§5. Идеалы, фактор кольца и разложение на множители

5.1. Идеалы. Подкольцо I коммутативного кольца K называется *идеалом*, если вместе с каждым своим элементом оно содержит и все его кратные. В n° 2.6.3 мы видели, что этими свойствами обладает ядро любого гомоморфизма колец. Множество всех элементов кольца, кратных фиксированному элементу $a \in K$, также является идеалом. Этот идеал обозначается

$$(a) = \{ka \mid k \in K\}, \tag{5-1}$$

и называется *главным* идеалом, порождённым a. Мы встречались с главными идеалами при построении колец вычетов $\mathbb{Z}/(n)$ и $\Bbbk[x]\,/\,(f)$, где они возникали как ядра эпиморфизмов

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)\,,\ m \mapsto [m]_n\,, \qquad \text{и} \qquad \Bbbk[x] \twoheadrightarrow \Bbbk[x]/(f)\,,\ g \mapsto [g]_f\,,$$

сопоставляющих целому числу (соотв. многочлену) его класс вычетов. Ещё в любом кольце K имеются *тривиальные* идеалы $(0) = \{0\}$ и $(1) = K$.

Упражнение 5.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей попарно равносильны: а) $I = K$ б) $1 \in I$ в) I содержит обратимый элемент.

Предложение 5.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных идеалов.

Доказательство. Из упр. 5.1 вытекает, что ни в каком поле нетривиальных идеалов нет. Наоборот, если в кольце нет нетривиальных идеалов, то главный идеал (b), порождённый любым ненулевым элементом b, совпадает со всем кольцом и, в частности, содержит единицу, т. е. $1 = ab$ для некоторого a. Тем самым, любой ненулевой элемент обратим. □

5.1.1. Нётеровость. Любое подмножество $M \subset K$ порождает идеал $(M) \subset K$, состоящий из всех элементов кольца K, представимых в виде

$$b_1a_1 + b_2a_2 + \dots + b_ma_m\,, \tag{5-2}$$

где $a_1, a_2, \dots, a_m$ — произвольные элементы множества M, $b_1, b_2, \dots, b_m$ — произвольные элементы кольца K, и число слагаемых $m \in \mathbb{N}$ также произвольно.

Упражнение 5.2. Убедитесь, что $(M) \subset K$ это и в самом деле идеал

Всякий идеал $I \subset K$ имеет вид (M) для подходящего $M \subset K$: например, можно положить $M = I$. Идеал $I \subset M$ называется *конечно порождённым*, если его можно породить конечным множеством M, т. е. если существуют такие $a_1, a_2, \dots, a_k \in I$, что

$$I = (a_1, a_2, \dots, a_k) = \{b_1a_1 + b_2a_2 + \dots + b_ka_k \mid b_i \in K\}\,.$$

Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Лемма 5.1
Следующие свойства коммутативного кольца K попарно эквивалентны:

1) любое подмножество $M \subset K$ содержит конечный набор элементов $a_1, a_2, \dots, a_k \in M$, порождающий тот же идеал, что и M
2) любой идеал $I \subset K$ конечно порождён
3) любая бесконечная возрастающая цепочка вложенных идеалов $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ стабилизируется в том смысле, что найдётся такое $n \in \mathbb{N}$, что $I_\nu = I_n$ для всех $\nu \geqslant n$.

Доказательство. Ясно, что (1) ⇒ (2). Чтобы из (2) вывести (3), заметим, что объединение $I = \bigcup I_\nu$ всех идеалов цепочки тоже является идеалом. Согласно (2), идеал I порождён конечным набором элементов. Все они принадлежат некоторому идеалу I_n. Тогда $I_n = I = I_\nu$ при $\nu \geqslant n$. Чтобы вывести (1) из (3), будем по индукции строить цепочку идеалов $I_n = (a_1, a_2, \dots, a_n)$, начав с произвольного элемента $a_1 \in M$ и добавляя на k-том шагу очередную образующую $a_k \in M \smallsetminus I_{k-1}$ до тех пор, пока это возможно, т. е. пока $M \not\subset I_k$. Так как $I_{k-1} \subsetneq I_k$, этот процесс не может продолжаться бесконечно, и на каком-то шагу мы получим идеал, содержащий всё множество M, а значит, совпадающий с (M). □

Определение 5.1
Кольцо K, удовлетворяющее условиям лем. 5.1, называется *нётеровым*. Отметим, что любое поле нётерово.

Теорема 5.1
Если кольцо K нётерово, то кольцо многочленов $K[x]$ также нётерово.

Доказательство. Рассмотрим произвольный идеал $I \subset K[x]$ и обозначим через $L_d \subset K$ множество старших коэффициентов всех многочленов степени $\leqslant d$ из I, объединённое с нулём, а через $L_\infty = \bigcup\limits_d L_d$ — множество старших коэффициентов вообще всех многочленов из I, также объединённое с нулём.

Упражнение 5.3. Убедитесь, что все L_d (включая L_∞) являются идеалами в K.

Поскольку кольцо K нётерово, все идеалы L_d конечно порождены. Для каждого d (включая $d = \infty$) обозначим через $f_1^{(d)}, f_2^{(d)}, \dots, f_{m_d}^{(d)} \in K[x]$ многочлены, старшие коэффициенты которых порождают соответствующий идеал $L_d \subset K$. Пусть наибольшая из степеней многочленов $f_i^{(\infty)}$ (их старшие коэффициенты порождают идеал L_∞) равна $D \in \mathbb{N}$. Покажем, что идеал I порождается многочленами f_i^∞ и многочленами $f_j^{(d)}$ с $0 \leqslant d < D$.

Произвольный многочлен $g \in I$ сравним по модулю многочленов $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{m_\infty}^{(\infty)}$ с многочленом, степень которого строго меньше D. В самом деле, поскольку старший коэффициент многочлена g лежит в идеале L_∞, он имеет вид $\sum \lambda_i a_i$, где $\lambda_i \in K$, а a_i — старшие коэффициенты многочленов $f_i^{(\infty)}$. При $\deg g \geqslant D$ все разности

$$m_i = \deg g - \deg f_i^{(\infty)} \geqslant 0\,,$$

так что мы можем образовать многочлен $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{m_i}$, сравнимый с g по модулю I и имеющий строго меньшую, чем g степень. Заменим g на h и повторим эту процедуру, пока не получим многочлен $h \equiv g \pmod{(f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{m_\infty}^{(\infty)})}$ с $\deg h < D$. Теперь старший коэффициент многочлена h лежит в идеале L_d с $d < D$, и мы можем сокращать его старший член и строго уменьшать степень, вычитая из h подходящие комбинации многочленов $f_j^{(d)}$ с $0 \leqslant d < D$. □

Следствие 5.1
Если K нётерово, то кольцо многочленов $K[x_1, x_2, \dots, x_n]$ также нётерово. □

Упражнение 5.4. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Следствие 5.2
В нётеровом кольце любая бесконечная система полиномиальных уравнений эквивалентна некоторой своей конечной системе.

