§2. Идеалы и делимость (простейшие свойства).

всюду в этом параграфе слово «кольцо» означает «коммутативное кольцо с единицей»

2.1. Немного о строении идеалов. Любое множество элементов $A = \{a_\nu\}$ коммутативного кольца K порождает идеал $(a_\nu) \subset K$, состоящий из всевозможных *конечных* линейных комбинаций

$$b_1 a_{\nu_1} + b_2 a_{\nu_2} + \cdots + b_m a_{\nu_m}$$

элементов $a_\nu \in A$ с произвольными коэффициентами $b_i \in K$.

Упражнение 2.1. Проверьте, что идеалы $(x,y) \subset \mathbb{Q}[x,y]$ и $(2,x) \in \mathbb{Z}[x]$ не являются главными.

Ясно, что всякий идеал можно описать таким образом (взяв достаточно большое множество порождающих элементов a_ν). Кольцо K называется *нётеровым*, если каждый идеал $I \subset K$ порождается конечным набором элементов. Это условие можно переформулировать несколькими равносильными способами.

2.1.1. ЛЕММА. *Следующие свойства коммутативного кольца K попарно эквивалентны:*

1) *любое множество элементов $\{a_\nu\}$ содержит некоторое конечное подмножество, которое порождает тот же идеал, что и само множество;*

2) *любой идеал допускает конечное множество образующих;*

3) *для любой бесконечной цепочки вложенных идеалов $I_1 \subset I_2 \subset I_3 \subset \cdots$ существует $n \in \mathbb{N}$ такое, что $I_\nu = I_n \quad \forall\, \nu \geqslant n$.*

Доказательство. Ясно, что (1) $\Rightarrow$ (2). Чтобы из (2) вывести (3), заметим, что $I = \bigcup I_\nu$ тоже является идеалом, а значит, порождён конечным набором элементов. Все они принадлежат некоторому I_n, и тогда $I_\nu = I_n = I \;\forall\; \nu \geqslant n$. Чтобы вывести (1) из (3), построим цепочку идеалов $I_n = (a_1, a_2, \dots, a_n)$, по индукции добавляя образующие $a_i \notin (a_1, a_2, \dots, a_{n-1})$ из данного множества $\{a_\nu\}$. □

Упражнение 2.2. Покажите, что любое фактор кольцо любого нётерова кольца нётерово.

2.1.2. Предупреждение. Неверно, что все кольца нётеровы: например, в кольце многочленов от бесконечного числа переменных $\mathbb{Q}[x_1, x_2, x_3, \dots]$, элементами которого, по определению, являются всевозможные конечные суммы одночленов от конечного числа переменных x_ν с рациональными коэффициентами, многочлены без свободного члена составляют идеал $(x_1, x_2, \dots)$, который не является конечнопорождённым.

Упражнение 2.3. Будет ли конечно порождённым идеал, образованный в кольце бесконечно гладких функций $\mathbb{R} \longrightarrow \mathbb{R}$ всеми функциями, обращающимися в нуле в нуль вместе со всеми своими производными?

2.1.3. ПРЕДЛОЖЕНИЕ (ТЕОРЕМА ГИЛЬБЕРТА О БАЗИСЕ). *Если кольцо K нётерово, то кольцо многочленов $K[x]$ тоже нётерово.*

Доказательство. Рассмотрим произвольный идеал $I \subset K[x]$ и обозначим через $L_d \subset K$ множество старших коэффициентов всех многочленов d-той степени из I, а через $L_\infty \overset{\text{def}}{=} \bigcup\limits_d L_d$ — множество старших коэффициентов всех многочленов из I вообще.

Упражнение 2.4. Убедитесь, что все L_d и L_∞ являются идеалами в K.

Поскольку K нётерово, все эти идеалы конечно порождены. Пусть L_∞ порождается старшими коэффициентами $a_1, a_2, \dots, a_s \in K$ многочленов $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{s_\infty}^{(\infty)} \in I$ и пусть $\max_\nu(\deg f_\nu) = m$. Аналогично, для каждого $0 \leqslant k \leqslant m-1$ обозначим через $f_1^{(k)}, f_2^{(k)}, \dots, f_{s_k}^{(k)}$ те многочлены, старшие коэффициенты которых порождают идеал $L_k \subset K$. Идеал I порождается $s_0 + \cdots + s_{m-1} + s_\infty$ многочленами $f_\nu^{(\mu)}$. □

Упражнение 2.5. Убедитесь в этом.

