[x]/(f)$ является класс $[0]_f = (f)$, единицей — класс $[1]_f = 1 + (f)$. Так как константы не делятся на многочлены положительной степени, классы всех констант $c \in \mathbb{K}$ различны по модулю f . Иначе говоря, поле $\mathbb{K}$ гомоморфно вкладывается в кольцо $\mathbb{K}[x]/(f)$ в качестве подполя, образованного классами констант. Поэтому классы чисел $c \in \mathbb{K}$ обычно записываются как c , а не $[c]_f$.

УПРАЖНЕНИЕ 2.12. Покажите, что для любого $\alpha \in \mathbb{K}$ кольцо $\mathbb{K}[x]/(x - \alpha)$ изоморфно полю $\mathbb{K}$. Каждый многочлен $g \in \mathbb{K}[x]$ однозначно представляется в виде $g = fh + r$, где $\deg r < \deg f$. Поэтому в каждом классе $[g]_f$ есть ровно один многочлен $r \in [g]_f$ с $\deg(r) < \deg(f)$. Таким образом, каждый элемент кольца $\mathbb{K}[x]/(f)$ однозначно записывается в виде

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

Класс $\vartheta = [x]_f$ удовлетворяет в кольце $\mathbb{K}[x]/(f)$ уравнению $f(\vartheta) = 0$, ибо

$$f(\vartheta) = f([x]_f) = [f(x)]_f = [0]_f.$$

В таких обозначениях сложение и умножение вычетов представляет собою формальное сложение и умножение записей $a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}$ по стандартным правилам раскрытия скобок и приведения подобных слагаемых с учётом соотношения $f(\vartheta) = 0$. По этой причине кольцо $\mathbb{K}[x]/(f)$ часто обозначают через $\mathbb{K}[\vartheta]$, где $f(\vartheta) = 0$, и называют *расширением* поля $\mathbb{K}$ путём *присоединения* к нему корня ϑ многочлена $f \in \mathbb{K}[x]$.

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

$$\begin{aligned} (a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \\ (a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2bd) + (cb + ad)\sqrt{2}. \end{aligned}$$

УПРАЖНЕНИЕ 2.13. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых а) $\vartheta^3 + 1 = 0$ б) $\vartheta^3 + 2 = 0$.

Предложение 2.5

Пусть $\mathbb{K}$ — произвольное поле и $f \in \mathbb{K}[x]$. Кольцо $\mathbb{K}[x]/(f)$ является полем если и только если f неприводим в $\mathbb{K}[x]$.

Доказательство. Если $f = gh$, где степени f и g строго меньше $\deg f$, ненулевые классы $[g]$, $[h]$ являются делителями нуля в кольце $\mathbb{K}[x]/(f)$, что невозможно в поле. Если f неприводим, то $\text{нод}(f, g) = 1$ для любого $g \notin (f)$, и значит, $fh + gq = 1$ для некоторых $h, q \in \mathbb{K}[x]$, откуда $[q] \cdot [g] = [1]$, т. е. класс $[g]$ обратим в $\mathbb{K}[x]/(f)$. $\square$

УПРАЖНЕНИЕ 2.14. Найдите $(1 + \vartheta)^{-1}$ в поле $\mathbb{Q}[\vartheta]$, где $\vartheta^2 + \vartheta + 1 = 0$.

³Т. е. независимость классов $[g + h]_f$ и $[gh]_f$ от выбора представителей $g \in [g]_f$ и $h \in [h]_f$.

ТЕОРЕМА 2.1

Для любого поля $\mathbb{k}$ и произвольного $f \in \mathbb{k}[x]$ существует такое поле $\mathbb{F} \supset \mathbb{k}$, что в кольце $\mathbb{F}[x]$ многочлен f разлагается в произведение $\deg f$ линейных множителей.

Доказательство. Индукция по $n = \deg f$. Пусть для любого поля $\mathbb{k}$ и каждого многочлена степени $< n$ из $\mathbb{k}[x]$ искомое поле имеется⁴. Рассмотрим многочлен f степени n . Если он приводим, т. е. $f = gh$ и $\deg g, \deg h < n$, то по индуктивному предположению существует поле $\mathbb{L} \supset \mathbb{k}$ над которым g полностью разлагается на линейные множители, а также поле $\mathbb{F} \supset \mathbb{L}$ над которым полностью разлагается h , а с ним и f . Если f неприводим, рассмотрим поле $\mathbb{L} = \mathbb{k}[x]/(f)$. Оно содержит $\mathbb{k}$ в качестве классов констант, и многочлен f делится в $\mathbb{L}[x]$ на $(x - \vartheta)$, где $\vartheta = [x]_f \in \mathbb{L}$. Частное от этого деления имеет степень $n - 1$ и по индукции раскладывается на линейные множители над некоторым полем $\mathbb{F} \supset \mathbb{L}$. Тем самым и f полностью раскладывается над $\mathbb{F}$. $\square$

ТЕОРЕМА 2.2 (КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ)

Пусть многочлен $f = f_1 \dots f_m \in \mathbb{k}[x]$ является произведением m попарно взаимно простых многочленов $f_i \in \mathbb{k}[x]$. Тогда отображение

$$\varphi: \frac{\mathbb{k}[x]}{(f)} \rightarrow \frac{\mathbb{k}[x]}{(f_1)} \times \dots \times \frac{\mathbb{k}[x]}{(f_m)}, \quad [g]_f \mapsto ([g]_{f_1}, \dots, [g]_{f_m}), \quad (2-11)$$

корректно определено и является изоморфизмом колец.

