§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 этим свойством 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 гомоморфизмов факторизации $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)$, $m \mapsto [m]_n$, и $\Bbbk[x] \twoheadrightarrow \Bbbk[x]/(f)$, $g \mapsto [g]_f$, которые сопоставляют целому числу (соотв. многочлену) его класс вычетов. 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 5.1. 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 5.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных собственных идеалов.

Доказательство. Из упр. 5.1 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. □

5.1.1. Нётеровость. Любое подмножество $M \subset K$ порождает идеал $(M) \subset K$, состоящий из всех элементов кольца K, представимых в виде $b_1a_1 + b_2a_2 + \cdots + b_ma_m$, 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 5.2. Убедитесь, что $(M) \subset K$ это и в самом деле идеал, совпадающий 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 $I = (a_1, \ldots, a_k) = \{b_1a_1 + b_2a_2 + \cdots + b_ka_k \mid b_i \in K\}$, 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 5.1
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
3) любая бесконечная возрастающая цепочка вложенных идеалов $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ 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 $I_n = (a_1, \dots, a_n)$, 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 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 не выше d из I, а через $L_\infty = \bigcup_d L_d$ — множество старших коэффициентов вообще всех многочленов из I.

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 $f_i^{(\infty)}$, 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 $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{m_\infty}^{(\infty)}$ 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 $m_i = \deg g - \deg f_i^{(\infty)} \geqslant 0$, и можно 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 $\deg h < \deg g$. 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 строго уменьшать его степень, сокращая старший член путём вычитания из h подходящих комбинаций многочленов $f_j^{(d)}$ с $0 \leqslant d < D$. □

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

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

Следствие 5.2
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 $f_1, f_2, \dots, f_m \in M$, что среди многочленов f_ν, что каждый многочлен $g \in M$ представляется в виде $g = h_1f_1 + h_2f_2 + \cdots + h_mf_m$ 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 конечного множества уравнений $f_1(x_1,\dots,x_n) = f_2(x_1,\dots,x_n) = \cdots = f_m(x_1,\dots,x_n) = 0$. □

5.1.2. 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 $x_{\nu_1}^{m_1} x_{\nu_2}^{m_2} \cdots x_{\nu_s}^{m_s}$ не является нётеровым: его идеал $(x_1, x_2, \dots)$, состоящий из всех многочленов без свободного члена, нельзя породить конечным множеством многочленов.

Упражнение 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 сюръективное отображение факторизации

$$\pi : K \twoheadrightarrow X, \quad a \mapsto [a], \tag{5-2}$$

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

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab], \tag{5-3}$$

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 (5-3) сводят их проверку к проверке аксиом коммутативного кольца в K. В частности, нулевым элементом кольца X будет класс $[0]$. С другой стороны, если формулы (5-3) корректны, то они утверждают, что отображение (5-2) является гомоморфизмом колец. Но если это так, то согласно n° 2.6.3 на стр. 28 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 (5-2), является аддитивным сдвигом ядра на этот элемент:

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

Оказывается, что этих необходимых условий на классы также и достаточно для того, чтобы правила (5-3) были корректны, т. е. для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{5-4}$$

образует разбиение кольца K, и правила (5-3) корректно определяют на классах этого разбиения структуру коммутативного кольца с нулевым элементом $[0]_I = I$.

Упражнение 5.7. Убедитесь, что отношение сравнимости по модулю идеала

$$a_1 \equiv a_2 \,(\mathrm{mod}\, I)\,,$$

означающее, что $a_1 - a_2 \in I$, является отношением эквивалентности, и проверьте, что формулы (5-3) корректны.

Определение 5.2
Классы эквивалентности (5-4) называются *классами вычетов* (или *смежными классами*) по модулю идеала I. Множество этих классов с операциями (5-3) называется *фактор кольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм

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

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, для любого гомоморфизма коммутативных колец $\varphi : A \to B$ имеется канонический изоморфизм колец $\overline{\varphi} : A/\ker\varphi \simeq \in \varphi$, $[a]_{\ker\varphi} \mapsto \varphi(a)$, переводящий каждый класс

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

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

Пример 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 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 отношением нестрогого включения. В самом деле, обратимость всех ненулевых классов $[a]_{\mathfrak{m}}$ в фактор кольце $K/\mathfrak{m}$ 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.