2.1.4. СЛЕДСТВИЕ. *Кольцо $K[x_1, x_2, \dots, x_n]$ нётерово, если K нётерово.* □

2.1.5. СЛЕДСТВИЕ. *Всякая конечно порождённая коммутативная алгебра*[1] *над нётеровым кольцом нётерова.* □

Упражнение 2.6*. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Указание. Попытайтесь повторить рассуждение из n° 2.1.3, следя за младшими коэффициентами вместо старших.

2.2. Взаимная простота. Элементы $a, b \in K$ называются *взаимно простыми*, если в кольце K разрешимо уравнение $ax + by = 1$ или, что равносильно, когда $(a, b) = K$.

Упражнение 2.7. Убедитесь, что при взаимно простых a, b и произвольном m

а) a делит mb только если a делит m ;

б) если a делит m и b делит m, то и ab делит m.

Более общим образом, два идеала $I, J \subset K$ называются *взаимно простыми*, если существуют $x \in I$ и $y \in J$, такие что $x + y = 1$. Это условие равносильно тому, что идеал

$$I + J \stackrel{\text{def}}{=} (I, J) = \{x + y \mid x \in I\,,\ y \in J\}$$

(порождённый их объединением и состоящий из всевозможных сумм) совпадает со всем кольцом. Свойства взаимно простых идеалов обобщают свойства взаимно простых чисел.

2.2.1. ЛЕММА. *Если идеал I взаимно прост с каждым из идеалов $J_1, J_2, \dots, J_n$, то он взаимно прост и с их пересечением*[2].

Доказательство. Для каждого $\nu = 1, 2, \dots, n$ мы имеем элементы $x_\nu \in I$ и $y_\nu \in J_\nu$, такие что $x_\nu + y_\nu = 1$. Перемножая все эти эти равенства и раскрывая скобки, мы получим равенство вида

$$(\text{члены, содержащие множитель вида } x_\nu) + y_1 y_2 \cdots y_n = 1\,,$$

в котором первое слагаемое лежит в I, а второе — в $\bigcap_\nu J_\nu$. □

2.2.2. ПРЕДЛОЖЕНИЕ (КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ). *Пусть идеалы $I_1, I_2, \dots, I_n$ произвольного коммутативного кольца K с единицей попарно взаимно просты. Тогда для любого набора из n классов $[a_\nu] \in K/I_\nu$ (где $\nu = 1, 2, \dots, n$) существует $a \in K$, такое что $[a_\nu] = a \pmod{I_\nu}$ одновременно для всех ν, причём для любого другого $a' \in K$, обладающего этим свойством, мы будем иметь $a' - a \in \bigcap_\nu I_\nu$.*

Доказательство. По предыдущей лемме I_k взаимно прост с $\bigcap_{\nu \neq k} I_\nu$ для каждого $\nu \neq k$. Поэтому найдутся $x_k \in I_k$ и $y_k \in \bigcap_{\nu \neq k} I_\nu$, такие что $x_k + y_k = 1$. Это означает, что

$$y_k \pmod{I_\nu} = \begin{cases} 0\,, & \text{при } \nu \neq k \\ 1\,, & \text{при } \nu = k \end{cases}$$

и мы можем взять $a = \sum_{k=1}^{n} y_k a_k$. Для доказательства второго утверждения рассмотрим гомоморфизм колец $A \xrightarrow{a \mapsto (a \pmod{I_1}),\, a \pmod{I_2}),\, \dots,\, a \pmod{I_n}))} (A/I_1) \times (A/I_2) \times \cdots \times (A/I_n)$. По предыдущему, он сюрьективен, а его ядро, очевидно, совпадает с $\bigcap_\nu I_\nu$. □

2.2.3. СЛЕДСТВИЕ. *Для любого набора взаимно простых идеалов $I_1, I_2, \dots, I_n \subset K$ имеется канонический изоморфизм колец*

$$A/\bigcap_\nu I_\nu \xrightarrow[\sim]{a \mapsto (a \pmod{I_1}),\, a \pmod{I_2}),\, \dots,\, a \pmod{I_n}))} (A/I_1) \times (A/I_2) \times \cdots \times (A/I_n)$$

[1] по определению, *конечно порождённой коммутативной K-алгеброй* называется всякое кольцо вида

$$A = K[x_1, x_2, \dots, x_n]/I\ ;$$

классы $a_i = x_i \pmod{I}$ называются *образующими* K-алгебры A, а многочлены $f \in I$ — *соотношениями*. Говоря неформально, A состоит из всего, что можно получить из K и коммутирующих букв $a_1, a_2, \dots, a_n$ при помощи сложения и умножения с учётом полиномиальных соотношений $f(a_1, a_2, \dots, a_n) = 0$, где f пробегает I.

