§9. Гомоморфизмы колец, фактор кольца и идеалы.

9.1. Гомомрфизмы. Отображение колец $A \xrightarrow{\varphi} B$ называется *гомоморфизмом*, если для любой пары элементов $a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$\begin{aligned} f(a_1 + a_2) &= f(a_1) + f(a_2) \\ f(a_1 a_2) &= f(a_1) f(a_2)\,. \end{aligned} \tag{9-1}$$

Отметим, что этим условиям удовлетворяет *нулевой* (или *тривиальный*) гомоморфизм, отображающий все элементы из A в нуль кольца B.

Любой гомоморфизм колец, будучи гомоморфизмом аддитивных групп, обладает всеми свойствами, установленными нами в (n° 5.1). Например, из первого соотношения (9-1) автоматически следует, что $\varphi(0) = 0$ и $\forall\, a \in A\ \ \varphi(-a) = -\varphi(a)$.

Образ гомоморфизма колец является подкольцом в B. Прообраз нулевого элемента

$$\ker(\varphi) \stackrel{\text{def}}{=} \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}$$

называется *ядром* гомоморфизма колец. Ядро является подкольцом в A и вместе с каждым элементом $a \in \ker(\varphi)$ содержит также и все кратные ему элементы ab (с любыми $b \in A$):

$$\varphi(a) = 0 \quad \Rightarrow \quad \forall\, b \in A\ \ \varphi(ab) = \varphi(a)\varphi(b) = 0\,.$$

Как мы видели в (n° 5.1), прообраз произвольного элемента $\varphi(a) \in \operatorname{im}(\varphi)$ является смежным классом аддитивной группы $\ker(\varphi) \subset A$:

$$\varphi^{-1}(\varphi(a)) = a + \ker(\varphi) = \{b \in A \mid b - a \in \ker(\varphi)\}\,.$$

Иными словами, два элемента $a, b \in A$ тогда и только тогда переходят в один и тот же элемент кольца B, когда $a - b \in \ker(\varphi)$:

$$\varphi(a) = \varphi(b) \quad \Longleftrightarrow \quad \varphi(b - a) = \varphi(b) - \varphi(a) = 0\,.$$

В частности, для того чтобы гомоморфизм колец был вложением, необходимо и достаточно, чтобы $\ker(\varphi = \{0\}$ (в этом случае говорят, что φ *имеет нулевое ядро*).

9.1.1. ПРЕДЛОЖЕНИЕ. *Любой ненулевой гомоморфизм из поля в произвольное кольцо является вложением.*

Доказательство. Если $\varphi(a) = 0$ для какого-нибудь $a \neq 0$, то $\forall\, b \in A\ \ \varphi(b) = \varphi\left(ba^{-1}a\right) = \varphi\left(ba^{-1}\right)\varphi(a) = 0$. Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

9.1.2. Пример: действие гомоморфизма колец на единицу. Поскольку кольцо не является группой относительно операции умножения, гомоморфизм коммутативных колец с единицами $A \xrightarrow{\varphi} B$, вообще говоря, не обязан переводить единицу в единицу. Например, отображение $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/(6)$, отправляющее все чётные числа в нулевой класс, а все нечётные — в класс $[3]_6$, является гомоморфизмом колец, и $\varphi(1) = [3]_6 \neq [1]_6$. Тем не менее, вычисление из (n° 5.1): $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ влечёт в кольце равенство $\varphi(1)(\varphi(1) - 1) = 0$. Если в кольце B нет делителей нуля, из этого равенства следует, что либо $\varphi(1) = 0$, и тогда $\forall\, a \in A\ \ \varphi(a) = \varphi(1 \cdot a) = \varphi(1)\varphi(a) = 0$, либо $\varphi(1) = 1$. Таким образом, любой нетривиальный гомоморфизм в в целостное кольцо с единицей всё-таки переводит единицу в единицу.