Доказательство. Проверка того, что отображение (2-11) корректно определено¹, является гомоморфизмом колец и имеет нулевое ядро, дословно та же, что в н° 1.7 на стр. 34, и мы оставляем её читателям. Докажем, что гомоморфизм (2-11) сюръективен. Для каждого i обозначим через $F_i = f / f_i$ произведение всех многочленов f_v кроме i -го. Так как f_i взаимно прост с каждым f_v при $v \neq i$, многочлены F_i и f_i взаимно просты по лем. 1.3 на стр. 26. Поэтому существует такой многочлен $h_i \in \mathbb{k}[x]$, что $[1]_{f_i} = [F_i]_{f_i} [h_i]_{f_i} = [F_i h_i]_{f_i}$ в $\mathbb{k}[x]/(f_i)$. Мы заключаем, что класс многочлена $F_i h_i$ нулевой во всех кольцах $\mathbb{k}[x]/(f_v)$ с $v \neq i$ и равен единице в $\mathbb{k}[x]/(f_i)$. Поэтому для любого набора классов $[r_i]_{f_i} \in \mathbb{k}[x]/(f_i)$ многочлен $g = \sum_i r_i F_i h_i$ таков, что $[g]_{f_i} = [r_i]_{f_i}$ сразу для всех i . $\square$

2.3.2. Общие корни нескольких многочленов $f_1, \dots, f_m \in \mathbb{k}[x]$ с коэффициентами в поле $\mathbb{k}$ искать обычно проще, чем корни каждого из многочленов f_i в отдельности, так как общие корни являются корнями многочлена $\text{нод}(f_1, \dots, f_m)$, который находится при помощи алгоритма Евклида и как правило имеет меньшую степень, чем любой из f_i . Отметим, что при $\text{нод}(f_1, \dots, f_m) = 1$ многочлены f_i не имеют общих корней не только в поле $\mathbb{k}$, но и ни в каком большем кольце $K \supset \mathbb{k}$, поскольку существуют такие $h_i \in \mathbb{k}[x]$, что $f_1 h_1 + \dots + f_m h_m = 1$.

2.3.3. Кратные корни. Пусть $\mathbb{k}$ — произвольное поле. Число $\alpha \in \mathbb{k}$ называется m -кратным корнем многочлена $f \in \mathbb{k}[x]$, если $f(x) = (x - \alpha)^m \cdot g(x)$ и $g(\alpha) \neq 0$. Корни кратности $m = 1$ называются *простыми*, а более высоких кратностей — *кратными*.

ПРЕДЛОЖЕНИЕ 2.6

Число α является кратным корнем многочлена f если и только если $f(\alpha) = f'(\alpha) = 0$.

⁴Заметим, что при $n = 2$ это так: достаточно взять $\mathbb{F} = \mathbb{k}$.

¹Т. е. $\varphi([g]_f) = \varphi([h]_f)$ при $[g]_f = [h]_f$.

Доказательство. Если корень α кратный, то $f(x) = (x - \alpha)^2 g(x)$. Дифференцируя, получаем

$$f'(x) = (x - \alpha)(2g(x) + (x - \alpha)g'(x)),$$

откуда $f'(\alpha) = 0$. Если корень α не кратный, то $f(x) = (x - \alpha)g(x)$, где $g(\alpha) \neq 0$. Подставляя $x = \alpha$ в $f'(x) = (x - \alpha)g'(x) + g(x)$, получаем $f'(\alpha) = g(\alpha) \neq 0$. $\square$

Предложение 2.7

Если $\text{char } \mathbb{k} = 0$, то $\alpha \in \mathbb{k}$ является m -кратным корнем многочлена $f \in \mathbb{k}[x]$ если и только если

$$f(\alpha) = \frac{d}{dx}f(\alpha) = \dots = \frac{d^{m-1}}{dx^{m-1}}f(\alpha) = 0 \quad \text{и} \quad \frac{d^m}{dx^m}f(\alpha) \neq 0.$$

Доказательство. Если $f(x) = (x - \alpha)^m g(x)$, то $f'(x) = (x - \alpha)^{m-1}(mg(x) + (x - \alpha)g'(x))$. При $g(\alpha) \neq 0$ второй множитель в последнем равенстве ненулевой при $x = \alpha$. Поэтому α является m -кратным корнем f если и только если α является $(m - 1)$ -кратным корнем f' . $\square$

2.3.4. Сепарабельность. Многочлен $f \in \mathbb{k}[x]$ называется *сепарабельным*, если он взаимно прост со своей производной. Это равносильно отсутствию у f кратных корней в любом кольце $K \supset \mathbb{k}$. В самом деле, если $\deg \text{нод}(f, f') \geq 1$ или $f' = 0$, то по [теор. 2.1](#) $\text{нод}(f, f')$ или, соответственно, сам f имеет корень в некотором поле $\mathbb{F} \supset \mathbb{k}$, и по [предл. 2.6](#) этот корень кратный для f . Наоборот, если $\text{нод}(f, f') = 1$, то $pf + qf' = 1$ для подходящих $p, q \in \mathbb{k}[x]$, и поэтому f и f' не могут одновременно обратиться в нуль ни в каком расширении $K \supset \mathbb{k}$.

Пример 2.6 (СЕПАРАБЕЛЬНОСТЬ И НЕСЕПАРАБЕЛЬНОСТЬ НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ)

Если многочлен $f \in \mathbb{k}[x]$ неприводим, то он взаимно прост со всеми ненулевыми многочленами меньшей степени. Поэтому $\text{нод}(f, f') = 1$, если $f' \neq 0$ в $\mathbb{k}[x]$. Поскольку над полем характеристики нуль каждый многочлен положительной степени имеет ненулевую производную, все неприводимые многочлены над таким полем сепарабельны. Если $\text{char } \mathbb{k} = p > 0$, то $f' = 0$ если и только если¹ $f(x) = g(x^p)$ для некоторого $g(x) = b_m x^m + \dots + b_1 x + b_0 \in \mathbb{k}[x]$. Так как в характеристике p возведение в p -тую степень является гомоморфизмом колец² и тождественно действует на простом поле $\mathbb{F}_p$, для любого многочлена g с коэффициентами в простом конечном поле $\mathbb{k} = \mathbb{F}_p$ выполняются равенства

$$\begin{aligned} g(x^p) &= b_m x^{pm} + \dots + b_1 x^p + b_0 = b_m^p x^{pm} + \dots + b_1^p x^p + b_0^p = \\ &= (b_m x^m + \dots + b_1 x + b_0)^p = g^p(x). \end{aligned}$$

Поэтому в $\mathbb{F}_p[x]$ каждый многочлен с нулевой производной является чистой p -той степенью и тем самым приводим. Мы заключаем, что в $\mathbb{F}_p[x]$ все неприводимые многочлены тоже сепарабельны.

УПРАЖНЕНИЕ 2.15*. Покажите, что неприводимый многочлен над любым конечным полем сепарабелен.

Неприводимый многочлен над бесконечным полем положительной характеристики не обязательно сепарабелен. Например, можно показать, что над полем $\mathbb{k} = \mathbb{F}_p(t)$ рациональных функций от одной переменной t с коэффициентами в поле $\mathbb{F}_p$ многочлен $f(x) = x^p - t$ неприводим, но поскольку $f' = 0$, многочлен f не сепарабелен.