Доказательство. Пусть имеется бесконечный набор уравнений $f_\nu(x_1, x_2, \dots, x_n) = 0$, где $f_\nu \in K[x_1, x_2, \dots, x_n]$. Если K нётерово, то $K[x_1, x_2, \dots, x_n]$ тоже нётерово, и среди многочленов f_ν можно выбрать такой конечный набор $f_1, f_2, \dots, f_m$, что каждый из многочленов f_ν будет представляться в виде $f_\nu = g_1 f_1 + g_2 f_2 + \dots + g_m f_m$, а значит, обратится в нуль на любом решении конечной системы $f_1 = f_2 = \dots = f_m = 0$. □

5.1.2. Примеры ненётеровых колец. Кольцо многочленов от бесконечного числа переменных $\mathbb{Q}[x_1, x_2, x_3, \dots]$, элементами которого, по определению, являются всевозможные конечные суммы взятых с рациональными коэффициентами мономов вида $x_{\nu_1}^{m_1} x_{\nu_2}^{m_2} \cdots x_{\nu_s}^{m_s}$ (произведение конечного числа переменных x_ν в некоторых степенях), не является нётеровым: его идеал $(x_1, x_2, \dots)$, состоящий из всех многочленов без свободного члена, нельзя породить конечным множеством многочленов.

Упражнение 5.5. Докажите это и выясните, является ли конечно порождённым идеал, образованный в кольце бесконечно гладких функций $\mathbb{R} \to \mathbb{R}$ всеми функциями, которые обращаются в нуле в нуль вместе со всеми своими производными.

Предостережение 5.1. Подкольцо нётерова кольца может не быть нётеровым. Например, кольцо формальных степенных рядов $\mathbb{C}[\![z]\!]$ нётерово по упр. 5.4, тогда как его подкольцо образованное рядами, сходящимися всюду в $\mathbb{C}$, нётеровым не является.

Упражнение 5.6. Приведите пример бесконечной возрастающей цепочки строго вложенных идеалов в кольце сходящихся всюду в $\mathbb{C}$ степенных рядов с комплексными коэффициентами.

5.2. Фактор кольца. Пусть на коммутативном кольце K задано отношение эквивалентности, разбивающее K в дизъюнктное объединение классов эквивалентных элементов. Обозначим множество классов через X и рассмотрим сюрьективное отображение

$$\pi : K \twoheadrightarrow X, \tag{5-3}$$

переводящее элемент $a \in K$ в его класс эквивалентности $\pi(a) = [a] \in X$. Мы хотим задать на множестве X структуру коммутативного кольца так, чтобы отображение (5-3) оказалось гомоморфизмом колец, или — что то же самое — так, чтобы сложение и умножение классов задавалось формулами

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab]. \tag{5-4}$$

Из установленных нами в n° 2.6.3 свойств гомоморфизмов колец вытекает, что в этом случае класс $[0]$, содержащий $0 \in K$ и должный быть ядром гомоморфизма (5-3), с необходимостью является идеалом кольца K, а все остальные слои гомоморфизма (5-3) суть аддитивные сдвиги ядра на элементы кольца K, т. е.

$$\forall\, a \in K \quad [a] = a + [0] = \{a + b \mid b \in [0]\}\,.$$

Оказывается, что этих условий и достаточно: для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{5-5}$$

образует разбиение кольца K, и правила (5-4) корректно определяют на нём структуру коммутативного кольца с единицей $[1]_I$ и нулём $[0]_I = I$.

Упражнение 5.7. Убедитесь, что отношение сравнимости по модулю идеала

$$a_1 \equiv a_2 \pmod{I}\,,$$

означающее, что $a_1 - a_2 \in I$, является отношением эквивалентности, разбивающим K в точности на классы (5-5), и проверьте, что формулы (5-4) корректно определены на этих классах.

Определение 5.2

Классы эквивалентности (5-5) называются *классами вычетов* (или *смежными классами*) по модулю идеала I . Множество этих классов с операциями (5-4) называется *фактор кольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм

$$K \twoheadrightarrow K/I\,, \quad a \mapsto [a]_I\,, \tag{5-6}$$

сопоставляющий каждому элементу кольца его класс вычетов, называется *гомоморфизмом факторизации*

Пример 5.1 (кольца вычетов)

Рассматривавшиеся выше кольца $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$ суть фактор кольца кольца целых числел и кольца многочленов по главным идеалам $(n) \subset \mathbb{Z}$ и $(f) \subset \Bbbk[x]$ соответственно.

Пример 5.2 (образ гомоморфизма)

Согласно n° 2.6.3, образ любого гомоморфизма коммутативных колец $\varphi : K_1 \to K_2$ канонически изоморфен фактор кольцу $K_1/\ker(\varphi)$. При этом изоморфизме элементу

$$b = \varphi(a) \in \operatorname{im}\varphi \subset K_2$$

отвечает класс вычетов $[a]_{\ker\varphi} = \varphi^{-1}(b)$.

Упражнение 5.8. Покажите, что фактор кольцо нётерова кольца тоже нётерово.

Пример 5.3 (максимальные идеалы и гомоморфизмы вычисления)

Идеал $\mathfrak{m} \subset K$ называется *максимальным*, если фактор кольцо $K/\mathfrak{m}$ является полем. Название связано с тем, что идеал $\mathfrak{m} \subset K$ максимален , если и только если он собственный[1] и не

[1]отличен от $(0) = 0$ и $(1) = K$

содержится ни в каком строго большем собственном идеале. В самом деле, обратимость класса элемента $a \in K \smallsetminus \mathfrak{m}$ в фактор кольце $K/\mathfrak{m}$ означает существование таких элементов $b \in K$ и $x \in \mathfrak{m}$, что $ab = 1+x$ в K. А это, в свою очередь, означает, что идеал, порождённый $\mathfrak{m}$ и любым элементом $a \in K \smallsetminus \mathfrak{m}$ содержит 1.