[2] убедитесь, что пересечение идеалов тоже является идеалом

$\square$

2.3. Наибольший общий делитель. Пусть кольцо K целостное. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b. Поскольку равенства $a = mb$ и $b = na$ влекут равенство $a(1 - mn) = 0$, ассоциированность означает, что $a = sb$, где s обратим. Наибольшим общим делителем элементов $a_1, a_2, \dots, a_n$ кольца K называется всякое $d \in K$, делящее каждое a_i и делящееся на любой другой общий делитель всех a_i. Любые два наибольших общих делителя ассоциированы, поэтому $\text{НОД}(a_1, a_2, \dots, a_n)$ (если существует) определён однозначно с точностью до умножения на обратимые элементы. Подчеркнём, что в общем случае условие $\text{НОД}(a, b) = 1$ вовсе не означает взаимной простоты a и b, как она определялась в n° 2.2. Скажем, $\text{НОД}(x, y) = 1$ в $\mathbb{Q}[x, y]$, однако $fx + gy \neq 1$ ни при каких $f, g \in \mathbb{Q}[x, y]$. Но привычные свойства делимости целых чисел всё же можно распространить на любые области главных идеалов.

2.3.1. Пример: в любой области главных идеалов $\text{НОД}(a_1, a_2, \dots, a_n) = d \iff (a_1, a_2, \dots, a_n) = (d)$, поскольку элемент d, порождающий идеал $I = (a_1, a_2, \dots, a_n)$, делит каждое из a_i и делится на любой их общий делитель, ибо, как и все элементы из I, представим в виде $d = \sum x_\nu a_\nu$. Таким образом, в области главных идеалов НОД всегда существует, и условие $(a_1, a_2, \dots, a_n) = K$ (т.е. возможность представить единицу кольца в виде $1 = \sum x_\nu a_\nu$) равносильна условию $\text{НОД}(a_1, a_2, \dots, a_n) = 1$. В частности, китайская теорема об остатках оказывается применима к элементам, не имеющим необратимых общих делителей. Например, если целые числа $m_1, m_2, \dots, m_n$ таковы, что $\text{НОД}(m_i, m_j) = 1$, и $m = m_1 \cdot m_2 \cdot \ \cdots \ \cdot m_n$, то $\mathbb{Z}/(m) \simeq \prod\limits_{\nu=1}^{n} \mathbb{Z}/(m_\nu)$ (как в упр. 1.16). Разумеется, это же верно и в кольце многочленов с коэффициентами в произвольном поле.

2.4. Поле частных. Способ, которым поле $\mathbb{Q}$ получается из кольца $\mathbb{Z}$, дословно обобщается на произвольное целостное кольцо K. А именно, с K можно связать поле Q_K и гомоморфизм

$$K \overset{\iota}{\hookrightarrow} Q_K \tag{2-1}$$

обладающий следующим *свойством универсальности*: для любого гомоморфизма $K \xrightarrow{\varphi} \mathbb{F}$ в произвольное поле $\mathbb{F}$ существует единственное отображение полей $\mathbb{Q}_F \xrightarrow{\widetilde{\varphi}} \mathbb{F}$, такое что $\varphi = \widetilde{\varphi} \circ \iota$:

$$\begin{tikzcd} K \arrow[rr, "\iota"] \arrow[dr, "\varphi"'] & & Q_K \arrow[dl, "\widetilde{\varphi}"] \\ & \mathbb{F} & \end{tikzcd}$$

Этим свойством поле Q_K определяется однозначно с точностью до единственного изоморфизма перестановочного с ι, в том смысле, что для любого другого универсального гомоморфизма $K \xrightarrow{\iota'} Q'_K$ имеется единственный изоморфизм $\psi : Q_K \xrightarrow{\sim} Q'_K$, такой что $\iota' = \psi \circ \iota$.

