§4. Идеалы, факторкольца и разложение на множители

4.1. Идеалы. Подкольцо I коммутативного кольца K называется *идеалом*, если вместе с каждым своим элементом оно содержит и все его кратные. В n° 1.5.3 мы видели, что этим свойством обладает ядро любого гомоморфизма колец. Множество всех элементов кольца, кратных фиксированному элементу $a \in K$, также является идеалом. Он обозначается

$$(a) = \{ka \mid k \in K\}, \tag{4-1}$$

и называется *главным* идеалом, порождённым a. Главные идеалы использовались нами при построении колец вычетов[1] $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов факторизации $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)$, $m \mapsto [m]_n$, и $\Bbbk[x] \twoheadrightarrow \Bbbk[x]/(f)$, $g \mapsto [g]_f$, переводящих целое число (соотв. многочлен) в класс его вычета. Среди главных идеалов имеются *тривиальный* идеал (0), состоящий только из нулевого элемента, и *несобственный* идеал (1), совпадающий со всем кольцом. Идеалы, отличные от всего кольца, называются *собственными*.

Упражнение 4.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей эквивалентны: а) $I = K$ б) $1 \in I$ в) I содержит обратимый элемент.

Предложение 4.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных собственных идеалов.

Доказательство. Из упр. 4.1 вытекает, что в поле таких идеалов нет. Наоборот, если в кольце нет нетривиальных собственных идеалов, то главный идеал (b), состоящий из всех кратных произвольно взятого элемента $b \neq 0$, совпадает со всем кольцом. В частности, он содержит единицу, т. е. $1 = ab$ для некоторого a. Тем самым, любой ненулевой элемент b обратим. □

4.1.1. Нётеровость. Любое подмножество $M \subset K$ порождает идеал $(M) \subset K$, состоящий из всех элементов кольца K, представимых в виде $b_1a_1 + \ldots + b_ma_m$, где $a_1, \ldots, a_m$ — произвольные элементы множества M, а $b_1, \ldots, b_m$ — произвольные элементы кольца K, и число слагаемых $m \in \mathbb{N}$ также произвольно.

Упражнение 4.2. Убедитесь, что $(M) \subset K$ является идеалом и совпадает с пересечением всех идеалов, содержащих множество M.

Любой идеал $I \subset K$ имеет вид (M) для подходящего множества образующих $M \subseteq I$: например, всегда можно положить $M = I$. Идеалы $I = (a_1, \ldots, a_k) = \{b_1a_1 + \ldots + b_ka_k \mid b_i \in K\}$, допускающие конечное множество образующих, называются *конечно порождёнными*. Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Лемма 4.1
Следующие свойства коммутативного кольца K попарно эквивалентны:

1) любое подмножество $M \subset K$ содержит конечный набор элементов $a_1, \ldots, a_k \in M$, порождающий тот же идеал, что и M

2) любой идеал $I \subset K$ конечно порождён

[1] См. n° 1.4 на стр. 28 и n° 2.3.1 на стр. 43.

3) любая бесконечная возрастающая цепочка вложенных идеалов $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ в K 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) влечёт (2). Чтобы получить (3) из (2), 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 $I_n = (a_1, \ldots, a_n)$, начав с произвольного элемента $a_1 \in M$ и добавляя на k-том шагу очередную образующую $a_k \in M \setminus I_{k-1}$ 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 4.1
Кольцо K, удовлетворяющее условиям лем. 4.1, называется *нётеровым*. Отметим, что любое поле нётерово.

Теорема 4.1 (теорема Гильберта о базисе идеала)
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 не выше d из I, а через $L_\infty = \bigcup_d L_d$ — множество старших коэффициентов вообще всех многочленов из I.

Упражнение 4.3. 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 $f_1^{(d)}, \ldots, f_{m_d}^{(d)} \in K[x]$ многочлены, старшие коэффициенты которых порождают соответствующий идеал $L_d \subset K$. Пусть наибольшая из степеней многочленов $f_i^{(\infty)}$, старшие коэффициенты которых порождают идеал L_∞, равна D. Покажем, что идеал I порождается многочленами $f_i^{(\infty)}$ и $f_j^{(d)}$ с $d < D$.

Каждый многочлен $g \in I$ сравним по модулю многочленов $f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)}$ 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 $\delta_i = \deg g - \deg f_i^{(\infty)} \geqslant 0$, и можно образовать многочлен $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{\delta_i}$, сравнимый с g по модулю I и имеющий $\deg h < \deg g$. Заменяем g на h и повторяем процедуру, пока не получим многочлен $h \equiv g \pmod{(f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)})}$ с $\deg h < D$. Теперь старший коэффициент многочлена h лежит в идеале L_d с $d < D$, и мы можем строго уменьшать его степень, тем же способом сокращая старший член путём вычитания из h подходящих комбинаций многочленов $f_j^{(d)}$ с $0 \leqslant d < D$. □

Следствие 4.1
Если K нётерово, то кольцо многочленов $K[x_1, \ldots, x_n]$ также нётерово. □

Упражнение 4.4. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Следствие 4.2
Любая система полиномиальных уравнений с коэффициентами в нётеровом кольце эквивалентна некоторой конечной своей подсистеме.

Доказательство. Если кольцо K нётерово, то кольцо $K[x_1,\dots,x_n]$ тоже нётерово, и в любом множестве многочленов $M \subset K[x_1,\dots,x_n]$ можно указать такой конечный набор многочленов $f_1,\dots,f_m \in M$, что каждый многочлен $g \in M$ представляется в виде $g = h_1f_1 + \dots + h_mf_m$ для некоторых $h_i \in K[x_1,\dots,x_n]$. Поэтому любое уравнение вида $g(x_1,\dots,x_n) = 0$ с $g \in M$ является следствием m уравнений $f_1(x_1,\dots,x_n) = \dots = f_m(x_1,\dots,x_n) = 0$. □

4.1.2. Примеры ненётеровых колец. Кольцо многочленов от счётного множества переменных $\mathbb{Q}[x_1, x_2, x_3, \dots]$, элементы которого суть конечные линейные комбинации с рациональными коэффициентами всевозможных мономов вида $x_{\nu_1}^{m_1}x_{\nu_2}^{m_2}\dots x_{\nu_s}^{m_s}$ не является нётеровым: его идеал $(x_1, x_2, \dots)$, состоящий из всех многочленов без свободного члена, нельзя породить конечным множеством многочленов.