[1] Т. е. отличный от всего кольца.
[2] См. n° 1.7 на стр. 16.

Из леммы Цорна[1] 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 5.8. Убедитесь, что он полный, т. е. для любого линейно упорядоченного множества[2] M содержащих I собственных идеалов в K существует собственный идеал J^*, содержащий все идеалы из M.

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 5.9. Убедитесь, что:

а) каждый максимальный идеал кольца $\mathbb{C}[x]$ имеет вид $\ker \mathrm{ev}_p$ для некоторого $p \in \mathbb{C}$

б) каждый максимальный идеал кольца непрерывных функций $[0, 1] \to \mathbb{R}$ 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 $\ker \mathrm{ev}_p$ с $p \in \mathbb{R}$.

Пример 5.4 (простые идеалы и гомоморфизмы 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 5.10. Убедитесь в этом.

Согласно определениям, всякий максимальный идеал прост. Обратное неверно: скажем, главный идеал $(x) \subset \mathbb{Q}[x, y]$ прост, так как кольцо $\mathbb{Q}[x, y]/(x) \simeq \mathbb{Q}[x]$ целостное, 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 $\mathfrak{p} \subset K$ 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 5.11. Убедитесь, что пересечение конечного множества идеалов содержится в простом идеале $\mathfrak{p}$ только если хотя бы один из пересекаемых идеалов содержится в $\mathfrak{p}$.

[1] См. лем. 1.3 на стр. 18.

[2] В данном случае это означает, что для любых $J_1, J_2 \in M$ выполняется включение $J_1 \subseteq J_2$ или включение $J_2 \subseteq J_1$.

Пример 5.5 (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*[1]. 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 $a_1, \dots, a_n$ 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. 5.1 и идущего ниже упражнения:

Упражнение 5.12. Покажите, что фактор кольцо нётерова кольца тоже нётерово.

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*) $\nu : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$, сопоставляющая каждому ненулевому элементу $a \in K$ целое неотрицательное число $\nu(a)$ так, что $\forall\, a, b \in K \setminus \{0\}$ выполняется неравенство $\nu(ab) \geqslant \nu(a)$ и существуют такие $q, r \in K$, что

$$a = bq + r\,, \text{ где } \nu(r) < \nu(b) \text{ или } r = 0. \tag{5-6}$$

Элементы q, r называются *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) $\mathbb{Z}$ с $\nu(z) = |z|$ б) $\Bbbk[x]$ с $\nu(f) = \deg f$
в) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a + bi \in \mid a, b \in \mathbb{Z},\ i^2 = -1\}$ 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 $\nu(z) = |z|^2$.

Все четыре кольца из упр. 5.13 являются кольцами главных идеалов в силу следующей теоремы.

Теорема 5.2
Любое евклидово кольцо является кольцом главных идеалов[2].

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 $\nu(ab) = \nu(a)$ для $a, b \neq 0$ равносильно обратимости элемента b.

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

[2] Отметим, что обратное неверно, но содержательное обсуждение контрпримеров требует техники, которой мы пока не владеем (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 $a_1, \dots, a_n$ есть наибольший общий делитель — такой элемент $d = \text{нод}(a_1, \dots, a_n) \in K$, который делит все элементы a_i, делится на любой общий делитель элементов a_i и представляется в виде $d = a_1 b_1 + \dots + a_n b_n$ с подходящими $b_i \in K$. Это простая переформулировка того, что порождённый элементами a_i идеал $(a_1, \dots, a_n) = \{x_1 a_1 + x_2 a_2 + \dots + x_n a_n \mid x_i \in K\}$ является главным и имеет вид (d) для некоторого $d \in K$. Отметим, что наибольший общий делитель определён не однозначно, а с точностью до умножения на произвольный обратимый элемент кольца.

Упражнение 5.15. Убедитесь, что в любом целостном[1] коммутативном кольце K главные идеалы (a) и (b) совпадают если и только если $a = sb$ для некоторого обратимого $s \in K$.

Поэтому всюду в дальнейшем обозначение $\text{нод}(a_1, \dots, a_n)$ 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 $\text{нод}(a_1, \dots, a_n) = 1$ означает, что у элементов a_i нет необратимых общих делителей. Поскольку в этом случае имеется представление $1 = a_1 b_1 + \dots + a_n b_n$ с $b_i \in K$, в кольце главных идеалов отсутствие необратимых общих делителей у элементов a_i равносильно их *взаимной простоте* в смысле опр. 2.2 на стр. 24.