Максимальные идеалы в кольцах функций возникают как ядра *гомоморфизмов вычисления*. Пусть X — произвольное множество, $p \in X$ — любая точка, и K — подкольцо в кольце всех функций $X \to \Bbbk$, содержащее тождественно единичную функцию 1 и вместе с каждой функцией $f \in K$ содержащее и все пропорциональные ей функции cf, $c \in \Bbbk$. Гомоморфизм вычисления $\mathrm{ev}_p : K \to \Bbbk$ переводит функцию $f \in K$ в её значение $f(p) \in \Bbbk$. Он, очевидно, сюрьективен, и его ядро $\ker \mathrm{ev}_p = \{f \in K \mid f(p) = 0\}$ является максимальным идеалом в K.

Упражнение 5.9. Убедитесь, что каждый максимальный идеал кольца $\mathbb{C}[x]$ имеет вид $\ker \mathrm{ev}_p$ для некоторого $p \in \mathbb{C}$, и приведите пример максимального идеала $\mathfrak{m} \subset \mathbb{R}[x]$, отличного от всех идеалов $\ker \mathrm{ev}_p$ с $p \in \mathbb{R}$.

Упражнение 5.10. Покажите, что каждый максимальный идеал кольца непрерывных функций $[0,1] \to \mathbb{R}$ имеет вид ev_p для некоторой точки $p \in [0,1]$.

Пример 5.4 (простые идеалы и гомомрфизмы в поля)
Идеал $\mathfrak{p} \subset K$ называется *простым*,если в фактор кольце $K/\mathfrak{p}$ нет делителей нуля. Иначе говоря, идеал $\mathfrak{p} \subset K$ прост , если и только если из $ab \in \mathfrak{p}$ вытекает, что $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Например, главные идеалы $(p) \subset \mathbb{Z}$ и $(q) \subset \Bbbk[x]$, где $\Bbbk$ — поле, просты тогда и только тогда, когда число p просто, а многочлен q неприводим.

Упражнение 5.11. Убедитесь в этом.

Согласно определениям, всякий максимальный идеал прост. Обратное неверно: скажем, главный идеал $(x) \subset \mathbb{Q}[x,y]$ прост, т. к. $\mathbb{Q}[x,y]/(x) \simeq \mathbb{Q}[x]$, но не максимален, поскольку строго содержится в идеале (x,y) многочленов без свободного члена. Простые идеалы кольца K являются ядрами гомоморфизмов из кольца K во всевозможные поля. В самом деле, образ любого такого гомоморфизма, будучи подкольцом в поле, не имеет делителей нуля. Наоборот, фактор кольцо $K/\mathfrak{p}$ по простому идеалу $\mathfrak{p}$ является подкольцом своего поля частных $Q_{K/\mathfrak{p}}$, и композиция факторизации и вложения $K \twoheadrightarrow K/\mathfrak{p} \hookrightarrow Q_{K/\mathfrak{p}}$ задаёт гомоморфизм из K в поле $Q_{K/\mathfrak{p}}$ с ядром $\mathfrak{p}$.

Упражнение 5.12. Докажите, что а) простой идеал $\mathfrak{p} \subset A$ содержит пересечение конечного набора произвольных идеалов только тогда, когда он содержит хотя бы один из них б) произвольный идеал $\mathfrak{a} \subset A$ содержится в объединении конечного набора простых идеалов только тогда, когда он содержится в одном из них.

5.2.1. Конечно порождённые коммутативные алгебры. Пусть K — произвольное коммутативное кольцо с единицей. Всякое кольцо вида $A = K[x_1, x_2, \dots, x_n]/I$, где $I \subset K[x_1, x_2, \dots, x_n]$ — произвольный идеал, называется *конечно порождённой K-алгеброй*[1]. Классы $a_i = x_i \pmod{I}$ называются *образующими* K-алгебры A, а многочлены $f \in I$ — *соотношениями* между этими образующими.

[1]или, более торжественно, *конечно порождённой коммутативной алгеброй* над кольцом K

Говоря неформально, K-алгебра состоит из всевозможных выражений, которые можно составить из элементов кольца K и коммутирующих букв $a_1, a_2, \dots, a_n$ при помощи операций сложения и умножения, которые совершаются с учётом полиномиальных соотношений $f(a_1, a_2, \dots, a_n) = 0$, где f пробегает I. Из упр. 5.8 и сл. 5.1 мы получаем

Следствие 5.3
Всякая конечно порождённая коммутативная алгебра над нётеровым кольцом нётерова и все соотношения между её образующими являются следствиями конечного числа соотношений. □

5.3. Кольца главных идеалов. Целостное кольцо с единицей называется *кольцом главных идеалов*, если каждый его идеал является главным. Параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, который мы наблюдали выше, объясняется тем, что оба эти кольца являются кольцами главных идеалов. Мы фактически доказали это, когда строили в этих кольцах наибольший общий делитель. Ниже мы воспроизведём это доказательство ещё раз таким образом, чтобы оно годилось для чуть более широкого класса колец, допускающих *деление с остатком.*

5.3.1. Евклидовы кольца. Целостное кольцо K с единицей называется *евклидовым*, если существует *функция высоты* (или *евклидова норма*) $\nu : K \smallsetminus \{0\} \to \mathbb{N} \cup \{0\}$, сопоставляющая каждому ненулевому элементу $a \in K$ целое неотрицательное число $\nu(a)$ так, что $\forall\, a, b \in K \smallsetminus \{0\}$ выполняются два свойства:

$$\nu(ab) \geqslant \nu(a) \tag{5-7}$$

$$\exists\, q, r \in K \ : \ a = bq + r \ \text{ и либо } \nu(r) < \nu(b)\,, \text{ либо } r = 0\,. \tag{5-8}$$

Элементы q и r из (5-8), называются, соответственно, *неполным частным* и *остатком* от деления a на b. Подчеркнём, что их единственности (для данных a и b) не предполагается.

Упражнение 5.13. Докажите евклидовость колец: а) $\mathbb{Z}$, $\nu(z) = |z|$ б) $\Bbbk[x]$, $\nu(f) = \deg f$
в) $\mathbb{Z}[i] \overset{\text{def}}{=} \{\, a + bi \in \ \mid a, b \in \mathbb{Z},\ i^2 = -1 \}$, $\nu(z) = |z|^2$
г) $\mathbb{Z}[\omega] \overset{\text{def}}{=} \{ a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0 \}$, $\nu(z) = |z|^2$.