9.2. Идеалы. Подмножество I коммутативного кольца K называется *идеалом*, если оно удовлетворяет следующим двум условиям:

$$a_1, a_2 \in I \quad \Rightarrow \quad a_1 \pm a_2 \in I \tag{9-2}$$

$$a \in I \quad \Rightarrow \quad \forall\, b \in K\ \ ab \in I \tag{9-3}$$

Первое условие означает, что идеал является аддитивной подгруппой в кольце, второе — что вместе с каждым элементом идеал содержит и все кратные ему элементы. Выше мы видели, что этими свойствами обладает ядро любого гомоморфизма $K \xrightarrow{\varphi} K'$, так что ядра гомоморфизмов являются идеалами. Примерами идеалов являются подмножества вида

$$(a) = \{ka \mid k \in K\}\,, \tag{9-4}$$

состоящие из всех элементов, кратных фиксированному элементу $a \in K$. Идеалы вида (9-4) называются *главными*. Мы встречались с ними при построении колец вычетов $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов

$$\mathbb{Z} \xrightarrow{m \mapsto [m]_n} \mathbb{Z}/(n)\,, \quad \Bbbk[x] \xrightarrow{g \mapsto [g]_f} \Bbbk[x]/(f)$$

сопоставляющих целому числу (соотв. многочлену) класс его вычета.

Более общим образом, для любого набора элементов $a_1, a_2, \dots, a_m \in K$ множество всех элементов, представимых в виде $k_1a_1 + k_2a_2 + \dots + k_ma_m$ с произвольными $k_1, k_2, \dots, k_m \in K$

$$(a_1, a_2, \dots, a_m) \stackrel{\text{def}}{=} \{k_1a_1 + k_2a_2 + \dots + k_ma_m \mid k_1, k_2, \dots, k_m \in K\} \tag{9-5}$$

тоже является идеалом. Он называется *идеалом, порождённым* $a_1, a_2, \dots, a_m$. Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Отметим, что в любом кольце K имеются *тривиальные* идеалы $(0) = \{0\}$ и K.

Упражнение 9.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей попарно равносильны: а) $I = K$ б) $1 \in I$ в) I содержит какой-нибудь обратимый элемент.

9.2.1. ПРЕДЛОЖЕНИЕ. *Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных идеалов.*

Доказательство. Если K поле, $I \subset K$ — идеал, и $b \in I$ отличен от нуля, то $1 = b^{-1}b \in I$, и значит $I = K$, поскольку $\forall\, b \in K \quad b = 1 \cdot b \in I$ по свойству (9-3). Наоборот, тривиальность главного идеала $(b) = \{bc \mid c \in K\}$ означает, что либо $b = 0$, либо $(b) \ni 1$. В последнем случае $bc = 1$ для некоторого c, т. е. b обратим. Тем самым, если все главные идеалы тривиальны, то все ненулевые элементы обратимы. □

9.3. Факторизация. Пусть произвольное коммутативное кольцо K разбито в объединение непустых непересекающихся подмножеств:

$$K = \bigsqcup_{x \in X} K_x\,, \tag{9-6}$$

занумерованных элементами некоторого множества X. Иначе можно сказать, что имеется сюрьективное отображение множеств

$$K \overset{x}{\twoheadrightarrow} X\,, \tag{9-7}$$

сопоставляющее каждому элементу $a \in K$ номер $x(a)$ того подмножества разбиения (9-6), где лежит a. Для каждого $a \in K$ обозначим через $[a] = X_{x(a)} \subset K$ множество всех элементов, имеющих тот же номер, что и a, и будем называть его *классом элемента a*. Мы хотим задать на множестве X сложение и умножение, согласованные со сложением и умножением в кольце K, т. е. определить их формулами

$$x(a) + x(b) = x(a + b)\,, \quad x(a) \cdot x(b) = x(ab)\,.$$

Это то же самое, что задать сложение и умножение классов разбиения (9-6) формулами

$$[a] + [b] = [a + b]\,, \quad [a] \cdot [b] = [ab]\,. \tag{9-8}$$

Покажем, что эти формулы тогда и только тогда корректно наделяют множество X структурой коммутативного кольца, когда класс $[0] \subset K$ является идеалом в K, а все остальные классы представляют собой смежные классы по модулю этого идеала, т. е.

$$\forall\, a \in K \ \ [a] = a + I = \{a + i \mid i \in I\} = \{b \in A \mid b - a \in I\}\,.$$