Упражнение 4.5. 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 4.1. Подкольцо нётерова кольца может не быть нётеровым. Например, кольцо формальных степенных рядов $\mathbb{C}[\![z]\!]$ нётерово по упр. 4.4, тогда как его подкольцо образованное рядами, сходящимися всюду в $\mathbb{C}$, нётеровым не является.

Упражнение 4.6. Приведите пример бесконечной возрастающей цепочки строго вложенных идеалов в кольце сходящихся всюду в $\mathbb{C}$ степенных рядов из $\mathbb{C}[\![x]\!]$.

4.2. Факторкольца. Пусть на коммутативном кольце K задано отношение эквивалентности, разбивающее K в дизъюнктное объединение классов эквивалентных элементов. Обозначим множество классов через X и рассмотрим сюръективное отображение факторизации

$$\pi : K \twoheadrightarrow X, \quad a \mapsto [a], \tag{4-2}$$

переводящее элемент $a \in K$ в его класс эквивалентности $[a] \subset K$, являющийся элементом множества X. Мы хотим задать на множестве X структуру коммутативного кольца, определив сложение и умножение теми же сами правилами

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab], \tag{4-3}$$

которые мы использовали в кольцах вычетов. Если эти правила корректны, то аксиомы коммутативного кольца в X будут автоматически выполнены, как и для колец вычетов, поскольку формулы (4-3) сводят их проверку к проверке аксиом коммутативного кольца в K. В частности, нулевым элементом кольца X будет класс $[0]$. С другой стороны, если формулы (4-3) корректны, то они утверждают, что отображение (4-2) является гомоморфизмом колец. Но если это так, то согласно n° 1.5.3 на стр. 31 класс нуля $[0] = \ker\pi$, служащий ядром этого гомоморфизма, является идеалом в K, а класс $[a] \subset K$ произвольного элемента $a \in K$, служащий прообразом точки $[a] \in X$ при гомоморфизме (4-2), является аддитивным сдвигом ядра на элемент a:

$$[a] = \pi^{-1}(\pi(a)) = a + \ker\pi = a + [0] = \{a + b \mid b \in [0]\}.$$

Оказывается, что этих необходимых условий на классы также и достаточно для того, чтобы правила (4-3) были корректны, т. е. для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{4-4}$$

образует разбиение кольца K, и правила (4-3) корректно определяют на классах этого разбиения структуру коммутативного кольца с нулевым элементом $[0]_I = I$.

Упражнение 4.7. 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, и проверьте, что формулы (4-3) корректны.

Определение 4.2
Классы эквивалентности (4-4) называются *классами вычетов* (или *смежными классами*) по модулю идеала I. Множество этих классов с операциями (4-3) называется *факторкольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм $K \twoheadrightarrow K/I$, $a \mapsto [a]_I$, сопоставляющий каждому элементу кольца его класс вычетов, называется *гомоморфизмом факторизации*.

Пример 4.1 (кольца вычетов)
Рассматривавшиеся выше кольца $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$ суть факторы кольца целых числел и кольца многочленов по главным идеалам $(n) \subset \mathbb{Z}$ и $(f) \subset \Bbbk[x]$ соответственно.

Пример 4.2 (образ гомоморфизма)
Согласно n° 1.5.3, для любого гомоморфизма коммутативных колец $\varphi : A \to B$ имеется канонический изоморфизм колец $\overline{\varphi} : A/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$, $[a]_{\ker\varphi} \mapsto \varphi(a)$, переводящий каждый класс

$$[a]_{\ker\varphi} = a + \ker\varphi = \varphi^{-1}(\varphi(a))$$

в его образ $\varphi(a) = \varphi([a])$ при гомоморфизме φ.

Пример 4.3 (максимальные идеалы и гомоморфизмы вычисления)
Идеал $\mathfrak{m} \subset K$ называется *максимальным*, если факторкольцо $K/\mathfrak{m}$ является полем. Название связано с тем, что собственный[1] идеал $\mathfrak{m} \subset K$ максимален, если и только если он не содержится ни в каком строго большем собственном идеале, т. е. является максимальным элементом в чуме[2] собственных идеалов кольца K, частично упорядоченных по включению. В самом деле, обратимость всех ненулевых классов $[a]_{\mathfrak{m}}$ в факторкольце $K/\mathfrak{m}$ означает, что для любого $a \notin \mathfrak{m}$ найдутся такие $b \in K$, $m \in \mathfrak{m}$, что $ab + m = 1$ в K. Последнее равносильно тому, что идеал $(\mathfrak{m}, a) \supsetneq \mathfrak{m}$, порождённый $\mathfrak{m}$ и элементом $a \notin \mathfrak{m}$, содержит 1 и совпадает с K, т. е. что идеал $\mathfrak{m}$ не содержится ни в каком строго большем собственном идеале.

Из леммы Цорна[3] вытекает, что любой собственный идеал произвольного коммутативного кольца с единицей содержится в некотором максимальном идеале. В самом деле, множество всех собственных идеалов, содержащих произвольно заданный идеал $I \subset K$, тоже составляет чум по включению.

Упражнение 4.8. Убедитесь, что он полный, т. е. для любого линейно упорядоченного множества[4] M содержащих I собственных идеалов в K существует собственный идеал J^*, содержащий все идеалы из M.

[1] Т. е. отличный от всего кольца.
[2] См. n° 0.7 на стр. 16.
[3] См. сл. 0.1 на стр. 20.
[4] В данном случае это означает, что для любых $J_1, J_2 \in M$ выполняется включение $J_1 \subseteq J_2$ или включение $J_2 \subseteq J_1$.

По лемме Цорна существует такой собственный идеал $\mathfrak{m} \supset I$, который не содержится ни в каком большем собственном идеале, содержащем I. Такой идеал $\mathfrak{m}$ автоматически максимален по включению и в чуме всех собственных идеалов кольца K.

Максимальные идеалы возникают в кольцах функций как ядра *гомоморфизмов вычисления*. А именно, пусть X — произвольное множество, $p \in X$ — любая точка, $\Bbbk$ — любое поле, и K — какое-нибудь 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 $f(p) \in \Bbbk$. Поскольку он сюръективен, его ядро $\ker \mathrm{ev}_p = \{f \in K \mid f(p) = 0\}$ является максимальным идеалом в K.