¹См. [прим. 2.3](#) на стр. 38.

²См. [прим. 1.7](#) на стр. 28.

2.4. Поле комплексных чисел $\mathbb{C} \stackrel{\text{def}}{=} \mathbb{R}[t]/(t^2 + 1)$ получается из поля $\mathbb{R}$ присоединением корня неприводимого над $\mathbb{R}$ многочлена $t^2 + 1 = 0$ и состоит из элементов $x + iy$, где $x, y \in \mathbb{R}$, а $i \stackrel{\text{def}}{=} [t]$ удовлетворяет соотношению $i^2 = -1$. Обратным к ненулевому числу $x + yi$ является число

$$\frac{1}{x + yi} = \frac{x - iy}{(x + iy)(x - iy)} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2} \cdot i.$$

Комплексное число $z = x + yi$ удобно изображать на плоскости $\mathbb{R}^2$ с фиксированной прямоугольной системой координат (x, y) радиус вектором z , ведущим из начала координат в точку $z = (x, y)$, как на рис. 2♦1. Координаты (x, y) называются *действительной* и *мнимой* частями числа $z \in \mathbb{C}$ и обозначаются через $\text{Re}(z)$ и $\text{Im}(z)$, а длина $|z| \stackrel{\text{def}}{=} \sqrt{x^2 + y^2}$ называется *модулем* или *абсолютной величиной* комплексного числа z . Множество всех таких $\vartheta \in \mathbb{R}$, что поворот плоскости вокруг нуля на угол ϑ совмещает направление координатной оси x с направлением вектора z , называется *аргументом* числа z и обозначается $\text{Arg}(z) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}$, где $\alpha \in \mathbb{R}$ — ориентированная длина какой-нибудь дуги единичной окружности, ведущей из точки $(1, 0)$ в точку $z/|z|$. Таким образом, каждое комплексное число имеет вид $z = |z| \cdot (\cos \alpha + i \cdot \sin \alpha)$, где $\alpha \in \text{Arg}(z)$, и $\text{Re}(z) = |z| \cdot \cos \alpha$, $\text{Im}(z) = |z| \cdot \sin \alpha$.

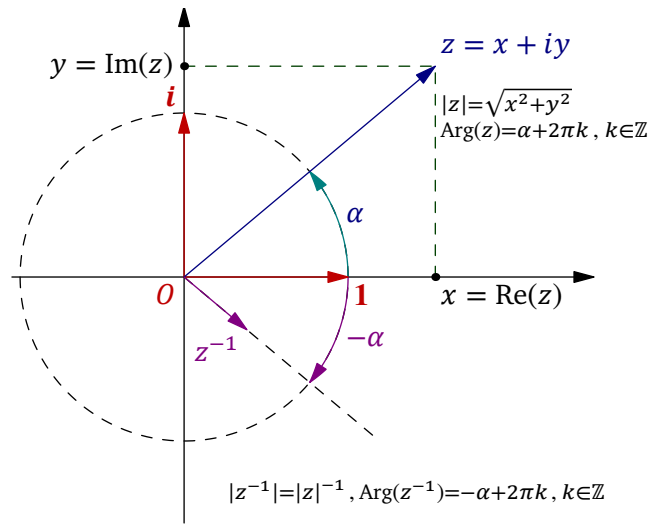


Рис. 2♦1. Числа $z = |z| \cdot (\cos \alpha + i \sin \alpha)$ и $z^{-1} = |z|^{-1}(\cos \alpha - i \sin \alpha)$.

На множестве векторов в $\mathbb{R}^2$ имеется своя внутренняя операция сложения векторов, относительно которой радиус векторы точек $z \in \mathbb{R}^2$ образуют абелеву группу. Зададим на множестве векторов в $\mathbb{R}^2$ операцию умножения требованием, чтобы длины перемножаемых векторов перемножались, а аргументы — складывались, т. е.

$$\begin{aligned} |z_1 z_2| &= |z_1| \cdot |z_2| \\ \text{Arg}(z_1 z_2) &= \text{Arg}(z_1) + \text{Arg}(z_2) \stackrel{\text{def}}{=} \{\vartheta_1 + \vartheta_2 \mid \vartheta_1 \in \text{Arg}(z_1), \vartheta_2 \in \text{Arg}(z_2)\}. \end{aligned} \quad (2-12)$$

УПРАЖНЕНИЕ 2.16. Проверьте корректность нижней формулы, т. е. убедитесь, что любые два числа в правом множестве отличаются на целое кратное 2π .

¹Любые две таких дуги отличаются друг от друга на целое число оборотов, а «ориентированность» означает, что длину дуги следует брать со знаком «+», если движение вдоль неё происходит против часовой стрелки, и со знаком «−» если по часовой стрелке.

Лемма 2.1

Множество радиус векторов точек z евклидовой координатной плоскости $\mathbb{R}^2$ с описанными выше сложением и умножением является полем. Отображение $\mathbb{C} \rightarrow \mathbb{R}^2$, сопоставляющее комплексному числу $x + iy \in \mathbb{C}$ точку $z = (x, y) \in \mathbb{R}^2$, является изоморфизмом полей.

Доказательство. Радиус векторы точек плоскости образуют абелеву группу по сложению. Очевидно также, что ненулевые векторы образуют абелеву группу относительно операции умножения, задаваемой формулами (2-12). Единицей этой группы служит единичный направляющий вектор оси x , а обратный к ненулевому z вектор z^{-1} имеет $|z^{-1}| = 1/|z|$ и $\text{Arg}(z^{-1}) = -\text{Arg}(z)$ (см. рис. 2◊1). Для проверки дистрибутивности заметим, что для любого $a \in \mathbb{R}^2$ отображение

$$a : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \quad z \mapsto az,$$

состоящее в умножении всех векторов на a по формулам (2-12), представляет собою *поворотную гомотетию*² плоскости $\mathbb{R}^2$ относительно начала координат на угол $\text{Arg}(a)$ с коэффициентом $|a|$. Аксиома дистрибутивности $a(b + c) = ab + ac$ утверждает, что поворотная гомотетия перестановочна со сложением векторов¹. Но это действительно так, поскольку и повороты и гомотетии переводят параллелограммы в параллелограммы. Таким образом, радиус векторы точек евклидовой координатной плоскости $\mathbb{R}^2$ образуют поле. Векторы, параллельные горизонтальной координатной оси, составляют в нём подполе, изоморфное полю $\mathbb{R}$. Если обозначить через i единичный направляющий вектор вертикальной координатной оси, то радиус вектор каждой точки $z = (x, y) \in \mathbb{R}^2$ однозначно запишется в виде $z = x + iy$, где числа $x, y \in \mathbb{R}$ понимаются как векторы, параллельные горизонтальной координатной оси, а сложение и умножение происходят по правилам поля $\mathbb{R}^2$. При этом $i^2 = -1$ и для любых векторов $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ выполняются равенства $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$ и