Все четыре кольца из предыдущего упражнения являются кольцами главных идеалов в силу следующей теоремы.

Предложение 5.2
Любое евклидово кольцо является кольцом главных идеалов[1].

Доказательство. Пусть $I \subset K$ — идеал, и $d \in I$ — ненулевой элемент наименьшей высоты. Покажем, что каждый элемент $a \in I$ делится на d. Поделим a на d с остатком: $a = dq + r$. Так как $a, d \in I$, остаток $r = a - dq \in I$. Поскольку строгое неравенство $\nu(r) < \nu(d)$ невозможно, мы заключаем, что $r = 0$. □

Упражнение 5.14. Покажите, что в любом евклидовом кольце равенство $\nu(ab) = \nu(a)$ в свойстве (5-7) равносильно тому, что элемент b обратим.

[1]отметим, что обратное неверно, но контрпримеры приходят из достаточно продвинутой арифметики и геометрии, и для их содержательного обсуждения требуется техника, которой мы пока не владеем (впрочем, см. замечание 3 на стр. 365 книги *Э. Б. Винберг.* Курс алгебры. М. «Факториал», 1999)

5.3.2. НОД и взаимная простота. В кольце главных идеалов K у любого набора элементов $a_1, a_2, \dots, a_n$ есть наибольший общий делитель $d = \text{нод}(a_1, a_2, \dots, a_n) \in K$, делящий каждый из элементов a_i и делящийся на любой другой общий делитель. Это простая переформулировка того, что идеал, порождённый элементами $a_1, a_2, \dots, a_n$, является главным. В самом деле, поскольку

$$(a_1, a_2, \dots, a_n) = \{x_1a_1 + x_2a_2 + \dots + x_na_n \mid x_i \in K\} = (d)$$

для некоторого $d \in K$, элемент d, как и все элементы $(a_1, a_2, \dots, a_n)$, имеет вид $d = \sum x_\nu a_\nu$, и значит, делится на любой общий делитель чисел a_i. С другой стороны, все элементы $(a_1, a_2, \dots, a_n) = (d)$, включая сами a_i, делятся на d.

Отметим, что наибольший общий делитель d определён не однозначно, а с точностью до умножения на произвольный обратимый элемент кольца.

Упражнение 5.15. В любом целостном коммутативном кольце K равенство ненулевых главных идеалов $(a) = (b)$ равносильно тому, что $a = sb$, где $s \in K$ обратим.

Поэтому всюду в дальнейшем обозначение $\text{нод}(a_1, a_2, \dots, a_n)$ подразумевает некоторый класс элементов, рассматриваемых с точностью до умножения на обратимую константу, и все формулы, которые будут писаться, будут относиться к произвольно выбранному конкретному представителю этого класса.

Из наличия представления $\text{нод}(a_1, a_2, \dots, a_n) = x_1a_1 + x_2a_2 + \dots + x_na_n$ вытекает, что в любом кольце главных идеалов отсутствие необратимых общих делителей у элементов $a_1, a_2, \dots, a_n$ равносильна их *взаимной простоте*, т. е. возможности представить единицу кольца в виде[1] $1 = x_1a_1 + x_2a_2 + \dots + x_na_n$ с подходящими $x_i \in K$.

5.4. Факториальность. Всюду в этом разделе мы обозначаем через K *целостное*[2] кольцо. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b. Из равенств $a = mb$ и $b = na = nmb$ вытекает равенство $b(1 - nm) = 0$, откуда $mn = 1$. Таким образом, ассоциированность элементов означает, что они получаются друг из друга умножением на обратимый элемент кольца. Например, в кольце целых чисел $\mathbb{Z}$ числа a и b ассоциированы тогда и только тогда, когда $a = \pm b$.

5.4.1. Неприводимые элементы. Напомним, что элемент $q \in K$ называется *неприводимым*, если он необратим, и из равенства $q = mn$ вытекает, что m или n обратим. Другими словами, неприводимость элемента q означает, главный идеал q не содержится строго ни в каком другом главном идеале, т. е. максимален в множестве главных идеалов. Например, неприводимыми элементами в кольце целых чисел являются простые числа, а в кольце многочленов — неприводимые многочлены.

В кольце главных идеалов любые два неприводимых элемента p, q либо взаимно просты[3], либо ассоциированы, поскольку порождённый ими идеал $(p, q) = (d)$ для некоторого $d \in K$, и в силу сказанного выше из $(p) \subset (d)$ и $(q) \subset (d)$ вытекает, что либо $(d) = (K) = (1)$, либо $(d) = (p) = (q)$.

В произвольном кольце два неассоциированных неприводимых элемента могут не быть взаимно простыми. Например, в $\mathbb{Q}[x, y]$ элементы x и y не взаимно просты и не ассоциированы.

---

[1] иначе взаимную простоту $a_1, a_2, \dots, a_n$ можно описать равенством $(a_1, a_2, \dots, a_n) = K$

[2] т. е. с единицей и без делителей нуля

[3] в смысле опр. 2.2 на стр. 21, т. е. найдутся $x, y \in K : px + qy = 1$

Предложение 5.3
В любом кольце главных идеалов K следующие свойства элемента $p \in K$ попарно эквивалентны друг другу:

1) фактор кольцо $K/(p)$ является полем
2) в фактор кольце $K/(p)$ нет делителей нуля
3) p неприводим, т. е. $p = ab \Rightarrow a$ или b обратим в K .

Доказательство. Импликация (1) $\Rightarrow$ (2) тривиальна и имеет место в любом кольце[1] K. Покажем, что в любом целостном кольце[2] K имеет место импликация (2) $\Rightarrow$ (3). Из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и если в $K/(p)$ нет делителей нуля, то один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, и значит, $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим.

Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Коль скоро в K нет никаких иных идеалов, кроме главных, максимальность идеала (p) в множестве главных идеалов означает, что он максимален в множестве всех собственных идеалов. Согласно прим. 5.3 на стр. 72, это равносильно тому, что $K/(p)$ — поле. □

Упражнение 5.16. Проверьте, что идеалы $(x, y) \subset \mathbb{Q}[x, y]$ и $(2, x) \in \mathbb{Z}[x]$ не являются главными.

Предложение 5.4
В любом нётеровом кольце всякий элемент является произведением конечного числа неприводимых.