Упражнение 2.8. Выведите эту единственность из универсальности $K \xrightarrow{\iota} Q_K$ и $K \xrightarrow{\iota'} Q'_K$.

Для построения Q_K рассмотрим множество всех формальных дробей a/b, в которых $a, b \in K$ и $b \neq 0$. Зададим на этом множестве отношение эквивалентности, полагая

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \quad \iff \quad a_1 b_2 - a_2 b_1 = 0 \,.$$

Это отношение рефлексивно, симметрично и транзитивно[3]. Таким образом, множество всех дробей разбивается в объединение непересекающихся классов эквивалентности. Обозначим множество классов эквивалентности через Q_K и определим сложение и умножение классов стандартными правилами

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2} \,.$$

[3]равенство $a_1 b_3 - a_3 b_1 = 0$ выводится из равенств $a_1 b_2 - a_2 b_1 = 0$ и $a_2 b_3 - a_3 b_2 = 0$ умноженем первого на b_3, второго — на b_1 и вычитанием

Упражнение 2.9. Проверьте, что если $a'b'' - a''b' = 0$, то $(a'/b') \cdot (c/d) \sim (a''/b'') \cdot (c/d)$ и $(a'/b') + (c/d) \sim (a''/b'') + (c/d)$ для любой дроби (c/d).

Упражнение 2.10. Проверьте, что Q_K является полем, а гомоморфизм (2-1), отображающий $a \in K$ в класс дроби $a/1$, инъективен.

Универсальность гомоморфизма (2-1) следует из того, что всякое продолжение любого ненулевого гомоморфизма $K \xrightarrow{\varphi} \mathbb{F}$ с K на Q_K обязано переводить $a/b = ab^{-1} \in Q_F$ в $\varphi(a)\varphi(b)^{-1} \in \mathbb{F}$, так что нам ничего не остаётся, как определить $Q_K \xrightarrow{\widetilde{\varphi}} \mathbb{F}$ правилом $a/b \longmapsto \varphi(a)\varphi(b)^{-1}$.

Упражнение 2.11. Проверьте, что это правило и в самом деле корректно определяет гомоморфизм.

Заметим, что применительно к $K = \mathbb{Z}$ только что доказанная нами универсальность означает, что поле $\mathbb{Q}$ единственным образом вкладывается в любое поле $\mathbb{F}$ характеристики нуль, и в частности, остаётся на месте при любом автоморфизме $\mathbb{F} \longrightarrow \mathbb{F}$.

2.4.1. Пример: рациональные функции. Пусть $\mathbb{F}$ — произвольное поле. Поле частных целостного кольца $\mathbb{F}[x_1, x_2, \dots, x_n]$ обозначается $\mathbb{F}(x_1, x_2, \dots, x_n)$ и называется *полем рациональных функций* от n переменных. Рациональные функции от одной переменной устроены особенно просто. Каждую несократимую дробь $p(t)/q(t) \in \mathbb{F}(t)$, знаменатель которой является произведением взаимно простых многочленов $q(t) = q_1(t)q_2(t)\dots q_m(t)$, можно однозначно представить в виде суммы *простейших дробей*

$$\frac{p(t)}{q(t)} = h(t) + \frac{p_1(t)}{q_1(t)} + \frac{p_2(t)}{q_2(t)} + \dots + \frac{p_m(t)}{q_m(t)} \,, \tag{2-2}$$

в которой $\deg h = \deg p - \deg q$ и $\deg p_i < \deg q_i$. В самом деле, домножая обе части (2-2) на q, получаем в $\mathbb{F}[t]$ равенство

$$p = hq + p_1Q_1 + p_2Q_2 + \dots + p_mQ_m \,, \quad \text{где } Q_i = \prod_{\nu \neq i} q_\nu \quad \text{и} \quad \deg(\textstyle\sum p_\nu Q_\nu) < \deg Q \,, \tag{2-3}$$

которое показывает, что многочлены h и $r = \sum p_\nu Q_\nu$ однозначно определяются как неполное частное и остаток от деления p на q в $\mathbb{F}[t]$, а каждый из p_i — как единственный многочлен степени $< \deg q_i$, представляющий в фактор кольце $\mathbb{F}[t]/(q_i)$ класс $r^{-1} \pmod{q_i} \equiv p\,Q_i^{-1} \pmod{q_i}$ (Q_i обратим по модулю q_i, поскольку $\text{нод}(q_i, Q_i) = 1$). Таким образом, чтобы построить разложение (2-2), надо поделить p на q с остатком: $p/q = h + r/q$, потом представить r в виде $r = p_1Q_1 + q_1r_1$ с $\deg p_1 < \deg q_1$ и $\deg r_1 < \deg Q_1$, что даёт $r/q = p_1/q_1 + r_1/Q_1$, где $Q_1 = q_2 \, \cdots \, q_n$ уже не содержит q_1 и т. д. по индукции.