Упражнение 4.9. Убедитесь, что: а) каждый максимальный идеал кольца $\mathbb{C}[x]$ имеет вид $\ker \mathrm{ev}_p$ для некоторого $p \in \mathbb{C}$ б) в кольце непрерывных функций $[0,1] \to \mathbb{R}$ каждый максимальный идеал имеет вид $\ker \mathrm{ev}_p$ для некоторой точки $p \in [0,1]$. в) Укажите в кольце $\mathbb{R}[x]$ максимальный идеал, отличный от всех идеалов вида $\ker \mathrm{ev}_p$, где $p \in \mathbb{R}$.

Пример 4.4 (простые идеалы и гомоморфизмы в поля)
Идеал $\mathfrak{p} \subset K$ называется *простым*, если в факторкольце $K/\mathfrak{p}$ 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 4.10. Убедитесь в этом.

Согласно определениям, всякий максимальный идеал прост. Обратное неверно: скажем, главный идеал $(x) \subset \mathbb{Q}[x,y]$ прост, так как кольцо $\mathbb{Q}[x,y]/(x) \simeq \mathbb{Q}[y]$ целостное, но не максимален, поскольку строго содержится в идеале (x,y) многочленов без свободного члена[1]. 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, факторкольцо $K/\mathfrak{p}$ по простому идеалу $\mathfrak{p} \subset K$ 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 4.11. Убедитесь, что пересечение конечного множества идеалов содержится в простом идеале $\mathfrak{p}$ только если хотя бы один из пересекаемых идеалов содержится в $\mathfrak{p}$.

Пример 4.5 (конечно порождённые коммутативные алгебры)
Пусть K — произвольное коммутативное кольцо с единицей. Всякое кольцо вида

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

где $I \subset K[x_1, \dots, x_n]$ — произвольный идеал, называется *конечно порождённой K-алгеброй*[2]. Классы $a_i = [x_i]_I$ называются *образующими* K-алгебры A, а многочлены $f \in I$ — *соотношениями* между этими образующими. Говоря неформально, K-алгебра состоит из всевозможных выражений, которые можно составить из элементов кольца K и коммутирующих букв $a_1, \dots, a_n$

[1] Т. е. в ядре гомоморфизма вычисления в нуле: $\mathrm{ev}_{(0,0)} : \mathbb{Q}[x,y] \twoheadrightarrow \mathbb{Q}$, $f(x,y) \mapsto f(0,0)$.

[2] Или, более торжественно, *конечно порождённой коммутативной алгеброй* над кольцом K.

при помощи операций сложения и умножения, производимых с учётом полиномиальных соотношений $f(a_1, \dots, a_n) = 0$ для всех f из I. Из сл. 4.1 и идущего следом упр. 4.12:

Упражнение 4.12. Покажите, что факторкольцо нётерова кольца тоже нётерово.

мы получаем

Следствие 4.3
Всякая конечно порождённая коммутативная алгебра над нётеровым коммутативным кольцом нётерова, и все соотношения между её образующими являются следствиями конечного числа соотношений. □

4.3. Области главных идеалов. Целостное кольцо с единицей называется *областью главных идеалов*, если каждый его идеал является главным. Наблюдавшийся нами в §§ 1, 2 параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, объясняется тем, что оба кольца являются областями главных идеалов. Мы фактически установили это при построении наибольших общих делителей[1]. Ключевым элементом наших рассуждений было *деление с остатком*.

Пример 4.6 (евклидовы кольца)
Целостное кольцо K с единицей называется *евклидовым*, если на нём имеется *функция высоты*

$$\nu : K \to \mathbb{Z}_{\geqslant 0} = \mathbb{N} \cup \{0\},$$

с двумя свойствами: (1) $\nu(a) = 0 \iff a = 0$; (2) для любых ненулевых $a, b \in K$ найдётся такое $q \in K$, что $\nu(a - bq) < \nu(b)$. Все такие q называются *неполными частными*, а соответствующие разности $r = a - bq$ — *остатками* от деления a на b относительно высоты ν. Подчеркнём, что никакой их единственности для заданных a, b не предполагается. В каждом ненулевом идеале I евклидова кольца K имеется ненулевой элемент $d \in I$ наименьшей в I высоты. Поскольку для любого $a \in I$ найдётся такое $q \in K$, что $\nu(a - dq) < \nu(d)$, и при этом $a - dq \in I$, мы заключаем, что $a - dq = 0$ и, тем самым, $I = (d)$. Поэтому каждое евклидово кольцо K является областью главных идеалов.

Упражнение 4.13. Докажите евклидовость колец: а) $\mathbb{Z}$ с $\nu(z) = |z|$
б) $\Bbbk[x]$, где $\Bbbk$ — поле, с $\nu(f) = 2^{\deg f}$ при $f \neq 0$ и $\nu(0) = 0$
в) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z},\ i^2 = -1 \}$ с $\nu(z) = |z|^2$
г) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\}$ с $\nu(z) = |z|^2$.

Функцию высоты $\nu : K \to \mathbb{Z}_{\geqslant 0}$ на любом евклидовом кольце K всегда можно выбрать так, чтобы для всех $a \in K$ и всех ненулевых $b \in K$ выполнялось дополнительное свойство $\nu(ab) \geqslant \nu(a)$. Для этого, задавшись какой-нибудь высотой ν', для всех $a \in K$ положим

$$\nu(a) = \min\nolimits_{x \in K \setminus 0} \nu'(ax).$$

Тогда по построению $\nu(ab) \geqslant \nu(a)$ для всех $a \in K$ и всех ненулевых $b \in K$. Очевидно, что $\nu(a) = 0$, если и только если $a = 0$. Убедимся, что ν обладает и вторым свойством евклидовой высоты. Пусть $\nu(b) = \nu'(bc)$ для ненулевого $c \in K$. Поскольку существует такое $q \in K$, что $\nu'(ac - bcq) < \nu'(bc)$, мы заключаем, что $\nu(a - bq) \leqslant \nu'\big((a - bq)c\big) < \nu'(bc) = \nu(b)$, как и требовалось. Высота ν со свойством $\nu(ab) \geqslant \nu(a)$ для всех ненулевых $b \in K$ называется *приведённой*.