Доказательство. Если элемент a неприводим, доказывать нечего. 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 строго вложенных друг в друга главных идеалов $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$, что невозможно. □

Определение 5.3
Целостное кольцо называется *факториальным*, если каждый его необратимый элемент является произведением конечного числа неприводимых элементов, причём любые два таких разложения $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_k$ состоят из одинакового числа сомножителей $k = m$, и после надлежащей их перенумерации найдутся такие обратимые элементы s_ν, что $q_\nu = p_\nu s_\nu$ при всех ν.

5.4.2. Простые элементы. Элемент $p \in K$ называется *простым*, если порождённый им главный идеал $(p) \subset K$ прост, т. е. в фактор кольце $K/(p)$ нет делителей нуля. Это означает, что для любых $a, b \in K$ из того, что произведение ab делится на p, вытекает, что a или b делится на p.

[1] см. n° 2.4.1 на стр. 22
[2] не обязательно являющемся кольцом главных идеалов

Всякий простой элемент p автоматически неприводим: если $p = xy$, то один из сомножителей, скажем x, делится на p, и тогда $p = pyz$, откуда $yz = 1$ и y обратим. Согласно предл. 5.3 в кольце главных идеалов верно и обратное: все неприводимые элементы кольца главных идеалов просты.

Однако, в общей ситуации простота является более сильным свойством, чем неприводимость. Например, в кольце $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$ число 2 неприводимо, но не просто, поскольку в фактор кольце

$$\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2, x^2-5) = \mathbb{Z}[x]/(2, x^2+1) \simeq \mathbb{F}_2[x]/(x^2+1) \simeq \mathbb{F}_2[x]/\big((x+1)^2\big)$$

есть делитель нуля $(x+1) \pmod{(2, x^2+1)}$. Это означает, что число $1+\sqrt{5}$ не делится на 2 в $\mathbb{Z}[\sqrt{5}]$, а его квадрат $(1+\sqrt{5})^2 = 6+2\sqrt{5}$ — делится, несмотря на то, что 2 является *неприводимым* элементом кольца $\mathbb{Z}[\sqrt{5}]$.

Упражнение 5.17. Убедитесь, что 2, $\sqrt{5}+1$, $\sqrt{5}-1$ неприводимы и попарно неассоциированы в кольце $\mathbb{Z}[\sqrt{5}]$. Из этого вытекает, в частности, что 4 имеет в $\mathbb{Z}[\sqrt{5}]$ два *различных* разложения на неприводимые множители: $2\cdot 2 = 4 = \left(\sqrt{5}+1\right)\cdot\left(\sqrt{5}-1\right)$.

Предложение 5.5
Целостное нётерово кольцо K факториально тогда и только тогда, когда все его неприводимые элементы просты.

Доказательство. Покажем, что если K факториально, то любой неприводимый элемент $q \in K$ прост. Пусть произведение ab делится на q. Таким образом, разложение ab на неприводимые множители содержит множитель, ассоциированный с q. В силу единственности, разложение произведения ab является произведением разложений a и b. Поэтому q ассоциирован с одним из неприводимых делителей a или b, т. е. a или b делится на q, что и требовалось.

Пусть теперь все неприводимые элементы просты. В нётеровом кольце каждый элемент является произведением конечного числа неприводимых. Покажем, что в любом целостном кольце равенство

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m \,, \tag{5-9}$$

где все сомножители просты, возможно только если $k = m$ и каждый p_i ассоциирован с q_i (может быть, после надлежащей перенумерации). Коль скоро произведение в правой части (5-9) делится на p_1, один из сомножителей этого произведения делится на p_1. Будем считать, что это $q_1 = sp_1$. Поскольку q_1 неприводим, элемент s обратим. Пользуясь целостностью кольца K, сокращаем равенство (5-9) на p_1 и получаем более короткое равенство $p_2 p_3 \cdots p_k = (sq_2)q_3 \cdots q_m$, к которому применимы те же рассуждения. □

Следствие 5.4
Всякое кольцо главных идеалов факториально. □

Пример 5.5 (суммы двух квадратов, продолжение прим. 3.5 на стр. 45)
Согласно упр. 5.13, кольцо гауссовых чисел $\mathbb{Z}[i] \subset \mathbb{C}$ является кольцом главных идеалов, а потому в нём справедлива теорема об однозначности разложения на неприводимые множители. Выясним, какие целые простые числа $p \in \mathbb{Z}$ остаются неприводимыми в кольце

гауссовых чисел. В $\mathbb{Z}[i]$ разложение любого целого вещественного числа, будучи инвариантным относительно комплексного сопряжения, содержит вместе с каждым невещественным неприводимым множителем также и сопряжённый ему множитель. Поэтому простое $p \in \mathbb{Z}$, не являющееся простым в $\mathbb{Z}[i]$, представляется в виде

$$p = (a + ib)(a - ib) = a^2 + b^2 \quad \text{с ненулевыми } a, b \in \mathbb{Z} .$$

Таким образом, простое $p \in \mathbb{Z}$ тогда и только тогда приводимо в $\mathbb{Z}[i]$, когда p является суммой двух квадратов. С другой стороны, неприводимость $p \in \mathbb{Z}[i]$ означает, что фактор кольцо $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)$ является полем[1], что равносильно неприводимости многочлена $x^2 + 1$ над $\mathbb{F}_p$, т. е. отсутствию у него корней в $\mathbb{F}_p$. Мы заключаем, что простое $p \in \mathbb{Z}$ является суммой двух квадратов, если и только если -1 квадратичный вычет по модулю p. Как мы видели в n° 3.5.2 на стр. 48, это происходит в точности тогда, когда $(p - 1)/2$ чётно, т. е. для простых $p = 4k + 1$ и $p = 2$.

Упражнение 5.18. Покажите, что натуральное число n тогда и только тогда является квадратом или суммой двух квадратов натуральных чисел, когда в его разложение на простые множители простые числа $p = 4k + 3$ входят лишь в чётных степенях.

5.4.3. НОД в факториальном кольце. В факториальном кольце K наибольший общий делитель набора элементов $a_1, a_2, \dots , a_m \in K$ допускает следующее описание. Для каждого класса ассоциированных неприводимых элементов $q \in K$ обозначим через m_q максимальное целое число, такое что q^{m_q} делит каждое из чисел a_i. Тогда, с точностью до умножения на обратимые константы,

$$\text{нод}(a_1, a_2, \dots , a_m) = \prod_q q^{m_q} .$$

Так как любой элемент факториального кольца является произведением конечного числа неприводимых, числа m_q отличны от нуля лишь для конечного числа классов q. Поэтому написанное произведение корректно определено и, в силу факториальности K, делится на любой общий делитель чисел a_i.