Разложение (2-2) часто бывает полезно при интегрировани и дифференцировании рациальных функций, разложении функций в степенные ряды[4], вычислении разнообразных сумм и т. п. Как правило, его быстрее всего получить методом неопределенных коэффициентов: зная оценки сверху на степени h и p_i, записать эти многочлены с неопределенными коэффициентами и использовать (2-3) для получения соотношений между ними, скажем, подставляя в обе части конкретные значения $t \in \mathbb{F}$ (например, корни многочленов q_i) или, на худой конец, сравнивая коэффициенты при одинаковых степенях t.

Упражнение 2.12. Найдите первообразную и 2005-ю производную от $x^4/(1 + x^2)$.

Указание. Запишите $x^4/(x^2 + 1) = x^2 + \alpha/(x + i) + \beta/(x - i)$. Для отыскания $\alpha, \beta \in \mathbb{C}$ умножьте обе части на общий знаменатель и подставьте $x = \pm i$.

Упражнение 2.13. Покажите, что любая дробь вида $p/q^d \in \mathbb{F}(x)$ с $\deg p < d \cdot \deg q$ однозначно записывается в виде $\sum\limits_{\nu=1}^{d} p_\nu/q^\nu$, где $\deg p_\nu < \deg q$ при всех ν.

Указание. Это не что иное как запись p в q-ической позиционной системе счисления. То же самое верно и для натуральных чисел: всякое $p < q^k$ единственным образом представляется в виде $\sum\limits_{\nu=1}^{d} p_\nu/q^\nu$ с $p_\nu < q$; мы постоянно пользуемся этим в повседневной жизни, полагая $q = 10$.

Упражнение 2.14. Сформулируйте и докажите аналог разложения в сумму простейших дробей
а) в поле $\mathbb{Q}$ б) в поле частных произвольной области главных идеалов[5].

2.5. Максимальность, простота и неприводимость. Мы видели, что кольцо $\mathbb{Z}/(p)$ является полем тогда и только тогда, когда p простое число, а кольцо $\mathbb{F}[x]/(f)$ (где $\mathbb{F}$ — поле) является

[4] ср. с упр. 1.9

[5] один из возможных вариантов см. в книге *С. Ленг. Алгебра*. М. «Мир» (1968) гл. 5 §5 с. 145

полем тогда и только тогда, когда многочлен f неприводим. В произвольном кольце K понятия простоты, неприводимости и свойства кольца вычетов быть полем превращаются в три *различных* свойства.

Идеал $\mathfrak{m} \subset K$ называется *максимальным*, если фактор кольцо $K/\mathfrak{m}$ является полем. Название объясняется тем, что для максимальности идеала $\mathfrak{m}$ необходимо и достаточно, чтобы он не содержался собственным образом ни в каком другом нетривиальном идеале. Действительно, обратимость ненулевого элемента $a \in K$ по модулю $\mathfrak{m}$ равносильна разрешимости уравнения

$$ax + y = 1$$

относительно $x \in K$ и $y \in I$. С другой стороны, разрешимость этого уравнения означает, что идеал $(\mathfrak{m}, a)$, порождённый $\mathfrak{m}$ и элементом a, совпадает с K (ибо содержит единицу).

Идеал $\mathfrak{p} \subset K$ называется *простым*, если в фактор кольце $K/\mathfrak{p}$ нет делителей нуля. Необратимый элемент $p \in K$ называется *простым*, если главный идеал $(p) \subset K$ прост. Таким образом, простота p равносильна тому, что всякое произведение делится на p только если хотя бы один из его сомножителей делится на p. Ясно, что любой максимальный идеал прост, но обратное неверно: скажем, идеал $(y) \subset \mathbb{Q}[x, y]$ прост, но не максимален, ибо $\mathbb{Q}[x, y]/(y) \simeq \mathbb{Q}[x]$.