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1),$$

которыми описывается сложение и умножение вычетов $[x + yt]$ в поле $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$. $\square$

2.4.1. Комплексное сопряжение. Числа $z = x + iy$ и $\bar{z} \stackrel{\text{def}}{=} x - iy$ называются *комплексно сопряжёнными*. В терминах комплексного сопряжения обратное к ненулевому $z \in \mathbb{C}$ число можно записать как $z^{-1} = \bar{z}/|z|^2$. На геометрическом языке комплексное сопряжение $z \mapsto \bar{z}$ представляет собою симметрию комплексной плоскости относительно вещественной оси x . С алгебраической точки зрения сопряжение является инволютивным¹ автоморфизмом поля $\mathbb{C}$, т. е. $\bar{\bar{z}} = z$ для всех $z \in \mathbb{C}$, и $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$, $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$ для всех $z_1, z_2 \in \mathbb{C}$.

2.4.2. Тригонометрия. Почти вся школьная тригонометрия представляет собою трудно для восприятия закодированную запись заурядных алгебраических вычислений с комплексными числами, лежащими на единичной окружности.

Пример 2.7 (Формулы сложения аргументов)

Произведение $z_1 z_2$ чисел $z_1 = \cos \varphi_1 + i \sin \varphi_1$ и $z_2 = \cos \varphi_2 + i \sin \varphi_2$ согласно лем. 2.1 равно $\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)$, а лобовое перемножение этих чисел путём раскрытия скобок

²Поворотной гомотетией относительно точки 0 на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки 0 и растяжения в ϱ раз относительно 0. Так такие растяжения и повороты коммутируют друг с другом, неважно в каком порядке выполняется эта композиция.

¹Т. е. является гомоморфизмом аддитивных групп.

¹Эндоморфизм $\iota : X \rightarrow X$ произвольного множества X называется *инволюцией*, если $\iota \circ \iota = \text{Id}_X$. По предл. 0.4 на стр. 14 всякая инволюция автоматически биективна.

даёт $z_1 z_2 = (\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2) + i(\cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2)$, откуда $\cos(\varphi_1 + \varphi_2) = \cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2$ и $\sin(\varphi_1 + \varphi_2) = \cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2$. Таким образом мы доказали тригонометрические формулы сложения аргументов.

ПРИМЕР 2.8 (ТРИГОНОМЕТРИЧЕСКИЕ ФУНКЦИИ КРАТНЫХ УГЛОВ)

По лем. 2.1 число $z = \cos \varphi + i \sin \varphi \in \mathbb{C}$ имеет $z^n = \cos(n\varphi) + i \sin(n\varphi)$. Раскрывая скобки в биноме $(\cos \varphi + i \sin \varphi)^n$ по форм. (0-8) на стр. 7, получаем равенство

$$\begin{aligned} \cos(n\varphi) + i \sin(n\varphi) &= (\cos \varphi + i \sin \varphi)^n = \\ &= \cos^n \varphi + i \binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi - i \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \dots = \\ &= \left(\binom{n}{0} \cos^n \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi + \binom{n}{4} \cos^{n-4} \varphi \sin^4 \varphi - \dots \right) + \\ &\quad + i \cdot \left(\binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \binom{n}{5} \cos^{n-5} \varphi \sin^5 \varphi - \dots \right) \end{aligned}$$

закрывающее в себе сразу все мыслимые формулы для кратных углов:

$$\cos(n\varphi) = \binom{n}{0} \cos^n \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi + \binom{n}{4} \cos^{n-4} \varphi \sin^4 \varphi - \dots$$

$$\sin(n\varphi) = \binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \binom{n}{5} \cos^{n-5} \varphi \sin^5 \varphi - \dots$$

Например, $\cos 3\varphi = \cos^3 \varphi - 3 \cos \varphi \cdot \sin^2 \varphi = 4 \cos^3 \varphi - 3 \cos^2 \varphi$.

УПРАЖНЕНИЕ 2.17. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ через радикалы от рациональных чисел.

2.4.3. Корни из единицы и круговые многочлены. Решим в поле $\mathbb{C}$ уравнение $z^n = 1$. Сравнивая модули левой и правой части, заключаем, что $|z| = 1$. Сравнивая аргументы, получаем $n \operatorname{Arg}(z) = \operatorname{Arg}(1) = \{2\pi k \mid k \in \mathbb{Z}\}$. С точностью до прибавления целых кратных 2π существует ровно n различных вещественных чисел, попадающих при умножении на n в множество $\{2\pi k \mid k \in \mathbb{Z}\}$. Это все геометрически различные углы $2\pi k/n$ с $0 \leq k \leq n-1$. Мы заключаем, что уравнение $z^n = 1$ имеет ровно n корней

$$\zeta_k = \cos(2\pi k/n) + i \sin(2\pi k/n), \quad \text{где } k = 0, 1, \dots, (n-1), \quad (2-13)$$

расположенных в вершинах правильного n -угольника, вписанного в единичную окружность так, что его вершина ζ_0 находится в точке 1, см. рис. 2♦2 и рис. 2♦3.

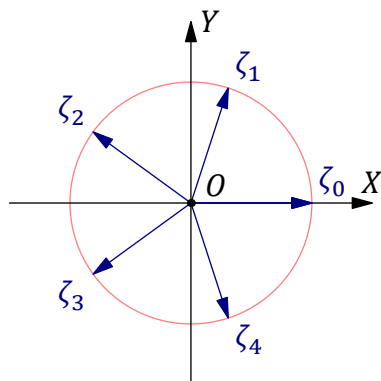


Рис. 2♦2. Группа μ_5 .

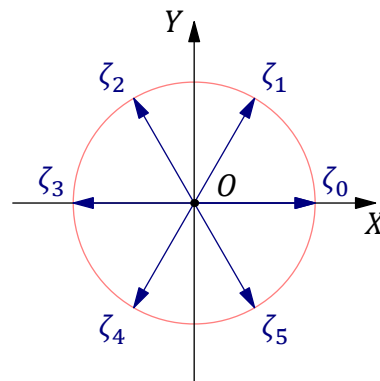


Рис. 2♦3. Группа μ_6 .