5.5. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Обозначим через Q_K его поле частных. Кольцо многочленов $K[x]$ является подкольцом в кольце многочленов $Q_K[x]$. Назовём *содержанием* многочлена

$$f = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in K[x]$$

наибольший общий делитель $\operatorname{cont}(f) \stackrel{\text{def}}{=} \text{нод}(a_0, a_1, \dots , a_n)$ его коэффициентов.

Лемма 5.2
$\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$ для любых $f, g \in K[x]$.

Доказательство. Достаточно для каждого неприводимого $q \in K$ убедиться в том, что q делит все коэффициенты произведения fg , если и только если q делит все коэффициенты

[1] см. предл. 5.3 на стр. 76

одного из многочленов f, g. Поскольку неприводимые элементы факториального кольца просты, фактор кольцо $R = K/(q)$ целостное. Применим к произведению fg гомоморфизм

$$K[x] \to R[x]\,, \quad f \mapsto [f]_q\,,$$

редукции по модулю q, заменяющий коэффициенты многочленов на их классы вычетов по модулю q. Так как кольцо $R[x]$ тоже целостное, произведение $[fg]_q = [f]_q[g]_q$ обращается в нуль, если и только если один из сомножителей $[f]_q$, $[g]_q$ равен нулю. □

Лемма 5.3 (редуцированное представление)
Каждый многочлен $f(x) \in Q_K[x]$ представляется в виде $f(x) = \frac{a}{b} \cdot f_{\mathrm{red}}(x)$, где $f_{\mathrm{red}} \in K[x]$, $a, b \in K$, и $\mathrm{cont}(f_{\mathrm{red}}) = \text{нод}(a, b) = 1$, причём числа a, b и многочлен f_{red} определяются по f однозначно с точностью до умножения на обратимые элементы кольца K.

Доказательство. Вынесем из коэффициентов f их общий знаменатель, потом вынесем из всех коэффициентов полученного многочлена их наибольший общий делитель. В результате мы получим многочлен содержания 1, умноженный на число из Q_K, которое запишем несократимой дробью a/b. Докажем единственность такого представления.

Если $(a/b) \cdot f_{\mathrm{red}}(x) = (c/d) \cdot g_{\mathrm{red}}(x)$ в $Q_K[x]$, то $ad \cdot f_{\mathrm{red}}(x) = bc \cdot g_{\mathrm{red}}(x)$ в $K[x]$. Сравнивая содержание обеих частей, получаем $ad = bc$. В виду отсутствия общих неприводимых множителей и у a и b, и у c и d, это возможно, только если a ассоциирован с c, а b — с d. Но тогда с точностью до умножения на обратимую константу и $f_{\mathrm{red}}(x) = g_{\mathrm{red}}(x)$. □

Следствие 5.5 (лемма Гаусса)
Многочлен $f \in K[x]$ содержания 1 неприводим в кольце $Q_K[x]$ тогда и только тогда, когда он неприводим в $K[x]$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ в $Q_K[x]$. Записывая многочлены g и h в редуцированном виде из лем. 5.3 и сокращая возникающую дробь, приходим к равенству

$$f(x) = \frac{a}{b} \cdot g_{\mathrm{red}}(x) \cdot h_{\mathrm{red}}(x)\,,$$

в котором $g_{\mathrm{red}}, h_{\mathrm{red}} \in K[x]$ имеют содержание 1, и $\text{нод}(a, b) = 1$ несократима. По лем. 5.2 содержание произведения $g_{\mathrm{red}}h_{\mathrm{red}}$ также равно 1, так что написанное выше равенство даёт редуцированное представление для многочлена f. В силу его единственности, элементы a и b обратимы в K, а $f = g_{\mathrm{red}}h_{\mathrm{red}}$ с точностью до умножения на обратимую константу. □

Теорема 5.2
Кольцо многочленов над факториальным кольцом факториально.

Доказательство. Так как кольцо главных идеалов $Q_K[x]$ факториально, всякий многочлен $f \in K[x]$ раскладывается в $Q_K[x]$ в произведение неприводимых множителей $f_\nu \in Q_K[x]$. Записывая их в редуцированном виде из лем. 5.3 и сокращая числовую дробь, получаем равенство $f = \frac{a}{b} \prod f_{\nu,\mathrm{red}}$, в котором $f_{\nu,\mathrm{red}} \in K[x]$ — многочлены содержания 1, неприводимые в $Q_K[x]$ (и, тем более, в $K[x]$), а $a, b \in K$ взаимно просты. Поскольку $\mathrm{cont}\left(\prod f_{\nu,\mathrm{red}}\right) = 1$, это равенство даёт редуцированное представление для $f = \mathrm{cont}(f) \cdot f_{\mathrm{red}}$. В силу его единственности, $b = 1$ и $f = a \prod f_{\nu,\mathrm{red}}$ 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 $K[x]$.

Докажем единственность такого разложения. Пусть в $K[x]$ выполняется равенство

$$a_1 a_2 \cdots a_k \cdot p_1 p_2 \cdots p_s = b_1 b_2 \cdots b_m \cdot q_1 q_2 \cdots q_r ,$$

в котором $a_\alpha, b_\beta \in K$ — неприводимые константы, а $p_\mu, q_\nu \in K[x]$ — неприводимые многочлены. Поскольку неприводимые многочлены имеют содержание 1, сравнивая содержание обеих частей, приходим к равенству $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_m$ в K. В силу факториальности K, имеем $k = m$ и (после надлежащей перенумерации сомножителей) $a_i = s_i b_i$, где s_i обратимы. Следовательно, с точностью до умножения на обратимую константу из K в кольце многочленов $K[x]$ выполняется равенство $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$. В силу факториальности $Q_K[x]$ и неприводимости p_i и q_i также и в $Q_K[x]$, мы заключаем, что $r = s$ и (после надлежащей перенумерации сомножителей) $p_i = q_i$ с точностью до постоянного множителя из Q_K. Из единственности редуцированного представления (лем. 5.3) вытекает, что эти постоянные множители являются обратимыми константами из K. □

Следствие 5.6
Если K — факториальное кольцо (скажем, область главных идеалов или поле), то кольцо многочленов $K[x_1, x_2, \dots, x_n]$ от любого числа переменных факториально. □

5.6. Разложение многочленов с целыми коэффициентами. Разложение многочлена $f \in \mathbb{Z}[x]$ на множители в $\mathbb{Q}[x]$ разумно начать с отыскания его рациональных корней, что делается за конечное число проб.