Упражнение 4.14. Покажите, что в евклидовом кольце с приведённой высотой ν равенство $\nu(ab) = \nu(a)$ выполняется для ненулевых a, b, если и только если b обратим.

[1] См. n° 1.2.1 на стр. 24 и предл. 2.3 на стр. 41.

Существуют области главных идеалов, не являющиеся евклидовыми кольцами. Например, таковым является кольцо всех чисел вида $a + b\zeta \in \mathbb{C}$, где $a, b \in \mathbb{Z}$, а $\zeta = (1 + \sqrt{-19})/2$, однако содержательное обсуждение этого примера выходит за рамки понятий, которыми мы пока владеем. В прим. 4.7 на стр. 75 будет дана характеризация областей главных идеалов в терминах высот с немного более слабыми свойствами, чем у евклидовой высоты.

4.3.1. НОД и взаимная простота. В кольце главных идеалов K идеал

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

порождённый любым набором элементов $a_1, \dots, a_n$, является главным и имеет вид (d) для некоторого $d \in K$. Таким образом, элемент d представляется в виде $d = a_1b_1 + \dots + a_nb_n$, где $b_i \in K$, делит все элементы a_i и делится на любой общий делитель элементов a_i, т. е. является *наибольшим общим делителем*[1] элементов $a_1, \dots, a_n$. Отметим, что наибольший общий делитель определён не однозначно, а с точностью до умножения на произвольный обратимый элемент из K.

Упражнение 4.15. Убедитесь, что в любом целостном коммутативном кольце K главные идеалы (a) и (b) совпадают, если и только если $a = sb$ для некоторого обратимого $s \in K$.

Поэтому всюду далее обозначение нод$(a_1, \dots, a_n)$ подразумевает целый класс элементов, получающихся друг из друга умножениями на обратимые константы, и все формулы, которые будут писаться, относятся к произвольно выбранному конкретному представителю этого класса[2]. В частности, равенство нод$(a_1, \dots, a_n) = 1$ означает, что у элементов a_i нет необратимых общих делителей. Так как в этом случае $1 = a_1b_1 + \dots + a_nb_n$ с $b_i \in K$, отсутствие необратимых общих делителей у элементов a_i в кольце главных идеалов равносильно их *взаимной простоте* в смысле опр. 1.2 на стр. 27.

Упражнение 4.16. Проверьте, что идеалы $(x, y) \subset \mathbb{Q}[x, y]$ и $(2, x) \in \mathbb{Z}[x]$ не являются главными.

4.4. Факториальность. Всюду в этом разделе мы по умолчанию обозначаем через K *целостное* кольцо. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b или, что то же самое, если $(a) = (b)$. Из упр. 4.15 выше вытекает, что a и b ассоциированы, если и только если они получаются друг из друга умножением на обратимый элемент кольца. Например, целые числа a и b ассоциированы в кольце $\mathbb{Z}$, если и только если $a = \pm b$, а многочлены $f(x)$ и $g(x)$ с коэффициентами из поля $\Bbbk$ ассоциированы в $\Bbbk[x]$, если и только если $f(x) = cg(x)$, где $c \in \Bbbk^*$ — ненулевая константа.

4.4.1. Неприводимые элементы. Ненулевой необратимый элемент q называется *неприводимым*, если из равенства $q = mn$ вытекает, что m или n обратим. Другими словами, неприводимость элемента q означает, что главный идеал (q) собственный и не содержится строго ни в каком другом собственном главном идеале, т. е. максимален в частично упорядоченном отношением включения множестве собственных главных идеалов. Неприводимыми элементами в кольце $\mathbb{Z}$ являются простые числа, а в кольце $\Bbbk[x]$, где $\Bbbk$ — поле, — неприводимые многочлены.

В кольце главных идеалов любые два неприводимых элемента p, q либо взаимно просты[3], либо ассоциированы, поскольку идеал $(p, q) = (d)$ для некоторого $d \in K$, и в виду максимальности (p) и (q) включения $(p) \subset (d)$ и $(q) \subset (d)$ влекут либо равенство $(d) = (K) = (1)$, либо равенство $(d) = (p) = (q)$. Обратите внимание, что в произвольном целостном кольце два

[1] См. зам. 1.3. на стр. 27.

[2] Что, конечно же, требует проверки корректности всех таких формул, которую мы, как правило, будем оставлять читателю в качестве упражнения.

[3] В смысле опр. 1.2 на стр. 27, т. е. существуют такие $x, y \in K$, что $px + qy = 1$.

неассоциированных неприводимых элемента могут и не быть взаимно простыми. Например, в $\mathbb{Q}[x, y]$ неприводимые многочлены x и y не взаимно просты и не ассоциированы.

Предложение 4.2
В кольце главных идеалов K следующие свойства ненулевого элемента $p \in K$ эквивалентны:

1) идеал (p) максимален, т. е. факторкольцо $K/(p)$ является полем

2) идеал (p) прост, т. е. в факторкольце $K/(p)$ нет делителей нуля

3) p неприводим, т. е. из равенства $p = ab$ вытекает, что a или b обратим в K.

Доказательство. Импликация (1) $\Rightarrow$ (2) очевидна и имеет место в любом коммутативном кольце с единицей. Импликация (2) $\Rightarrow$ (3) имеет место в любом целостном кольце K. Действительно, из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и так как в $K/(p)$ нет делителей нуля, один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, откуда $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим.

Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Так как каждый собственный идеал в K главный, максимальность идеала (p) в чуме собственных главных идеалов означает его максимальность в чуме всех собственных идеалов. В прим. 4.3 на стр. 70 мы видели, что это равносильно тому, что $K/(p)$ поле. □

Предложение 4.3
Каждый ненулевой необратимый элемент целостного нётерова кольца 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 $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$, что противоречит нётеровости. □

Определение 4.3
Целостное кольцо K называется *факториальным*, если каждый его необратимый ненулевой элемент является произведением конечного числа неприводимых, причём любые два таких разложения $p_1 \ldots p_m = q_1 \ldots q_k$ состоят из одинакового числа $k = m$ сомножителей, и после надлежащей их перенумерации можно указать такие обратимые $s_\nu \in K$, что $q_\nu = p_\nu s_\nu$ при всех ν.