Корни (2-13) образуют абелеву группу относительно операции умножения. Эта группа обозначается μ_n и называется *группой корней n -й степени из единицы*. Корень $\zeta \in \mu_n$ называется *первообразным корнем степени n из единицы*, если все остальные элементы группы μ_n представляются в виде ζ^k с $k \in \mathbb{N}$. Например, первообразным является корень $\zeta_1 = \cos(2\pi/n) + i \sin(2\pi/n)$, имеющий наименьший положительный аргумент. Но бывают и другие: на рис. 2♦2 все четыре отличных от 1 элемента группы μ_5 являются первообразными корнями, тогда как в группе μ_6 на рис. 2♦3 первообразными являются только ζ_1 и $\zeta_5 = \zeta_1^{-1} = \zeta_1^5$. Множество всех первообразных корней обозначается через $R_n \subset \mu_n$.

УПРАЖНЕНИЕ 2.18. Покажите, что $\zeta_1^k = \cos(2\pi k/n) + i \sin(2\pi k/n) \in R_n$ если и только если $\text{нод}(k, n) = 1$.

Приведённый многочлен $\Phi_n(z) = \prod_{\zeta \in R_n} (z - \zeta)$, корнями которого являются все первообразные корни n -й степени из единицы и только они, называется *n -тым круговым или циклотомическим* многочленом. Например, пятый и шестой круговые многочлены имеют вид

$$\begin{aligned}\Phi_5(z) &= (z - \zeta_1)(z - \zeta_2)(z - \zeta_3)(z - \zeta_4) = z^4 + z^3 + z^2 + z + 1 \\ \Phi_6(z) &= (z - \zeta_1)(z - \zeta_5) = z^2 - z + 1.\end{aligned}$$

УПРАЖНЕНИЕ 2.19*. Попытайтесь доказать, что при всех $n \in \mathbb{N}$ многочлен Φ_n имеет целые коэффициенты и неприводим¹ в $\mathbb{Q}[x]$.

ПРИМЕР 2.9 (уравнение $z^n = a$)

Число $z = |z| \cdot (\cos \varphi + i \sin \varphi) \in \mathbb{C}$ является корнем уравнения $z^n = a$ если и только если $|z|^n = |a|$ и $n\varphi \in \text{Arg}(a)$. При $a \neq 0$ имеется ровно n таких чисел. Они выражаются через $r = |a|$ и $\alpha \in \text{Arg } a$ по формуле

$$z_k = \sqrt[n]{r} \cdot \left(\cos \frac{\alpha + 2\pi k}{n} + i \sin \frac{\alpha + 2\pi k}{n} \right), \quad 0 \leq k \leq n-1,$$

и располагаются в вершинах правильного n -угольника, вписанного в окружность радиуса $\sqrt[n]{r}$ с центром в нуле так, что радиус вектор одной из его вершин образует с осью x угол α/n .

2.5. Конечные поля можно строить присоединяя к $\mathbb{F}_p = \mathbb{Z}/(p)$ корень какого-нибудь неприводимого многочлена $f \in \mathbb{F}_p[x]$. Если $\deg f = n$, то получающееся таким образом поле вычетов $\mathbb{F}_p[x]/(f)$ состоит из p^n элементов вида $a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}$, где $a_i \in \mathbb{F}_p$ и $f(\vartheta) = 0$.

ПРИМЕР 2.10 (поле $\mathbb{F}_9$)

Многочлен $x^2 + 1 \in \mathbb{F}_3[x]$ неприводим, так как не имеет корней в $\mathbb{F}_3$. Присоединяя к $\mathbb{F}_3$ его корень, получаем поле $\mathbb{F}_9 \stackrel{\text{def}}{=} \mathbb{F}_3[x]/(x^2 + 1)$, состоящее из девяти элементов вида $a + bi$, где $a, b \in \mathbb{F}_3 = \{-1, 0, 1\}$ и $i^2 = -1$. Расширение $\mathbb{F}_3 \subset \mathbb{F}_9$ похоже на расширение $\mathbb{R} \subset \mathbb{C}$. Аналогом комплексного сопряжения в поле $\mathbb{F}_9$ является гомоморфизм Фробениуса² $F_3 : \mathbb{F}_9 \rightarrow \mathbb{F}_9, z \mapsto z^3$, тождественно действующий на простом подполе $\mathbb{F}_3 \subset \mathbb{F}_9$ и переводящий i в $-i$.

УПРАЖНЕНИЕ 2.20. Составьте для поля $\mathbb{F}_9$ таблицы умножения и обратных элементов, перечислите в $\mathbb{F}_9$ все квадраты и кубы и убедитесь, что мультипликативная группа $\mathbb{F}_9^\times$ изоморфна μ_8 .

¹Т. е. не являются произведениями многочленов строго меньшей степени.

²См. прим. 1.10 на стр. 32.

ПРИМЕР 2.11 (поле $\mathbb{F}_4$)

Многочлен $x^2 + x + 1 \in \mathbb{F}_2[x]$ неприводим, так как не имеет корней в $\mathbb{F}_2$. Присоединяя к $\mathbb{F}_2$ его корень, получаем поле $\mathbb{F}_4 \stackrel{\text{def}}{=} \mathbb{F}_2[x]/(x^2 + x + 1)$, состоящее из $0, 1, \omega = [x]$ и $1 + \omega = \omega^2 = \omega^{-1}$, причём¹ $\omega^2 + \omega + 1 = 0$. Расширение $\mathbb{F}_2 \subset \mathbb{F}_4$ тоже похоже на $\mathbb{R} \subset \mathbb{C}$, если понимать второе расширение как результат присоединения к $\mathbb{R}$ первообразного комплексного кубического корня ω из единицы, который также удовлетворяет уравнению $\omega^2 + \omega + 1 = 0$. В поле $\mathbb{F}_4$ аналогом комплексного сопряжения $\mathbb{C} \rightarrow \mathbb{C}$, переводящего $\omega \in \mathbb{C}$ в $\bar{\omega} = \omega^2$, также является гомоморфизм Фробениуса¹ $F_2 : \mathbb{F}_4 \rightarrow \mathbb{F}_4, z \mapsto z^2$, который тождественно действует на простом подполе $\mathbb{F}_2 \subset \mathbb{F}_4$ и переводит корни многочлена $x^2 + x + 1$ друг в друга.