Упражнение 5.19. Покажите, что несократимая дробь $a = p/q \in \mathbb{Q}$ может быть корнем многочлена $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in \mathbb{Z}[x]$, только если p делит a_0, а q делит a_n.

Точное знание комплексных корней f тоже весьма полезно при разложении в $\mathbb{Z}[x]$.

Упражнение 5.20. Разложите $x^4 + 4$ в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

После того, как эти простые соображения исчерпаны, можно попробовать более трудоёмкие способы.

5.6.1. Редукция коэффициентов многочлена $f \in \mathbb{Z}[x]$ по модулю m

$$\mathbb{Z}[x] \to \big(\mathbb{Z}/(m)\big)[x] , \quad f \mapsto [f]_m \tag{5-10}$$

переводит полином $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ с целыми коэффициентами в полином $[a_n]_m x^n + [a_{n-1}]_m x^{n-1} + \dots + [a_1]_m x + [a_0]_m$ с коэффициентами в $\mathbb{Z}/(m)$ и является гомоморфизмом колец[1]. Поэтому равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_m = [g]_n \cdot [h]_m$ во всех кольцах $\big(\mathbb{Z}/(m)\big)[x]$, так что из неприводимости многочлена $[f]_m$ хотя бы при одном m вытекает его неприводимость в $\mathbb{Z}[x]$.

Если число $m = p$ простое, кольцо коэффициентов $\mathbb{Z}/(m) = \mathbb{F}_p$ является полем, и кольцо многочленов $\mathbb{F}_p[x]$ в этом случае факториально. При малых p разложение многочлена небольшой степени на неприводимые множители в $\mathbb{F}_p[x]$ можно осуществить простым перебором, и анализ полученного разложения может дать существенную информацию о возможном разложении в $\mathbb{Z}[x]$.

[1] мы уже пользовались этим в доказательстве лем. 5.2 на стр. 78

Пример 5.6
Покажем, что многочлен $f(x) = x^5 + x^2 + 1$ неприводим в кольце $\mathbb{Z}[x]$. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$. Сделаем редукцию по модулю 2. Так как у $[f]_2 = x^5 + x^2 + 1$ нет корней и в $\mathbb{F}_2$, оба многочлена $[g]_2$, $[h]_2$ неприводимы в $\mathbb{F}_2[x]$. Но единственный неприводимый многочлен второй степени в $\mathbb{F}_2[x]$ это $x^2 + x + 1$, и $x^5 + x^2 + 1$ на него не делится. Тем самым, $[f]_2$ неприводим над $\mathbb{F}_2$, а значит, и над $\mathbb{Z}$.

Пример 5.7 (критерий Эйзенштейна)
Пусть все коэффициенты приведённого многочлена $f \in \mathbb{Z}[x]$ делятся на простое число $p \in \mathbb{N}$, а младший коэффициент, делясь на p, не делится при этом на p^2. Покажем, что f неприводим в $\mathbb{Z}[x]$. В силу сделанных предположений об f при редукции по модулю p от него остаётся только старший моном $[f(x)]_p = x^n$. Если $f(x) = g(x)h(x)$ в $\mathbb{Z}[x]$, то в силу единственности разложения на простые множители в $\mathbb{F}_p[x]$ оба сомножителя g, h тоже должны редуцироваться в чистые степени $[g]_p = x^k$ и $[h]_p = x^m$. Это означает, что все их коэффициенты кроме старшего, делятся на p. Но тогда младший коэффициент f, будучи произведением младших коэффициентов g, h, должен делиться на p^2, что не так.

Пример 5.8 (неприводимость кругового многочлена Φ_p)
Покажем, что круговой многочлен $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x^p - 1)/(x - 1)$ неприводим в $\mathbb{Z}[x]$ при простом p. Для этого перепишем его как многочлен от переменной $t = x - 1$:

$$f(t) = \Phi_p(t+1) = \frac{(t+1)^p - 1}{t} = t^p + \binom{p}{1}t^{p-1} + \cdots + \binom{p}{p-1}t$$

и применим критерий Эйзенштейна из прим. 5.7.

5.6.2. Алгоритм Кронекера позволяет путём эффективного, но довольно трудоёмкого вычисления либо явно найти разложение заданного многочлена с целыми коэффициентами в кольце $\mathbb{Z}[x]$, либо убедиться, что его нет[1]. Пусть $\deg f = 2n$ или $\deg f = 2n+1$. Тогда в любом нетривиальном разложении $f = gh$ в $\mathbb{Z}[x]$ степень одного из делителей, скажем h, не превосходит n. Чтобы выяснить, делится ли f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени $\leqslant n$, достаточно подставить в f любые $n+1$ различных чисел $z_0, z_1, \dots, z_n \in \mathbb{Z}$ и рассмотреть все возможные наборы чисел $d_0, d_1, \dots, d_n$, в которых d_i делит $f(z_i)$. Таких наборов имеется конечное число, и набор значений $h(z_i)$ многочлена h (буде такой многочлен существует) является одним из этих наборов $d_0, d_1, \dots, d_n$. По упр. 3.10 в $\mathbb{Q}[x]$ есть ровно один многочлен степени $\leqslant n$ принимающий значения d_i в точках z_i. Это *интерполяционный многочлен Лагранжа*

$$f_d(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)} \qquad (5\text{-}11)$$

Таким образом, если h существует, то находится среди тех из многочленов (5-11), что имеют целые коэффициенты. Остаётся явно разделить f на все эти многочлены и либо убедиться, что они не делят f, либо найти среди них делитель f.

[1] откуда, по лемме Гаусса, будет следовать, что его нет и в $\mathbb{Q}[x]$

Ответы и указания к некоторым упражнениям

Упр. 5.1. Импликации (а)⇒(б)⇒(в) очевидны. Если $s \in I$ обратим, то среди его кратных есть единица, а среди её кратных — все элементы кольца. Значит, (в)⇒(а).

Упр. 5.2. Первое утверждение очевидно, во втором можно взять $M = I$.