В самом деле, пусть $[0]$ — идеал в K и равенство классов $[a_1] = [a_2]$ означает, что $a_2 - a_1 \in [0]$. Тогда формулы (9-8) корректно задают операции над классами, т. е. при $[a_1] = [a_2]$ и $[b_1] = [b_2]$ мы получим $[a_1 + b_1] = [a_2 + b_2]$ и $[a_1 b_1] = [a_2 b_2]$. Действительно, если $a_2 = a_1 + \alpha$ и $b_2 = b_1 + \beta$, где $\alpha, \beta \in [0]$, то $a_2 + b_2 = a_1 + b_1 + (\alpha + \beta)$ и $a_2 + b_2 = a_1 b_1 + (\alpha b_1 + \beta a_1 + \alpha\beta)$, где заключённые в скобки члены лежат в $[0]$, поскольку $[0]$ идеал. Выполнение аксиом коммутативного кольца в K автоматически влечёт их выполнение в X. Например, дистрибутивность проверяется выкладкой

$$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a(b + c)] = [ab + bc] = [ab] + [bc] = [a] \cdot [b] + [a] \cdot [c]\,.$$

Упражнение 9.2. Проверьте аналогичным образом выполнение всех остальных аксиом.

Наоборот, если формулы (9-8) корректно задают на X структуру кольца, то отображение (9-7) является гомоморфизмом колец с ядром $\ker(x) = [0]$. Следовательно $[0] = \ker(x)$ — идеал в K, и любой класс $[a] = x^{-1}(x(a))$ является смежным классом ядра.

9.3.1. Определение фактор кольца. Множество аддитивных смежных классов идеала $I \subset K$ со структурой кольца, заданной формулами (9-8), обозначается K/I и называется *фактор кольцом* кольца K по идеалу I.

9.3.2. Строение гомоморфизма. Из предыдущего следует, что образ любого гомоморфизма коммутативных колец $K_1 \xrightarrow{\varphi} K_2$ изоморфен фактор кольцу $K_1/\ker(\varphi)$, а сам гомоморфизм раскладывается в композицию вложения $K_1/\ker(\varphi) \simeq \mathrm{im}\,(\varphi) \overset{\varphi'}{\hookrightarrow} K_2$ и эпиморфизма факторизации $K_1 \overset{\varphi''}{\twoheadrightarrow} K_1/\ker(\varphi) \simeq \mathrm{im}\,(\varphi)$, т. е. мы имеем коммутативную диаграмму

$$\begin{tikzcd} K_1 \arrow[rr, "\varphi"] \arrow[dr, "\varphi''"'] & & K_2 \\ & G/\ker(\varphi) \simeq \mathrm{im}\,(f) \arrow[ur, hook, "\varphi'"'] & \end{tikzcd} \tag{9-9}$$

аналогичную (5-10).

9.3.3. Пример: редукция целочисленных многочленов по модулю n. Рассмотрим в кольце $\mathbb{Z}[x]$ главный идеал (n), где $n \neq 1$ — целая константа. Этот идеал состоит из многочленов, все коэффициенты которых делятся на n. Фактор кольцо $\mathbb{Z}[x]/(n)$ изоморфно кольцу $\big(\mathbb{Z}/(n)\big)[x]$ многочленов с коэффициентами в кольце вычетов $\mathbb{Z}/(n)$. В самом деле, отображение

$$\begin{gathered} \varrho_n : \mathbb{Z}[x] \xrightarrow{f \mapsto [f]_n} \big(\mathbb{Z}/(n)\big)[x]\,, \quad \text{где} \\ \big[a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0\big]_n \overset{\text{def}}{=} [a_m]_n\, x^m + [a_{m-1}]_n\, x^{m-1} + \cdots + [a_1]_n\, x + [a_0]_n\,, \end{gathered} \tag{9-10}$$

является сюрьективным гомоморфизмом колец с $\ker(\varrho_n) = (n)$.

Гомоморфизм (9-10) называется *редукцией по модулю* n. Он часто бывает полезен для доказательства неприводимости того или иного многочлена $f \in \mathbb{Z}[x]$. Ход мысли при этом таков: если $f = gh$ в $\mathbb{Z}[x]$, то во всех кольцах $\big(\mathbb{Z}/(n)\big)[x]$ выполняется равенство $[f]_n = [g]_n \cdot [h]_n$. Если $n = p$ — простое, то кольцо $\mathbb{Z}/(n) = \mathbb{F}_p$ является полем, в частности, в $\mathbb{F}_p[x]$ имеется однозначное разложение на неприводимые множители. Более того, все потенциальные неприводимые делители любого многочлена $[f]_p$, в принципе, можно перебрать, ибо над $\mathbb{F}_p$ есть лишь конечное число многочленов заданной степени.