УПРАЖНЕНИЕ 2.21. Убедитесь, что мультипликативная группа $\mathbb{F}_4^\times$ изоморфна μ_3 .

ТЕОРЕМА 2.3

Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ существует конечное поле $\mathbb{F}_q$ из $q = p^n$ элементов.

Доказательство. Рассмотрим в $\mathbb{F}_p[x]$ многочлен $f(x) = x^q - x$. По теор. 2.1 существует такое поле $\mathbb{F} \supset \mathbb{F}_p$, что f полностью раскладывается в $\mathbb{F}[x]$ в произведение q линейных множителей. Так как $f'(x) = -1$, многочлен f сепарабелен⁰, и все эти множители различны. Таким образом, в поле $\mathbb{F}$ имеется ровно q таких чисел α , что $\alpha^q = \alpha$. Обозначим множество этих чисел через $\mathbb{F}_q$ и покажем, что $\mathbb{F}_q \subset \mathbb{F}$ является подполем. Очевидно, что $0, 1 \in \mathbb{F}$ лежат в $\mathbb{F}_q$. Если $\alpha \in \mathbb{F}_q$, то $\alpha^{-1} \in \mathbb{F}_q$, так как $(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$, и $-\alpha \in \mathbb{F}_q$, так как $(-\alpha)^q = -\alpha^q = -\alpha$ при $p \neq 2$, а в характеристике два $-\alpha = \alpha$. Если $\alpha, \beta \in \mathbb{F}_q$, то $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, т.е. $\alpha\beta \in \mathbb{F}_q$. Поскольку $\text{char } \mathbb{F} = p$, в поле $\mathbb{F}$ выполняется равенство⁰ $(\alpha + \beta)^p = \alpha^p + \beta^p$. Применяя его n раз, заключаем, что $(\alpha + \beta)^q = (\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ для всех $\alpha, \beta \in \mathbb{F}_q$, откуда $\alpha + \beta \in \mathbb{F}_q$. $\square$

УПРАЖНЕНИЕ 2.22. Покажите, что число элементов в любом конечном поле является степенью его характеристики.

2.5.1. Конечные мультипликативные подгруппы поля. Рассмотрим абелеву группу A , операцию в которой будем записывать мультипликативно. Если группа A конечна, то среди степеней любого элемента $b \in A$ встречаются одинаковые, скажем $b^n = b^k$ с $n > k$. Умножая обе части этого равенства на b^{-k} , заключаем, что $b^{n-k} = 1$. Таким образом, для каждого $b \in A$ существует такое $m \in \mathbb{N}$, что $b^m = 1$. Наименьшее из этих m называется *порядком* элемента b и обозначается $\text{ord } b$. Если $\text{ord } b = n$, то элементы $b^0 = 1, b^1 = b, b^2, \dots, b^{n-1}$ попарно различны, и каждая целая степень b^k совпадает с одним из них: если $k = nq + r$, где r — остаток от деления k на n , то $b^k = (b^n)^q b^r = b^r$. В частности, $b^m = 0$ если и только если $m \vdots \text{ord } b$.

УПРАЖНЕНИЕ 2.23. Покажите, что порядок любого элемента из конечной абелевой группы A делит $|A|$.

Группа A называется *циклической*, если она исчерпывается целыми степенями какого-нибудь элемента $a \in A$, т.е. $A = \{a^n \mid n \in \mathbb{Z}\}$. Для конечной группы A это равносильно равенству $\text{ord } a = |A|$. Каждый обладающий этим свойством элемент $a \in A$ называется *образующей* циклической группы A . Например, группа $\mu_n \subset \mathbb{C}$ комплексных корней n -й степени из единицы⁰ циклическая, и её образующими являются первообразные корни.

¹ Отметим, что $-1 = 1$ в $\mathbb{F}_2$, что позволяет обходиться без минусов.

¹ См. прим. 1.10 на стр. 32.

⁰ См. п° 2.3.4 на стр. 45.

⁰ См. прим. 1.10 на стр. 32.

⁰ См. п° 2.4.3 на стр. 48.

ПРЕДЛОЖЕНИЕ 2.8

Если порядки элементов мультипликативной абелевой группы A ограничены сверху, то максимальный из них делится на порядок любого элемента $a \in A$.

Доказательство. Достаточно для любых двух элементов $a_1, a_2 \in A$, имеющих порядки m_1, m_2 , построить элемент $b \in A$, порядок которого равен $\text{но}(m_1, m_2)$. Если $\text{но}(m_1, m_2) = 1$, положим $b = a_1 a_2$. Тогда $b^{m_1 m_2} = a_1^{m_1} a_2^{m_2} = 1$. Если $b^k = 1$, то $a_1^k = a_2^{-k}$, откуда $1 = a_1^{km_1} = a_2^{-km_1}$, и значит, $km_1 \vdots m_2$. Так как m_1 и m_2 взаимно просты, $k \vdots m_2$. Меняя роли a_1 и a_2 , заключаем, что $k \vdots m_1$, а значит, $k \vdots m_1 m_2$. Тем самым, $\text{ord}(b) = m_1 m_2 = \text{но}(m_1, m_2)$.

Если $\text{но}(m_1, m_2) \neq 1$, то для каждого простого $p \in \mathbb{N}$ обозначим через $v_i(p)$ показатель, с которым p входит в разложение числа m_i на простые множители⁰. Тогда

$$\text{но}(m_1, m_2) = \prod_p p^{\max(v_1(p), v_2(p))}.$$

Положим $\ell_1 = \prod p^{v_1(p)}$ по всем простым $p \in \mathbb{N}$ с $v_1(p) > v_2(p)$, и $\ell_2 = \text{но}(m_1, m_2) / \ell_1$. Тогда $\text{но}(\ell_1, \ell_2) = 1$ и $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ для некоторых $k_1, k_2 \in \mathbb{N}$. Элементы $b_1 = a_1^{k_1}$, $b_2 = a_2^{k_2}$ имеют взаимно простые порядки ℓ_1, ℓ_2 , и по уже доказанному их произведение $b = b_1 b_2$ имеет порядок $\ell_1 \ell_2 = \text{но}(m_1, m_2)$. $\square$

СЛЕДСТВИЕ 2.3

Любая конечная подгруппа A в мультипликативной группе $\mathbb{K}^\times$ произвольного поля $\mathbb{K}$ является циклической.