5.4. Факториальность. Всюду в этом разделе мы по умолчанию обозначаем через K *целостное*[3] 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, 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.

5.4.1. Неприводимые элементы. 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, что 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.

Отметим, что кольце главных идеалов любые два неприводимых элемента p, q либо взаимно просты[4], либо ассоциированы, поскольку порождённый ими идеал $(p, q) = (d)$ для некоторого $d \in K$, и 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 неассоциированных неприводимых элемента могут и не быть взаимно простыми. Например, в $\mathbb{Q}[x, y]$ элементы x и y не взаимно просты и не ассоциированы.

Предложение 5.2
В любом кольце главных идеалов K следующие свойства элемента $p \in K$ попарно эквивалентны друг другу:

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

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

[3] См. сноску (1) выше.

[4] В смысле опр. 2.2 на стр. 24, т. е. существуют такие $x, y \in K$, что $px + qy = 1$.

1) фактор кольцо $K/(p)$ является полем

2) в фактор кольце $K/(p)$ нет делителей нуля

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

Доказательство. Импликация (1) ⇒ (2) очевидна и имеет место в любом коммутативном кольце с единицей[1]. Покажем, что в любом целостном кольце[2] K справедлива импликация (2) ⇒ (3). Из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$. 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) ⇒ (1). Так как каждый собственный идеал в K главный, максимальность идеала (p) в чуме главных идеалов означает его максимальность в чуме всех собственных идеалов. В прим. 5.3 на стр. 68 мы видели, что 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 5.3
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 противоречит нётеровости. □

Определение 5.3
Целостное кольцо K называется *факториальным*, если каждый его необратимый элемент является произведением конечного числа неприводимых, причём любые два таких разложения

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_k$$

состоят из одинакового числа $k = m$ сомножителей, после надлежащей перенумерации которых можно указать такие обратимые элементы $s_\nu \in K$, 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. 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. 5.2 в кольце главных идеалов верно и обратное: все неприводимые элементы кольца главных идеалов просты. Однако в произвольном целостном кольце простота является более

[1] См. n° 2.4.1 на стр. 25.
[2] Не обязательно являющимся кольцом главных идеалов.

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

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

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 5.17. 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 5.4
Целостное нётерово кольцо K факториально тогда и только тогда, когда 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. В силу своей единственности, разложение произведения ab на неприводимые множители является произведением таких разложени для 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 и, стало быть, простых элементов. Покажем, что в любом целостном кольце равенство $p_1 \cdots p_k = q_1 \cdots q_m$, в котором все сомножители просты, возможно только если $k = m$ и после надлежащей перенумерации каждый p_i окажется ассоциирован с q_i. Так как произведение $q_1 \cdots q_m$ делится на p_1, один из его сомножителей делится на p_1. Будем считать, что это $q_1 = sp_1$. Поскольку q_1 неприводим, элемент s обратим. Пользуясь целостностью кольца K, сокращаем обе части равенства $p_1 \cdots p_k = q_1 \cdots q_m$ 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 5.6 (суммы двух квадратов, продолжение прим. 3.6 на стр. 47)
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 $p = (a+ib)(a-ib) = a^2+b^2$ с ненулевыми $a, b \in \mathbb{Z}$. Таким образом, простое $p \in \mathbb{Z}$ приводимо в $\mathbb{Z}[i]$ если и только если 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 $p \in \mathbb{Z}$

[1] См. предл. 5.2 на стр. 71.

является суммой двух квадратов если и только если -1 квадратичный вычет по модулю p. Как мы видели в n° 3.5.2 на стр. 50, это происходит при $p = 2$ и тех $p > 2$, для которых $(p-1)/2$ чётно, т. е. для $p = 4k+1$.

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 $a_1, \dots, a_m \in K$ допускает следующее описание. Для каждого класса ассоциированных неприводимых элементов $q \in K$ обозначим через m_q максимальное такое целое число, 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 $f = a_0 + a_1x + \dots + a_nx^n \in K[x]$ 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 одного из многочленов f, g. Поскольку неприводимые элементы факториального кольца просты, фактор кольцо $R = K/(q)$ целостное. Применим к произведению fg гомоморфизм редукции по модулю q: $K[x] \to R[x]$, $a_0 + a_1x + \dots + a_nx^n \mapsto [a_0]_q + [a_1]_qx + \dots [a_n]_qx^n$, заменяющий все коэффициенты каждого многочлена классами их вычетов по модулю q.