Необратимый элемент $q \in K$ называется *неприводимым*, если из равенства $ab = q$ следует, что один из сомножителей a, b обратим. В целостном кольце всякий простой элемент p неприводим, поскольку равенство $ab = p$ означает, что один из сомножителей, скажем a, имеет вид pm, а тогда $p(1 - mb) = 0$ и b обратим. Но обратное неверно, и примеры непростых неприводимых элементов часто возникают в кольцах алгебраических чисел.

Упражнение 2.15. Найдите непростой неприводимый элемент в кольце $\mathbb{Z}[\sqrt{5}]$.

2.5.1. ПРЕДЛОЖЕНИЕ. *В области главных идеалов неприводимость элемента q равносильна максимальности идеала (q). В частности, простота элемента равносильна его неприводимости.*

Доказательство. Если идеал (q) максимален, то q прост, а значит и неприводим. Если q неприводим, и идеал (q) содержится в некотором другом идеале (d), т. е. $q = ds$, то либо d обратим, и $(d) = K$, либо s обратим, и $(q) = (d)$. Значит, (q) максимален. $\square$

2.6. Факториальные кольца. Целостное кольцо называется *факториальным*, если каждый его необратимый элемент a является произведением конечного числа неприводимых $a = q_1 q_2 \cdots q_m$, причём любое другое разложение $a = q_1' q_2' \cdots q_k'$ в произведение неприводимых содержит то же число сомножителей $k = m$ и, после надлежащей перенумерации, каждый q_ν' будет ассоциирован с q_ν. Разложение любого элемента в конечное произведение неприводимых множителей имеется во многих кольцах, а вот единственность такого разложения является довольно тонким ограничением на кольцо.

2.6.1. ПРЕДЛОЖЕНИЕ. *В произвольном нётеровом кольце всякий элемент является произведением конечного числа неприводимых.*

Доказательство. Пусть a приводим. Запишем его в виде произведения необратимых элементов. Каждый приводимый сомножитель этого произведения снова запишем в виде произведения необратимых элементов и т. д. Эта процедура закончится, когда все сомножители станут неприводимы, что и требуется. Если же она никогда не закончится, мы сможем образовать бесконечную последовательность $\{a_i\}$, в которой каждый a_{i+1} делит a_i, но не ассоциирован с ним. Тогда главные идеалы $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ образуют бесконечную строго возрастающую цепочку, что невозможно. $\square$

2.6.2. ПРЕДЛОЖЕНИЕ. *В факториальном кольце каждый неприводимый элемент прост. Наоборот, целостное кольцо, в котором каждый элемент является произведением конечного числа неприводимых, а все неприводимые элементы просты, факториально.*

Доказательство. Пусть K факториально, $q \in K$ неприводим, и ab делится на q. Из-за единственности разложения на неприводимые множители, q входит в разложение произведения ab, которое, в силу той же единственности, является произведением разложений a и b. Стало быть, q делит один из сомножителей, а значит прост. Наоборот, пусть все неприводимые элементы просты, и мы имеем равенство $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, в котором все множители неприводимы, а значит просты. Из простоты p_1 вытекает, что произведение в правой части содержит множитель, делящийся на p_1. Пусть это $q_1 = sp_1$. Поскольку q_1 неприводим, s обратим. Вынося p_1, получим $p_1(p_2 \cdots p_k - sq_2 \cdots q_m) = 0$, откуда следует более короткое равенство $p_2 p_3 \cdots p_k = (sq_2) q_3 \cdots q_m$ и т. д. □

2.6.3. СЛЕДСТВИЕ. *Все области главных идеалов факториальны.* □

Упражнение 2.16. Рассмотрим произвольный набор элементов $a_1, a_2, \ldots, a_m$ факториального кольца K. Пусть каждый из элементов раскладывается на неприводимые множители как

$$a_i = q_1 q_2 \cdots q_r \cdot p_{i,1} q_{i,2} \cdots q_{i,s_i} \ ,$$

где $q_1, q_2, \ldots, q_r$ входят во все разложения, а все остальные сомножители $p_{\mu,\nu}$ попарно не ассоциированы. Покажите, что $\text{нод}(a,b) = q_1 q_2 \cdots q_r$ равен произведению всех общих неприводимых делителей.