Доказательство. Обозначим через m максимальный из порядков элементов группы A . Согласно [предл. 2.8](#), все элементы группы A являются корнями многочлена $x^m - 1 = 0$. Поэтому их не более m и все они исчерпываются степенями имеющегося в A элемента m -того порядка. $\square$

ТЕОРЕМА 2.4

Всякое конечное поле изоморфно одному из полей $\mathbb{F}_q$, построенных в [теор. 2.3](#) на стр. 50.

Доказательство. Пусть поле $\mathbb{F}$ имеет характеристику p и состоит из q элементов. По [сл. 2.3](#) мультипликативная группа $\mathbb{F}^\times$ является циклической. Обозначим её образующую через $\zeta \in \mathbb{F}^\times$. Тогда $\mathbb{F} = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2}\}$ и $\zeta^{q-1} = 1$. Чтобы доказать теорему, построим ещё одно поле из q элементов, изоморфное как полю $\mathbb{F}$, так и подходящему полю из [теор. 2.3](#). Для этого обозначим через $g \in \mathbb{F}_p[x]$ приведённый многочлен минимальной степени с корнем ζ .

УПРАЖНЕНИЕ 2.24. Убедитесь, что такой многочлен g существует, неприводим в $\mathbb{F}_p[x]$ и делит все многочлены $f \in \mathbb{F}_p[x]$ с корнем ζ .

Из упражнения вытекает, что кольцо $\mathbb{F}_p[x]/(g)$ является полем, а правило $[h]_g \mapsto h(\zeta)$ корректно задаёт ненулевой гомоморфизм колец $\mathbb{F}_p[x]/(g) \rightarrow \mathbb{F}$. Он инъективен по [предл. 1.3](#) на стр. 31 и сюръективен, так как все ζ^m содержатся в его образе. Тем самым, $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$. В частности, поле $\mathbb{F}$ состоит из $q = p^n$ элементов $a_{n-1}\zeta^{n-1} + \dots + a_1\zeta + a_0$, где $a_i \in \mathbb{F}_p$, $n = \deg g$.

Так как ζ является корнем многочлена $f(x) = x^q - x$, из [упр. 2.24](#) вытекает, что $f = gu$ для некоторого $u \in \mathbb{F}_p[x]$. Подставляя в это равенство q элементов поля $\mathbb{F}_q$, построенного в [теор. 2.3](#) и состоящего в точности из q корней многочлена f , мы заключаем, что хотя бы один

⁰См. [упр. 1.8](#) на стр. 26.

из них — назовём его $\xi \in \mathbb{F}_q$ — является корнем многочлена g . Правило $[h]_g \mapsto h(\xi)$ корректно задаёт вложение полей $\mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$, сюръективное, поскольку оба поля состоят из q элементов. Тем самым, $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$. $\square$

Следствие 2.4 (из доказательства [ТЕОР. 2.4](#))

Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ в $\mathbb{F}_p[x]$ имеется неприводимый многочлен степени n . $\square$

Следствие 2.5

Каждое конечное поле $\mathbb{F}$ состоит из p^n элементов, где простое $p = \text{char } \mathbb{F}$, и для каждого $n \in \mathbb{N}$ и простого p имеется единственное с точностью до изоморфизма поле из p^n элементов. $\square$

Ответы и указания к некоторым упражнениям

Упр. 2.3. Ответ: $(y^n - x^n)/(y - x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \dots + yx^{n-2} + x^{n-1}$.

Упр. 2.5. $(a_0 + a_1x + a_2x^2 + \dots)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \dots = a_0 + a_1x^p + a_2x^{2p} + \dots$ (первое равенство справедливо, поскольку возведение в p -тую степень перестановочно со сложением, второе — по малой теореме Ферма).

Упр. 2.6. Если $f(x) = \sum a_k x^k$, то $f(x+t) = \sum_{k,v} a_k \binom{k}{v} \cdot x^{k-v} t^v = \sum_v t^v \cdot f_v(x)$, где

$$f_v(x) = \sum_{k \geq v} a_k \binom{k}{v} \cdot x^{k-v} = \frac{1}{v!} \frac{d^k}{dx^k} \sum_{k \geq 0} a_k x^k.$$

Упр. 2.7. Годаются дословно те же аргументы, что и в [упр. 1.8](#).

Существование. Если f неприводим, то сам он и является своим разложением. Если f приводим, то он раскладывается в произведение 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, в конце концов получится требуемое разложение.

Единственность. Для неприводимого $p \in \mathbb{k}[x]$ и любого $g \in \mathbb{k}[x]$ имеется следующая альтернатива: либо $\text{нод}(p, g) = \lambda p$, где $\lambda \in \mathbb{k}^\times$ — ненулевая константа, и в этом случае g делится на p , либо $\text{нод}(p, g) = 1$, и тогда g взаимно прост с p . Пусть все сомножители в равенстве $p_1 \dots p_k = q_1 \dots q_m$ неприводимы. Поскольку $\prod q_i$ делится на p_1 , многочлен p_1 не может быть взаимно прост с каждым q_i в силу [лем. 1.3](#) на стр. 26. Поэтому найдётся q_i , делящийся на p_1 . После надлежащей перенумерации можно считать, что это q_1 . Так как q_1 неприводим, $q_1 = \lambda p_1$, где λ — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

Упр. 2.8. При умножении любой из строк таблицы $\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$ на ненулевую константу равенства $p = rf + sg$, $q = uf + wg$ сохраняются, а многочлен $rw - us$ умножается на эту константу. Если заменить любую строку таблицы на её сумму с другой строкой, умноженной на любой многочлен, равенства $p = rf + sg$, $q = uf + wg$ сохраняются, а многочлен $rw - us$ вообще не поменяется (ср. с [упр. 1.6](#) на стр. 25). Пусть в итоговой таблице

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix}$$

$h_1 m_2 - h_2 m_1 = \delta \in \mathbb{k}^\times$. Умножая это равенство на f и на g и пользуясь тем, что $d' = fh_1 + gh_2$, а $fm_1 = -gm_2$, получаем

$$\begin{aligned} \delta f &= fh_1 m_2 - fh_2 m_1 = fh_1 m_2 + gh_2 m_2 = d' m_2 \\ \delta g &= gh_1 m_2 - gh_2 m_1 = -fh_1 m_1 - gh_2 m_1 = -d' m_1. \end{aligned}$$

Поэтому $f = d' m_2 \delta^{-1}$ и $g = -d' m_1 \delta^{-1}$ делятся на d' . Для любого $q = fs = gt$ из равенства

$$\delta q = qh_1 m_2 - qh_2 m_1 = gth_1 m_2 - fsh_2 m_1 = -c'(th_1 + sh_2),$$

где $c' = fm_1 = -gm_2$, заключаем, что $q = -c'(th_1 + sh_2)\delta^{-1}$ делится на c' .