Упр. 5.3. Если a и b являются старшими коэффициентами многочленов $f(x)$ и $g(x)$ из идеала I, причём $\deg f = m$ и $\deg g = n$, где $m \geqslant n$, то $a + b$ либо равно нулю, либо является старшим коэффициентом многочлена $f(x) + x^{m-n} \cdot g(x) \in I$ степени m. Аналогично, для любого $\alpha \in K$ произведение αa является старшим коэффициентом многочлена $\alpha f(x) \in I$ степени m.

Упр. 5.4. Повторите доказательство теор. 5.1, следя за младшими коэффициентами вместо старших.

Упр. 5.6. Обозначим через I_0 идеал, образованный всеми аналитическими функциями[1], обращающимися в нуль на множестве $\mathbb{Z} \subset \mathbb{C}$, а через I_k — идеал всех функций, обращающихся в нуль на множестве $\mathbb{Z} \smallsetminus \{1, 2, \dots, k\}$. Убедитесь, что $\sin(2\pi z)/\prod_{\alpha=1}^{k}(z-\alpha) \in I_k \smallsetminus I_{k-1}$, откуда $I_k \subsetneq I_{k+1}$.

Упр. 5.7. Из того, что I является абелевой подгруппой в K немедленно вытекает, что отношение $a_1 \equiv a_2 \pmod I$ рефлексивно, транзитивно и симметрично. Корректность операций проверяется так же, как в упр. 1.9: если $[a']_I = [a]_I$ и $[b']_I = [b]_I$, т. е. $a' = a + x$, $b' = b + y$ с некоторыми $x, y \in I$, то $a' + b' = a + b + (x + y)$ и $a'b' = ab + (ay + bx + xy)$ сравнимы по модулю I с $a + b$ и ab соответственно, поскольку суммы в скобках лежат в I (именно в этот момент мы пользуемся тем, что идеал вместе с каждым элементом содержит и все его кратные); таким образом, $[a' + b']I = [a + b]_I$ и $[a'b']_I = [ab]_I$.

Упр. 5.8. Рассмотрим эпиморфизм факторизации $\pi : K \twoheadrightarrow K/I$. Полный прообраз $\pi^{-1}(J)$ любого идеала $J \subset K/I$ является идеалом в K. Классы элементов, порождающих этот идеал в K порождают идеал J в K/I.

Упр. 5.9. Всякий идеал в $\mathbb{C}[x]$ является главным. Если фактор кольцо $\mathbb{C}[x]/(f)$ не имеет делителей нуля, то f неприводим. Над полем $\mathbb{C}$ неприводимые многочлены исчерпываются линейными, поэтому $f(x) = x - p$ для некоторого $p \in \mathbb{C}$ и $(f) = (x - p) = \ker \mathrm{ev}_p$. Для ответа на второй вопрос подойдёт главный идеал $\mathfrak{m} = (x^2 + 1)$.

Упр. 5.10. С помощью леммы о конечном покрытии докажите, что для любого идеала I в кольце непрерывных функций $X \to \mathbb{R}$ на произвольном компакте X найдётся точка $p \in X$, в которой все функции из идеала обращаются в нуль, что даёт включение $I \subset \ker \mathrm{ev}_p$.

Упр. 5.12. Рассмотрите сначала случаи, когда пересекаемых (соотв. объединяемых) идеалов всего два, затем воспользуйтесь индукцией.

Упр. 5.14. Если $\exists\, b^{-1}$, то $\nu(ab) \leqslant \nu(abb^{-1}) = \nu(a)$. Наоборот, если $\nu(ab) = \nu(a)$, то деля a на ab с остатком, получаем $a = abq + r$, где либо $\nu(r) < \nu(ab) = \nu(a)$, либо $r = 0$. Из равенства $r = a(1 - bq)$ вытекает, что либо $\nu(r) \geqslant \nu(a)$, либо $1 - bq = 0$. С учётом предыдущего, такое возможно только при $1 - bq = 0$ или $r = 0$. Во втором случае $a(1 - bq) = 0$, что тоже влечёт $1 - bq = 0$. Следовательно $bq = 1$ и b обратим.

[1] функция $\mathbb{C} \to \mathbb{C}$ называется *аналитической*, если она задаётся сходящимся всюду в $\mathbb{C}$ степенным рядом из $\mathbb{C}[\![z]\!]$

Упр. 5.15. Если $b = ax$ и $a = by = axy$, то $a(1 - xy) = 0$, откуда $xy = 1$.

Упр. 5.16. Многочлены x и y не имеют в $\mathbb{Q}[x, y]$ никаких общих делителей, кроме констант. Общими делителями элементов 2 и x в $\mathbb{Z}[x]$ являются только ± 1.

Упр. 5.17. По аналогии с комплексными числами, назовём *сопряжённым* к числу $\vartheta = a+b\sqrt{5}$ число $\overline{\vartheta} = a - b\sqrt{5}$, и будем называть *нормой* числа $\vartheta = a + b\sqrt{5}$ целое число $||\vartheta|| = a^2 - 5b^2 = \vartheta \cdot \overline{\vartheta}$. Легко видеть, что $\overline{\vartheta_1\vartheta_2} = \overline{\vartheta}_1 \cdot \overline{\vartheta}_2$, так что $||\vartheta_1\vartheta_2|| = \vartheta_1\vartheta_2\overline{\vartheta}_1\overline{\vartheta}_2 = ||\vartheta_1|| \cdot ||\vartheta_2||$. Поэтому $\vartheta \in \mathbb{Z}[\sqrt{5}]$ обратим тогда и только тогда, когда $||\vartheta|| = \pm 1$, и в этом случае $\vartheta^{-1} = \pm\overline{\vartheta}$. Поскольку $||2|| = 4$, а $||1 \pm \sqrt{5}|| = -4$, разложение этих элементов в произведение с необратимыми x и y возможно только, если $||x|| = ||y|| = \pm 2$. Однако элементов с нормой ± 2 в $\mathbb{Z}[\sqrt{5}]$ нет, т. к. равенство $a^2 - 5b^2 = \pm 2$ при редукции по модулю 5 превращается в равенство $a^2 = \pm 2$ в поле $\mathbb{F}_5$, где ± 2 не являются квадратами.

Упр. 5.19. Это следует из равенства $a_0q^n + a_1q^{n-1}p + \cdots + a_{n-1}qp^{n-1} + a_np^n = 0$

Упр. 5.20. Ответ: $(x^2 - 2x + 2)(x^2 + 2x + 2)$.