Упражнение 5.19. Проверьте, что это и в самом деле гомоморфизм колец.

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 $f \in Q_K[x]$ представляется в виде $f(x) = (a/b)\cdot f_{\text{red}}(x)$, где $f_{\text{red}} \in K[x]$, $a, b \in K$ и $\operatorname{cont}(f_{\text{red}}) = \text{нод}(a,b) = 1$, 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 $(a/b)\cdot f_{\text{red}}(x) = (c/d)\cdot g_{\text{red}}(x)$

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 у a и b и у c и d, это возможно, только если a ассоциирован с c, а b ассоциирован с d. Но тогда и $f_{\mathrm{red}}(x) = g_{\mathrm{red}}(x)$ с точностью до умножения на обратимую константу. □

Следствие 5.5 (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 редуцированном виде из лем. 5.3 и сокращая возникающую дробь, приходим к равенству

$$f(x) = \frac{a}{b} \cdot g_{\mathrm{red}}(x) \cdot h_{\mathrm{red}}(x)\,, \tag{5-7}$$

в котором $g_{\mathrm{red}}, h_{\mathrm{red}} \in K[x]$ имеют содержание 1, и нод$(a, b) = 1$. По лем. 5.2

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

т. е. правая часть в (5-7) является редуцированным представлением многочлена f. В силу единственности редуцированного представления элементы a и b обратимы в K, а $f = g_{\mathrm{red}} h_{\mathrm{red}}$ с точностью до умножения на обратимую константу. □

Теорема 5.3
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 редуцированном виде из лем. 5.3 и сокращая возникающую при этом числовую дробь, получаем равенство $f = \frac{a}{b} \prod f_{\nu,\mathrm{red}}$, в котором все многочлены $f_{\nu,\mathrm{red}} \in K[x]$ неприводимы в $Q_K[x]$ и имеют содержание 1, а числа $a, b \in K$ взаимно просты. Поскольку $\mathrm{cont}\left(\prod f_{\nu,\mathrm{red}}\right) = 1$, правая часть равенства является редуцированным представлением многочлена $f = \mathrm{cont}(f) \cdot f_{\mathrm{red}}$. В силу единственности редуцированного 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 $K[x]$

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

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 $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_m$ 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 многочленов p_i и q_i 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[1] вытекает, что эти постоянные множители являются обратимыми константами из K. □

[1] См. лем. 5.3 на стр. 74.

Следствие 5.6
Кольцо многочленов $K[x_1, \dots, x_n]$ над факториальным кольцом[1] K 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 5.20. 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 5.21. Разложите $x^4 + 4$ в $\mathbb{Z}[x]$ в произведение двух квадратных трёхчленов.

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

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

$$\mathbb{Z}[x] \to \frac{\mathbb{Z}}{(m)}[x], \quad a_0 + a_1 x + \dots + a_n x^n \mapsto [a_0]_m + [a_1]_m x + \dots [a_n]_m x^n \tag{5-8}$$

приводит все коэффициенты каждого многочлена по модулю m и является гомоморфизмом колец[2]. Поэтому равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_m = [g]_n \cdot [h]_m$ во всех кольцах $\big(\mathbb{Z}/(m)\big)[x]$. Таким образом 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 $\mathbb{Z}[x]$.

Пример 5.7
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 5.8 (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 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.

[1] В частности, над полем или над областью главных идеалов.
[2] Мы уже пользовались этим в доказательстве лем. 5.2 на стр. 74, см. упр. 5.19.

Пример 5.9 (неприводимость кругового многочлена Φ_p)
Покажем, что при простом $p \in \mathbb{N}$ круговой многочлен

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

неприводим в $\mathbb{Z}[x]$. Для этого перепишем его как многочлен от переменной $t = x - 1$

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

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. 5.8. Поэтому и $\Phi_p(x) = f(x-1)$ неприводим.