Упр. 2.9. Если многочлен степени ≤ 3 приводим, то у него есть делитель первой степени, корень которого будет корнем исходного многочлена.

Упр. 2.11. См. упр. 0.9 на стр. 10.

Упр. 2.12. Вложение $\varphi: \mathbb{K} \hookrightarrow \mathbb{K}[x]/(x-\alpha)$ в качестве констант сюръективно, поскольку число $\alpha \in \mathbb{K}$ переходит в класс $[x]$, и значит, для любого $g \in \mathbb{K}[x]$ число $g(\alpha)$ переходит в класс $[g]$.

Упр. 2.13. Обратным элементом к произвольному ненулевому $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ является $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Кольцо в (а) содержит делители нуля: $[t+1] \cdot [t^2-t+1] = [0]$ и, тем самым, не является полем. Кольцо в (б) является полем: многочлен $p = \vartheta^3 + 2$ не имеет корней в $\mathbb{Q}$, и значит, не делится в $\mathbb{Q}[x]$ ни на какой многочлен первой или второй степени; следовательно, p взаимно прост со всеми $g \in \mathbb{Q}[x]$, не делящимися на p , т. е. для любого $[g] \neq [0]$ существуют $h_1, h_2 \in \mathbb{Q}[x]$, такие что $h_1g + h_2p = 1$; тем самым, $[h_1] = [g]^{-1}$.

Упр. 2.14. Ответ: $(1 + \vartheta)^{-1} = -\vartheta$.

Упр. 2.15. Решение этой задачи опирается на теор. 2.3 на стр. 50 и теор. 2.4 на стр. 51. Обозначим через $\mathbb{F}_q$ конечное поле из q элементов⁰. Пусть $f \in \mathbb{F}_q[x]$ неприводим. Из доказательства теор. 2.1 на стр. 44 вытекает, что существует такое конечное поле $\mathbb{F}_r \supset \mathbb{F}_q$, что f полностью раскладывается на линейные множители в $\mathbb{F}_r[x]$. Так как поле $\mathbb{F}_r$ состоит из корней многочлена $g = x^r - x$, этот многочлен имеет общие корни с f , откуда $\text{нод}(f, g) \neq 1$ в $\mathbb{F}_q[x]$. Так как f неприводим, $g : f$ в $\mathbb{F}_q[x]$. А поскольку g сепарабелен, f тоже сепарабелен.

Упр. 2.17. Число $\zeta = \cos(2\pi/5) + i \cdot \sin(2\pi/5)$ является корнем многочлена

$$z^5 - 1 = (z - 1)(z^4 + z^3 + z^2 + z + 1).$$

Уравнение $z^4 + z^3 + z^2 + z + 1 = 0$ можно решить в радикалах, деля обе части на z^2 и вводя новую переменную $t = z + z^{-1}$.

Упр. 2.18. Пусть $\zeta = \cos(2\pi/n) + i \sin(2\pi/n)$ — первообразный корень с наименьшим положительным аргументом, и $\xi = \zeta^k$. Так как равенство $\zeta^m = \xi^x$ означает, что $m = kx + nu$ для некоторого $u \in \mathbb{Z}$, среди целых степеней корня ξ встречаются те и только те степени первообразного корня ζ , которые делятся на $\text{нод}(k, n)$.

Упр. 2.19. См. листок $2\frac{1}{2}$.

Упр. 2.22. Конечное поле $\mathbb{F}$ характеристики p является векторным пространством над своим простым подполем $\mathbb{F}_p \subset \mathbb{F}$, и в нём имеются такие векторы $v_1, \dots, v_m$, что любой вектор $w \in \mathbb{F}$ линейно выражается через них в виде $w = x_1v_1 + \dots + x_mv_m$, где все $x_i \in \mathbb{F}_p$. Удаляя из набора $v_1, \dots, v_m$ все векторы, которые линейно выражаются через оставшиеся, мы получим такой набор векторов $\{e_1, \dots, e_n\} \subset \{v_1, \dots, v_m\}$, через который каждый вектор $w \in \mathbb{F}$ выражается единственным способом, так как равенство $x_1e_1 + \dots + x_ne_n = y_1e_1 + \dots + y_ne_n$, в котором $x_i \neq y_i$ для какого-нибудь i , позволяет выразить e_i через остальные векторы как $e_i = \sum_{v \neq i} e_v(y_v - x_v)/(x_i - y_i)$, что невозможно. Коль скоро каждый элемент поля $\mathbb{F}$ однозначно записывается в виде $x_1e_1 + \dots + x_ne_n$, где каждый коэффициент x_i независимо принимает p значений, мы заключаем, что $|\mathbb{F}| = p^n$.

Упр. 2.23. См. доказательство теоремы Эйлера из прим. 1.6 на стр. 28.

⁰Согласно теор. 2.3 и теор. 2.4 такое поле единственно с точностью до изоморфизма и состоит из корней многочлена $x^q - x$ в таком расширении простого подполя поля $\mathbb{F}_q$, над которым этот многочлен полностью раскладывается на линейные множители.

Упр. 2.24. Отображение $\text{ev}_\zeta : \mathbb{F}_p[x] \rightarrow \mathbb{F}, f \mapsto f(\zeta)$, является гомоморфизмом колец. Поскольку поле $\mathbb{F}$ конечно, а кольцо многочленов $\mathbb{F}_p[x]$ бесконечно, у этого гомоморфизма ненулевое ядро. Многочлен g — это приведённый многочлен минимальной степени в $\ker \text{ev}_\zeta$. Если $g(x) = h_1(x)h_2(x)$, то $h_1(\zeta) = 0$ или $h_2(\zeta) = 0$, что по выбору g невозможно при $\deg h_1, \deg h_2 < \deg g$. Пусть $f(\zeta) = 0$ для $f = gh + r$, где $\deg r < \deg g$ или $r = 0$. Подставляя $x = \zeta$, получаем $r(\zeta) = 0$, откуда $r = 0$.