4.4.2. Простые элементы. Ненулевой элемент $p \in K$ называется *простым*, если порождённый им главный идеал $(p) \subset K$ прост, т. е. в факторкольце $K/(p)$ нет делителей нуля. Это означает, что для любых $a, b \in K$ произведение ab делится на p только если a или b делится на p. Каждый 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. 4.2 в кольце главных идеалов верно и обратное: все неприводимые элементы кольца главных идеалов просты. Однако в произвольном целостном кольце могут быть неприводимые непростые

элементы. Например, в кольце $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$ таковым является число 2, так как в факторе $\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2, x^2-5) = \mathbb{Z}[x]/(2, x^2+1) \simeq \mathbb{F}_2[x]/(x^2+1) \simeq \mathbb{F}_2[x]/\left((x+1)^2\right)$ есть нильпотент — класс $[x+1] \in \mathbb{Z}[x]/(2, x^2+5)$. Среди прочего это означает, что квадрат $(1+\sqrt{5})^2 = 6+2\sqrt{5}$ делится в кольце $\mathbb{Z}[\sqrt{5}]$ на 2, хотя $1+\sqrt{5}$ не делится на 2, при том что 2 и $\sqrt{5}+1$ неприводимы и не ассоциированы друг с другом в кольце $\mathbb{Z}[\sqrt{5}]$.

Упражнение 4.17. Убедитесь в этом, и покажите, что $2 \cdot 2 = 4 = \left(\sqrt{5}+1\right) \cdot \left(\sqrt{5}-1\right)$ суть два *различных* разложения числа 4 на неприводимые множители в $\mathbb{Z}[\sqrt{5}]$.

Предложение 4.4
Целостное нётерово кольцо K факториально, если и только если все его неприводимые элементы просты.

Доказательство. Покажем сначала, что если K факториально, то любой неприводимый элемент $q \in K$ прост. Пусть произведение ab делится на q. Тогда разложение ab на неприводимые множители содержит множитель, ассоциированный с q, и в силу своей единственности является произведением разложений a и b на неприводимые множители. Поэтому q ассоциирован с одним из неприводимых делителей a или b, т. е. a или b делится на q. Наоборот, пусть все неприводимые элементы в K просты. Тогда по предл. 4.3 на стр. 74 каждый элемент кольца K является произведением конечного числа простых. Покажем, что в целостном кольце равенство $p_1 \dots p_k = q_1 \dots q_m$, в котором все сомножители просты, возможно только если $k = m$ и после надлежащей перенумерации каждый $p_i = s_i q_i$, где s_i обратим. Поскольку произведение $q_1 \dots q_m$ делится на p_1, один из его сомножителей делится на p_1. Будем считать, что это $q_1 = sp_1$. Так как q_1 неприводим, элемент s обратим. Пользуясь целостностью K, сокращаем обе части равенства $p_1 \dots p_k = q_1 \dots q_m$ на p_1 и получаем более короткое равенство $p_2 p_3 \dots p_k = (sq_2)q_3 \dots q_m$, к которому применимы те же рассуждения. □

Следствие 4.4
Всякое кольцо главных идеалов факториально. □

Пример 4.7 (характеризация областей главных идеалов, продолжение прим. 4.6 на стр. 72)
Покажем, что целостное кольцо K является областью главных идеалов, если и только если на K имеется функция высоты $\nu : K \to \mathbb{Z}_{\geqslant 0} = \mathbb{N} \cup \{0\}$ со следующими двумя свойствами:

1) $\nu(a) = 0 \iff a = 0$; 2) если $a \notin (b)$, то найдутся $x, y \in K$ с $0 < \nu(ax+by) < \nu(b)$.

Действительно, пусть такая высота существует. Тогда в каждом идеале $I \subset K$ есть ненулевой элемент $d \in I$, на котором ν принимает наименьшее в I ненулевое значение. Если $a \in I \smallsetminus (d)$, то найдутся $x, y \in K$ с $0 < \nu(ax+dy) < \nu(d)$, что невозможно, ибо $ax+dy \in I$. Тем самым $I = (d)$ и K является областью главных идеалов. Наоборот, пусть K — область главных идеалов. Выберем в каждом классе ассоциированных простых элементов какого-нибудь представителя p и для каждого $a \in K$ обозначим через $\nu_p(a)$ показатель, с которым p входит в разложение a на простые множители: $a = \prod_p p^{\nu_p(a)}$. Положим $\nu(a) = 2^{\sum_p \nu_p(a)}$. Так как $\nu_p(a) = 0$ для всех p кроме конечного числа, это определение корректно. Если $b \nmid a$, то нод$(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}$ имеет положительную высоту, строго меньшую, чем $\nu(b)$, и представляется в виде $ax+by$, что и требуется. Более того, построенная высота ν *приведена* в том смысле[1], что $\nu(a) \leqslant \nu(ab)$ для всех a и всех ненулевых b, причём равенство равносильно обратимости b.

[1] Ср. с прим. 4.6 на стр. 72.

Пример 4.8 (гауссовы числа и суммы двух квадратов)
Элементы кольца $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1) \simeq \{x+iy \in \mathbb{C} \mid x,y \in \mathbb{Z}\}$ из упр. 4.13 (в) на стр. 72 называются *целыми гауссовыми числами*.

Упражнение 4.18. Убедитесь, что: а) в $\mathbb{Z}[i]$ обратимы только ± 1 и $\pm i$ б) $z \in \mathbb{Z}$ прост, если и только если прост $\overline{z}$.

Из упражнения вытекает, что разложение вещественного целого числа $n \in \mathbb{Z}$ на простые множители в области $\mathbb{Z}[i]$, будучи инвариантным относительно комплексного сопряжения, вместе с каждым невещественным неприводимым множителем содержит и его сопряжённый. Поэтому вещественное простое $p \in \mathbb{Z}$ становится приводимым в $\mathbb{Z}[i]$, если и только если оно имеет вид $p = (a+ib)(a-ib) = a^2+b^2$ с ненулевыми $a, b \in \mathbb{Z}$. С другой стороны, неприводимость $p \in \mathbb{Z}[i]$ означает, что факторкольцо $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)$ является полем[1], что равносильно неприводимости многочлена x^2+1 над $\mathbb{F}_p$. Последнее равносильно тому, что -1 не является квадратом в $\mathbb{F}_p$, и имеет место если и только если[2] $p = 4k+3$. Мы заключаем, что неприводимость простого $p \in \mathbb{Z}$ в области $\mathbb{Z}[i]$ равносильна тому, что $p = 4k+3$, и тому, что p не представляется в виде суммы двух квадратов целых чисел.