2.7. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо, и Q_K — его поле частных. Кольцо многочленов $K[x]$ является подкольцом в кольце многочленов $Q_K[x]$. Назовём *содержанием* многочлена $f = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in K[x]$ наибольший общий делитель его коэффициентов:

$$\operatorname{cont}(f) \overset{\text{def}}{=} \text{нод}(a_0, a_1, \ldots, a_n) \ .$$

Всякий многочлен $f(x) \in Q_K[x]$ можно записать в виде

$$f(x) = \frac{a}{b} \cdot \widetilde{f}(x) \,, \tag{2-4}$$

где $\widetilde{f}(x) \in K[x]$ имеет $\operatorname{cont}(f) = 1$, а $a, b \in K$ имеют $\text{нод}(a,b) = 1$, причём a, b и $\widetilde{f}(x)$ определяются по f однозначно с точностью до умножения на обратимые элементы из K, поскольку равенство

$$\frac{a}{b} \cdot \widetilde{f}(x) = \frac{c}{d} \cdot \widetilde{g}(x)$$

в $Q_K[x]$ означает равенство $ad \cdot \widetilde{f}(x) = bc \cdot \widetilde{g}(x)$ в $K[x]$; сравнивая содержание обеих частей, получаем $ad = bc$, что возможно только если a ассоциирован с c, а b с d, откуда $\widetilde{f}(x) = \widetilde{g}(x)$ с точностью до умножения на обратимую константу.

2.7.1. ЛЕММА. *Для любых двух многочленов f, g с коэффициентами в произвольном факториальном кольце K*

$$\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g) \ . \tag{2-5}$$

Доказательство. Достаточно для каждого неприводимого $q \in K$ показать, что q делит левую часть (2-5), если и только если он делит правую. Для этого применим к равенству (2-5) гомоморфизм редукции по модулю q

$$K[x] \xrightarrow{f \mapsto [f]_q} (K/(q))[x] \ ,$$

заменяющий коэффициенты многочленов на их классы вычетов по модулю q. Поскольку неприводимые элементы факториального кольца просты, кольцо $K/(q)$ целостное. Но тогда и кольцо многочленов $(K/(q))[x]$ целостное. Тем самым, произведение $[fg]_q = [f]_q [g]_q$ обращается в нуль, если и только если один из сомножителей $[f]_q$, $[g]_q$ равен нулю, что и требуется. □

2.7.2. СЛЕДСТВИЕ (ЛЕММА ГАУССА). *Пусть $f \in K[x]$ — произвольный, а $g \in K[x]$ имеет содержание 1. Если f делится на g в кольце $Q_K[x]$, то он делится на g и в $K[x]$.*

Доказательство. Если в $Q_K[x]$ выполняется равенство $\operatorname{cont}(f)\widetilde{f}(x) = f(x) = g(x) \cdot h(x) = g(x) \cdot \frac{c}{d} \cdot \widetilde{h}(x)$, где $\widetilde{f}, \widetilde{h} \in K[x]$, $c, d \in K$, $\operatorname{cont}\widetilde{f} = \operatorname{cont}(\widetilde{h}) = \text{нод}(c,d) = 1$, то $\operatorname{cont}(g\widetilde{h}) = 1$, и в силу единственности представления (2-4) мы должны иметь $\operatorname{cont}(f) = c$ и $d = 1$ (с точностью до умножения на обратимые элементы из K). □

Упражнение 2.17. Пусть многочлен $f \in K[x]$ раскладывается в $Q_K[x]$ в произведение двух многочленов. Покажите, что тогда и в $K[x]$ многочлен f можно разложить в произведение двух многочленов, причём тех же самых степеней, что и в $Q_K[x]$.

Упражнение 2.18. Покажите, что множество неприводимых элементов кольца $K[x]$ состоит из неприводимых констант и многочленов содержания 1, неприводимых в $Q_K[x]$.