5.6.2. Алгоритм Кронекера позволяет путём довольно трудоёмкого, но вполне эффективного конечного вычисления либо явно найти разложение заданного многочлена f с целыми коэффициентами в кольце $\mathbb{Z}[x]$, либо убедиться, что f неприводим в $\mathbb{Z}[x]$ (а значит, по лемме Гаусса, и в $\mathbb{Q}[x]$). Будем для определённости считать, что $\deg f = 2n$ или $\deg f = 2n+1$. Тогда в любом нетривиальном разложении $f = gh$ в $\mathbb{Z}[x]$ степень одного из делителей, назовём его h, не превосходит n. Чтобы выяснить, делится ли f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени не выше n, подставим в f любые $n+1$ различных чисел $z_0, z_1, \ldots, z_n \in \mathbb{Z}$ и выпишем все возможные наборы чисел $d_0, d_1, \ldots, d_n \in \mathbb{Z}$, в которых каждое d_i делит соответствующее $f(z_i)$. Таких наборов имеется конечное число, и набор значений $h(z_0), \ldots, h(z_n)$ многочлена h на числах z_i, если такой многочлен вообще существует, является одним из выписанных нами 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]

$$h(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)}. \tag{5-9}$$

Таким образом, делитель h многочлена f, если он существует, является одним из тех многочленов (5-9), что имеют целые коэффициенты. Остаётся явно разделить f на все такие многочлены и либо убедиться, что они не делят f, либо найти среди них делитель f.

[1] См. сл. 2.1 на стр. 26.
[2] См. упр. 3.12 на стр. 39.

Ответы и указания к некоторым упражнениям

Упр. 5.1. Импликации (а)⇒(б)⇒(в) очевидны. Если I содержит обратимый элемент, то среди его кратных есть единица, кратные которой исчерпывают всё кольцо.

Упр. 5.2. Первое утверждение очевидно, второе вытекает из того, что все суммы вида $b_1a_1+b_2a_2+\cdots+b_ma_m$, где $a_1,\ldots,a_m\in M$, $b_1,\ldots,b_m\in K$, лежат во всех идеалах„ содержащих множество M.

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 нуль, т. е. является старшим коэффициентом нулевого многочлена, 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 $\mathbb{Z}\smallsetminus\{1,\,2,\,\ldots\,,\,k\}$. 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. 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. 1.10: 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. Возьмите в качестве J^* объединение всех идеалов из M.

Упр. 5.9. В (а) всякий идеал в $\mathbb{C}[x]$ является главным. Если фактор кольцо $\mathbb{C}[x]/(f)$ 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. 5.11. Если в каждом идеале I_k есть элемент $x_k\in I_k\smallsetminus\mathfrak{p}$, то произведение этих элементов $x_1x_2\ldots x_m\in\bigcap I_k\subset\mathfrak{p}$, что противоречит простоте $\mathfrak{p}$.

Упр. 5.12. 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. 5.13. Для колец (в) и (г) свойство (**??**) очевидно, поскольку модули всех ненулевых элементов не меньше 1, а свойство (5-6) вытекает из того, что для любого $z\in\mathbb{C}$ существует такой элемент кольца w, что $|z-w|<1$. Беря такой w для $z=a/b$, получаем $|a-bw|<|b|$, так что можно положить $q=w$ и $r=a-bw$.

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

Упр. 5.14. Если $\exists\ b^{-1}$, то $v(ab) \leqslant v(abb^{-1}) = v(a)$. Наоборот, если $v(ab) = v(a)$, то деля a на ab с остатком, получаем $a = abq + r$, где либо $v(r) < v(ab) = v(a)$, либо $r = 0$. Из равенства $r = a(1 - bq)$ вытекает, что либо $v(r) \geqslant v(a)$, 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. 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 $\overline{\vartheta} = a - b\sqrt{5}$, 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 $||\vartheta|| = \pm 1$, и в этом случае $\vartheta^{-1} = \pm\overline{\vartheta}$. Поскольку $||2|| = 4$, а $||1 \pm \sqrt{5}|| = -4$, разложение этих элементов в произведение 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 $a^2 - 5b^2 = \pm 2$ при редукции по модулю 5 превращается в равенство $a^2 = \pm 2$ в поле $\mathbb{F}_5$, где числа ± 2 не являются квадратами.

Упр. 5.20. Это следует из равенства $a_0q^n + a_1q^{n-1}p + \cdots + a_{n-1}qp^{n-1} + a_np^n = 0$

Упр. 5.21. Ответ: $(x^2 - 2x + 2)(x^2 + 2x + 2)$.