Упражнение 4.19. Покажите, что произвольное $n \in \mathbb{N}$ является квадратом или суммой двух квадратов натуральных чисел, если и только если в его разложении на простые множители в кольце $\mathbb{Z}$ простые числа $p = 4k+3$ присутствуют только в чётных степенях.

4.4.3. НОД в факториальном кольце. В любом факториальном кольце K у любого конечного набора чисел $a_1, \ldots, a_m \in K$ имеется наибольший общий делитель[3]. Он имеет следующее явное описание. Зафиксируем в каждом классе ассоциированных простых элементов кольца K некоторый представитель p и для каждого $a \in K$ обозначим через $\nu_p(a) \in \mathbb{Z}_{\geqslant 0}$ показатель, с которым p входит в разложение a на простые множители[4], как в прим. 4.7 выше. Тогда, с точностью до умножения на обратимые элементы, $\text{нод}(a_1, \ldots, a_m) = \prod_p p^{\min_i \nu_p(a_i)}$.

Упражнение 4.20. Убедитесь, что правая часть делит каждое a_i и делится на любой общий делитель всех a_i.

Отметим, что если K не является областью главных идеалов, то $\text{нод}(a_1, \ldots, a_m)$ может не представляться в виде линейной комбинации элементов a_i с коэффициентами из K. Например, элементы x, y факториального кольца[5] $\mathbb{Q}[x,y]$ имеют $\text{нод}(x,y) = 1$, но нет таких $f, g \in \mathbb{Q}[x,y]$, что $fx+gy = 1$, ибо подставляя в это равенство $x = y = 0$, получим $0 = 1$.

4.5. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Обозначим через Q_K его поле частных. Кольцо $K[x]$ является подкольцом в $Q_K[x]$. Назовём *содержанием* многочлена $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ наибольший общий делитель его коэффициентов:

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

Лемма 4.2
$\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$ для любых $f, g \in K[x]$.

[1] См. предл. 4.2 на стр. 74.
[2] См. прим. 1.8 на стр. 31.
[3] В смысле зам. 1.3. на стр. 27, т. е. число, которое делит все a_i и делится на любой их общий делитель.
[4] Обратите внимание, что для каждого a показатель $\nu_p(a) \neq 0$ только для конечного множества простых чисел p.
[5] См. сл. 4.6 на стр. 78.

Доказательство. Достаточно для каждого простого $q \in K$ убедиться в том, что q делит все коэффициенты произведения fg, если и только если q делит все коэффициенты хотя бы одного из многочленов f, g. Для этого положим $R = K/(q)$ и применим к произведению fg гомоморфизм

$$K[x] \to R[x], \quad a_0 + a_1 x + \ldots + a_n x^n \mapsto [a_0]_q + [a_1]_q x + \ldots + [a_n]_q x^n,$$

заменяющий коэффициенты каждого многочлена их вычетами по модулю q.

Упражнение 4.21. Проверьте, что это и в самом деле гомоморфизм колец.

В силу простоты q кольцо R целостное. Поэтому $R[x]$ тоже целостное, и $[fg]_q = [f]_q[g]_q = 0$, если и только если $[f]_q = 0$ или $[g]_q = 0$. □

Лемма 4.3 (приведённое представление)
Каждый $f \in Q_K[x]$ представляется в виде $f(x) = (a/b) \cdot f_{\text{red}}(x)$, где $f_{\text{red}} \in K[x]$, $a, b \in K$ и $\text{cont}(f_{\text{red}}) = \text{нод}(a, b) = 1$, причём a, b и 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 $(a/b) \cdot f_{\text{red}}(x) = (c/d) \cdot g_{\text{red}}(x)$ в $Q_K[x]$, то $ad \cdot f_{\text{red}}(x) = bc \cdot g_{\text{red}}(x)$ в $K[x]$. Сравнивая содержание обеих частей, заключаем, что $ad = bc$, откуда $f_{\text{red}}(x) = g_{\text{red}}(x)$. В виду отсутствия общих неприводимых множителей у a и b и у c и d, равенство $ad = bc$ возможно лишь когда a ассоциирован с c, а b — с d. □

Следствие 4.5 (лемма Гаусса)
Многочлен $f \in K[x]$ содержания 1 неприводим в $Q_K[x]$, если и только если он неприводим в $K[x]$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ в $Q_K[x]$. Записывая многочлены g и h в приведённом виде из лем. 4.3 и сокращая возникающую дробь, приходим к равенству

$$f(x) = \frac{a}{b} \cdot g_{\text{red}}(x) \cdot h_{\text{red}}(x), \tag{4-5}$$

в котором $g_{\text{red}}, h_{\text{red}} \in K[x]$ имеют содержание 1, и $\text{нод}(a, b) = 1$. По лем. 4.2

$$\text{cont}(g_{\text{red}} h_{\text{red}}) = \text{cont}(g_{\text{red}}) \cdot \text{cont}(h_{\text{red}}) = 1,$$

т. е. правая часть в (4-5) является приведённым представлением многочлена f. В силу единственности приведённого представления элементы a и b обратимы в K, а $f = g_{\text{red}} h_{\text{red}}$ с точностью до умножения на обратимую константу. □

Теорема 4.2
Кольцо многочленов над факториальным кольцом факториально.