2.7.3. СЛЕДСТВИЕ. *Кольцо многочленов над факториальным кольцом факториально.*

Доказательство. Область главных идеалов $Q_K[x]$ факториальна. Всякий многочлен $f \in Q_K[x]$ раскладывается в $Q_K[x]$ на неприводимые множители, которые можно записать в виде (2-4). Поэтому

$$\operatorname{cont}(f)\widetilde{f}(x) = f(x) = \prod \frac{a_\nu}{b_\nu}\widetilde{f}_\nu = \frac{a}{b}\prod \widetilde{f}_\nu \ ,$$

где $\widetilde{f}_\nu \in K[x]$ неприводимы в $Q_K[x]$ (а тем более в $K[x]$) и $\operatorname{cont}(\widetilde{f}_\nu) = \text{нод}(a,b) = 1$. Поскольку $\operatorname{cont}(\prod \widetilde{f}_\nu) = 1$, в силу единственности представления (2-4) мы получаем $b = 1$ и $f = a\prod \widetilde{f}_\nu$ (с точностью до умножения на обратимые константы из K). Раскладывая $a \in K$ в произведение неприводимых констант, получаем разложение f в произведение неприводимых множителей в кольце $K[x]$. Единственность такого разложения следует из упр. 2.18, единственности представления (2-4) и единственности разложений на неприводимые множители в K и в $Q_K[x]$. $\square$

2.7.4. СЛЕДСТВИЕ. *Если K факториальное кольцо (например, область главных идеалов) или поле, то кольцо многочленов $K[x_1, x_2, \dots, x_n]$ от любого числа переменных факториально.* $\square$

2.7.5. Пример: разложение многочленов с целыми коэффициентами. Часто приходится иметь дело с разложением на множители многочленов $f \in \mathbb{Z}[x]$ в кольце $\mathbb{Q}[x]$. Все рациональные корни f легко находятся конечным числом проб.

Упражнение 2.19. Покажите, что несократимая дробь $a = p/q \in \mathbb{Q}$ может быть корнем многочлена $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Z}[x]$, только если p делит a_0, а q делит a_n.

Знание комплексных корней f тоже весьма полезно.

Упражнение 2.20. Разложите $x^4 + 4$ в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

В общем случае лемма Гаусса сводит вопрос о разложении в $\mathbb{Q}[x]$ к разложению в $\mathbb{Z}[x]$. После этого можно воспользоваться довольно трудоёмким, но вполне эффективным алгоритмом Кронекера, позволяющим либо явно найти разложение в $\mathbb{Z}[x]$, либо доказать что его нет[6]. Быстро[7] прикинуть, существует ли разложение $f = gh$ с $\deg g, \deg h < \deg f$, и если да, то каковы могут быть степени (а отчасти — и коэффициенты) g и h, позволяет редукция по простому модулю, аналогичная той, что мы использовали в n° 2.7.1.

Упражнение 2.21. Перечислите все неприводимые многочлены степени $\leqslant 3$ в $\mathbb{F}_2[x]$ и в $\mathbb{F}_3[x]$.

Упражнение 2.22. Выясните, приводим ли над $\mathbb{Q}$ многочлен $f(t) = x^5 + x^2 + 1$, отправив его в $\mathbb{F}_2[x]$.

Пусть, например, при редукции $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$ от многочлена f остаётся только старший моном x^n, где $n = \deg f$. Поскольку кольцо $\mathbb{F}_p[x]$ факториально, это означает, что g и h тоже редуцируются в свои старшие мономы. В частности, их свободные члены делятся на p, а стало быть, свободный член f делится на p^2. Мы получаем *критерий Эйзенштейна*: если все коэффициенты a_i приведённого[8] многочлена

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$$

делятся на p, но свободный член a_0, делясь на p, не делится при этом на p^2, то f неприводим в $\mathbb{Q}[x]$.

Упражнение 2.23. Покажите, что многочлен $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = (x^p - 1)/(x-1)$ неприводим в $\mathbb{Q}[x]$ при простом p.

Указание. Сделайте подстановку $x - 1 = t$ и примените критерий Эйзенштейна.

Упражнение 2.24. Пусть при гомоморфизме целостных колец $K \xrightarrow{\varphi} L$ многочлен $f \in K[x]$ перходит в многочлен, неприводимый над полем частных Q_L и имеющий ту же степень, что f. Покажите, что f не раскладывается в $K[x]$ в произведение двух многочленов меньшей степени.

---

[6] см. Э. Б. Винберг. *Курс алгебры*. М. «Факториал» (1999) гл. 3 §6 с. 124 или — в более подробном изложении — *Б. Л. ван дер Варден. Алгебра*. М. «Наука» (1976) гл. V §32 с. 122

[7] но уже «без гарантий»

[8] многочлен называется *приведённым* (или *унитарным*), если его старший коэффициент равен единице