Доказательство. Будучи кольцом главных идеалов, кольцо $Q_K[x]$ факториально, и каждый многочлен $f \in K[x] \subset Q_K[x]$ раскладывается в $Q_K[x]$ в произведение неприводимых множителей $f_\nu \in Q_K[x]$. Записывая их в приведённом виде из лем. 4.3 и сокращая возникающую при этом числовую дробь, получаем равенство $f = \frac{a}{b} \prod f_{\nu,\text{red}}$, в котором $a, b \in K$ имеют $\text{нод}(a, b) = 1$, а

все $f_{\nu,\mathrm{red}} \in K[x]$ неприводимы в $Q_K[x]$ и $\mathrm{cont}(f_{\nu,\mathrm{red}}) = 1$. Тогда $\mathrm{cont}\left(\prod f_{\nu,\mathrm{red}}\right) = 1$ по лем. 4.3, и правая часть равенства является приведённым представлением многочлена $f = \mathrm{cont}(f) \cdot f_{\mathrm{red}}$. В силу единственности приведённого представления $b = 1$ 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 $K[x]$

$$a_1 \dots a_k \cdot p_1 \dots p_s = b_1 \dots b_m \cdot q_1 \dots q_r\,,$$

где $a_\alpha, b_\beta \in K$ — 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 $a_1 \dots a_k = b_1 \dots b_m$ в K. Так как K факториально, мы заключаем, что $k = m$ и после надлежащей перенумерации сомножителей $a_i = s_i b_i$, где все $s_i \in K$ обратимы. Следовательно, с точностью до умножения на обратимую константу из K, в кольце $K[x]$ выполняется равенство $p_1 \dots p_s = q_1 \dots q_r$. Так как все p_i и q_i неприводимы в факториальном кольце $Q_K[x]$, мы заключаем, что $r = s$ и после надлежащей перенумерации сомножителей $p_i = q_i$ с точностью до постоянных множителей из поля Q_K. Из единственности приведённого представления[1] вытекает, что эти постоянные множители являются обратимыми константами из кольца K. □

Следствие 4.6
Кольцо многочленов $K[x_1, \dots, x_n]$ над факториальным кольцом[2] K факториально. □

4.6. 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 4.22. Покажите, что несократимая дробь $p/q \in \mathbb{Q}$ является корнем многочлена $a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ только если $p \mid a_0$ и $q \mid a_n$.

Точное знание комплексных корней многочлена f тоже весьма полезно.

Упражнение 4.23. Разложите $x^4 + 4$ в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

После того, как эти простые соображения будут исчерпаны, следует подключать более трудоёмкие способы.

4.6.1. Редукция коэффициентов $\mathbb{Z}[x] \to \mathbb{Z}/(m)\,[x]$, $f \mapsto [f]_m$, где

$$[f]_m \stackrel{\text{def}}{=} [a_0]_m + [a_1]_m x + \dots [a_n]_m x^n \text{ для } f = a_0 + a_1 x + \dots + a_n x^n\,, \tag{4-6}$$

приводит коэффициенты всех многочленов по модулю m и является гомоморфизмом колец[3]. Поэтому равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_m = [g]_n \cdot [h]_m$ во всех кольцах $\big(\mathbb{Z}/(m)\big)[x]$, и 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 такого разложения может дать существенную информацию о возможном разложении в $\mathbb{Z}[x]$.

[1] См. лем. 4.3 на стр. 77.
[2] В частности, над полем или над областью главных идеалов.
[3] Мы уже пользовались этим в доказательстве лем. 4.2 на стр. 76, см. упр. 4.21.

Пример 4.9
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 4.10 (критерий Эйзенштейна)
Пусть все за исключением старшего 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 об f предположений при редукции по модулю p от f 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 редуцируются в некоторые степени переменной: $[g]_p = x^k$ и $[h]_p = x^m$. Это означает, что все коэффициенты многочленов g и h кроме старшего делятся на p. Тогда младший коэффициент многочлена f, будучи произведением младших коэффициентов многочленов g и h, должен делиться на p^2, что не так.

Пример 4.11 (неприводимость кругового многочлена Φ_p)
Покажем, что при простом $p \in \mathbb{N}$ круговой многочлен $\Phi_p(x) = x^{p-1} + \ldots + x + 1 = (x^p - 1)/(x - 1)$ неприводим в $\mathbb{Z}[x]$. Для этого перепишем его как многочлен от переменной $t = x - 1$:

$$f(t) = \Phi_p(t+1) = (t+1)^p - 1 / t = t^{p-1} + \binom{p}{1} t^{p-2} + \ldots + \binom{p}{p-1}.$$

Поскольку при простом p все биномиальные коэффициенты $\binom{p}{k}$ с $1 \leqslant k \leqslant p-1$ делятся[1] на p, а свободный член $\binom{p}{p-1} = p$ не делится на p^2, многочлен $f(t)$ неприводим по критерию Эйзенштейна из прим. 4.10. Поэтому и $\Phi_p(x) = f(x-1)$ неприводим.

4.6.2. Алгоритм Кронекера позволяет путём довольно трудоёмкого, но вполне конечного вычисления либо явно разложить многочлен $f \in \mathbb{Z}[x]$ на множители в кольце $\mathbb{Z}[x]$, либо убедиться, что f неприводим в $\mathbb{Z}[x]$. Пусть $\deg f = 2n$ или $\deg f = 2n+1$. Тогда в любом нетривиальном разложении $f = gh$ степень одного из делителей, пусть это будет h, не превосходит n. Чтобы выяснить, делится ли f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени не выше n, подставим в f произвольные $n+1$ различных чисел $z_0, \ldots, z_n \in \mathbb{Z}$ и выпишем все возможные наборы чисел $d_0, \ldots, d_n \in \mathbb{Z}$, в которых каждое d_i делит соответствующее $f(z_i)$. Таких наборов имеется конечное число, и если искомый многочлен h существует, то набор его значений $h(z_0), \ldots, h(z_n)$ на числах z_i является одним из выписанных наборов $d_0, \ldots, d_n$. Для каждого такого набора в $\mathbb{Q}[x]$ есть ровно один многочлен h степени не выше n с $h(z_i) = d_i$ при всех i — это *интерполяционный многочлен Лагранжа*[2]

$$h(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)}. \tag{4-7}$$

[1] См. сл. 1.1 на стр. 30.
[2] См. прим. 2.5 на стр. 43.

Таким образом, делитель h многочлена f, если он существует, совпадает с одним из тех многочленов (4-7), что имеют целые коэффициенты. Остаётся явно разделить f на все такие многочлены и либо убедиться, что они не делят f, либо обнаружить среди них делитель f.

Ответы и указания к некоторым упражнениям

Упр. 4.1. Импликации (а)⇒(б)⇒(в) очевидны. Если I содержит обратимый элемент, то среди его кратных есть единица, кратные которой исчерпывают всё кольцо.

Упр. 4.2. Первое очевидно, второе вытекает из того, что суммы $b_1a_1 + \ldots + b_ma_m$, где $a_i \in M$, $b_i \in K$, лежат во всех идеалах, содержащих M.

Упр. 4.3. Если a и b являются старшими коэффициентами многочленов f и g из идеала I, и $\deg f = m$, а $\deg g = n$, где $m \geqslant n$, то $a + b$ либо нуль, т. е. является старшим коэффициентом нулевого многочлена, либо является старшим коэффициентом многочлена $f + x^{m-n}g \in I$ степени m. Аналогично, для любого $\alpha \in K$ произведение αa является старшим коэффициентом многочлена $\alpha f(x) \in I$ степени m.

Упр. 4.4. Повторите доказательство теор. 4.1, следя за младшими коэффициентами вместо старших.

Упр. 4.6. 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 $\mathbb{Z} \smallsetminus \{1,\ 2,\ \ldots\ ,\ k\}$. Убедитесь, что $\sin(2\pi z)/\prod\limits_{\alpha=1}^{k}(z-\alpha) \in I_k \smallsetminus I_{k-1}$, откуда $I_k \subsetneq I_{k+1}$.

Упр. 4.7. 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. 0.9: 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. 4.8. Возьмите в качестве J^* объединение всех идеалов из M.

Упр. 4.9. В (а) всякий идеал в $\mathbb{C}[x]$ является главным. Если факторкольцо $\mathbb{C}[x]/(f)$ не имеет делителей нуля, то многочлен f неприводим. Над полем $\mathbb{C}$ неприводимые многочлены исчерпываются линейными, поэтому $f(x) = x - p$ для некоторого $p \in \mathbb{C}$ и $(f) = (x - p) = \ker \mathrm{ev}_p$. В (б) с помощью леммы о конечном покрытии докажите, что для любого идеала I в кольце непрерывных функций $[0, 1] \to \mathbb{R}$ найдётся точка $p \in [0, 1]$, в которой все функции из I обращаются в нуль, что даст включение $I \subset \ker \mathrm{ev}_p$. В (в) подойдёт главный идеал $\mathfrak{m} = (x^2 + 1)$.

Упр. 4.11. Если в каждом идеале I_k есть элемент $x_k \in I_k \smallsetminus \mathfrak{p}$, то произведение этих элементов $x_1 \ldots x_m \in \bigcap I_k \subset \mathfrak{p}$, что противоречит простоте $\mathfrak{p}$.

Упр. 4.12. Рассмотрим эпиморфизм факторизации $\pi\colon K \twoheadrightarrow K/I$. 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. 4.13. В (в) и (г) для любого $z \in \mathbb{C}$ в рассматриваемом кольце существует такой элемент w, что $|z - w| < 1$. Взяв такой w для $z = a/b$, заключаем, что $|a - bw| < |b|$.

Упр. 4.14. 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

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

$r = a(1-bq)$ 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.

Упр. 4.15. Если $b=ax$ и $a=by=axy$, то $a(1-xy)=0$, откуда $xy=1$.

Упр. 4.16. 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. 4.17. По аналогии с комплексными числами, назовём *сопряжённым* к числу $\vartheta = a+b\sqrt{5}$ число $\overline{\vartheta} = a-b\sqrt{5}$, а целое число $\|\vartheta\| \stackrel{\text{def}}{=} \vartheta\cdot\overline{\vartheta} = a^2-5b^2$ назовём *нормой* числа ϑ. Легко видеть, что $\overline{\vartheta_1\vartheta_2} = \overline{\vartheta}_1\cdot\overline{\vartheta}_2$, откуда $\|\vartheta_1\vartheta_2\| = \vartheta_1\vartheta_2\overline{\vartheta}_1\overline{\vartheta}_2 = \|\vartheta_1\|\cdot\|\vartheta_2\|$. Поэтому $\vartheta\in\mathbb{Z}[\sqrt{5}]$ обратим тогда и только тогда, когда $\|\vartheta\|=\pm1$, и в этом случае $\vartheta^{-1}=\pm\overline{\vartheta}$. Поскольку $\|2\|=4$, а $\|1\pm\sqrt{5}\|=-4$, разложение этих элементов в произведение xy с необратимыми x и y возможно только при $\|x\| = \|y\| = \pm 2$. Но элементов нормы ±2 в $\mathbb{Z}[\sqrt{5}]$ нет, так как равенство $a^2-5b^2=\pm2$ при редукции по модулю 5 превращается в равенство $a^2=\pm2$ в поле $\mathbb{F}_5$, где числа ±2 не являются квадратами.

Упр. 4.18. Из равенства $z_1z_2=1$ вытекает равенство $|z_1|\cdot|z_2|=1$. Так как $|z|^2\in\mathbb{N}$ для всех $z\in\mathbb{Z}[i]$, гауссово число z может быть обратимо только если $|z|=1$.

Упр. 4.19. Пусть $n = p_1^{\alpha_1}\ldots p_s^{\alpha_r}q_1^{\beta_1}\ldots q_s^{\beta_s}$, где $p_i, q_j\in\mathbb{N}$ — попарно разные простые числа, причём p_i представляются в виде суммы двух квадратов, а q_j — нет, т. е. все $q_j\equiv 3\pmod 4$, а все p_i — нет. Тогда разложение n на простые множители в области $\mathbb{Z}[i]$ имеет вид

$$n = \prod\nolimits_i (x_i+iy_i)^{\alpha_i}(x_i-iy_i)^{\alpha_i}\prod\nolimits_j q_j^{\beta_j},\ \text{где } q_j\in\mathbb{N}.$$

Если все β_j чётные, то $n=(a+ib)(a-ib)=a^2+b^2$ для $a+ib=\prod_i(x_i+iy_i)^{\alpha_i}\prod_j q_j^{\beta_j/2}$. Наоборот, пусть $n=a^2+b^2=(a+ib)(a-ib)$, и разложение гауссова числа $a+ib$ на простые множители в $\mathbb{Z}[i]$ имеет вид $a+bi=\prod_k \ell_k^{\gamma_k}$. Тогда разложение числа n на простые множители в $\mathbb{Z}[i]$ имеет вид $\prod_k \ell_k^{\gamma_k}\overline{\ell}_k^{\gamma_k}$, и все вещественные простые множители входят в него в чётных степенях.

Упр. 4.22. Это следует из равенства $a_0q^n + a_1q^{n-1}p + \ldots + a_{n-1}qp^{n-1} + a_np^n = 0$

Упр. 4.23. Ответ: $(x^2-2x+2)(x^2+2x+2)$.