Упражнение 9.3. Перечислите все неприводимые многочлены степени $\leqslant 3$ в $\mathbb{F}_2[x]$ и в $\mathbb{F}_3[x]$.

Например, чтобы убедиться в неприводимости многочлена $f(x) = x^5 + x^2 + 1$ в кольце $\mathbb{Z}[x]$, достаточно рассмотреть его редукцию по модулю 2. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$, а т. к. у $[f]_2 = x^5 + x^2 + 1$ нет корней и в $\mathbb{F}_2$, оба многочлена $[g]_2$, $[h]_2$ неприводимы в $\mathbb{F}_2[x]$. Тогда x^5+x^2+1, согласно упр. 9.3, должен делиться в $\mathbb{F}_2[x]$ на x^2+x+1, что не так.

Ещё один пример: покажем, что многочлен деления круга на простое число частей

$$f(x)=x^{p-1}+x^{p-2}+\ \cdots\ +x+1=\frac{x^p-1}{x-1}\,,\quad \text{где } p \text{ простое}\,,$$

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

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

При редукции по модулю p от многочлена $f(t)$ остаётся только старший моном $[f(t)]_p=t^n$. Если $f(t)=g(t)h(t)$ в $\mathbb{Z}[t]$, то $[g(t)]_p[h(t)]_p=t^n$ в $\mathbb{F}_p[t]$, откуда вытекает[1], что g и h тоже редуцируются по модулю p в свои старшие мономы: $[g(x)]_p=x^m$, $[h(x)]_p=x^k$, где $m=\deg(g)$, $k=\deg(h)$. Тем самым, все коэффициенты g, h, кроме старшего, делятся на p. Но тогда младший коэффициент f, будучи произведением младших коэффициентов g, h, должен делиться на p^2, что не так. Следовательно, f неприводим.

Упражнение 9.4 (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. Покажите, что f неприводим в $\mathbb{Z}[x]$.

9.4. Кольца главных идеалов. Целостное кольцо K с единицей называется *кольцом главных идеалов*, если каждый идеал $I\subset K$ является *главным*, т. е. имеет вид $I=(d)=\{ad\mid a\in K\}$.

Параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, который мы наблюдали в предыдущих двух параграфах, объясняется тем, что оба этих кольца являются кольцами главных идеалов. Доказательство этого факта основано на возможности деления с остатком, и фактически было дано нами в (n° 7.7) и (n° 8.3.5), когда мы обсуждали свойства наибольших общих делителей. Сейчас мы воспроизведём его ещё раз таким образом, чтобы оно годилось для любого кольца, допускающего «деление с остатком» в следующем точном смысле.

9.4.1. Евклидовы кольца. Целостное кольцо K с единицей называется *евклидовым*, если существует функция

$$K\setminus\{0\}\xrightarrow{\ \nu\ }\mathbb{N}\cup\{0\}\,,$$

сопоставляющая каждому ненулевому элементу $a\in K$ целое неотрицательное число $\nu(a)$, которое называется *евклидовой нормой* (или *высотой*) элемента a так, что $\forall\,a,b\in K\setminus\{0\}$ выполняются следующие два свойства:

$$\nu(ab)\geqslant\nu(a)\tag{9-11}$$

$$\exists\,q,r\in K\ :\ a=bq+r\ \text{ и либо } \nu(r)<\nu(b)\,,\text{ либо } r=0\,.\tag{9-12}$$

Так, в кольце целых чисел $\mathbb{Z}$ функцией высоты является абсолютная величина, а в кольце многочленов $\Bbbk[x]$ с коэффициентами в поле $\Bbbk$ высотой служит степень многочлена.

Упражнение 9.5. Покажите, что кольца

а) $\mathbb{Z}[i]\overset{\text{def}}{=}\{a+bi\in\ \mid a,b\in\mathbb{Z}\,,\ i^2=-1\}$

б) $\mathbb{Z}[\omega]\overset{\text{def}}{=}\{a+b\omega\in\mathbb{C}\mid a,b\in\mathbb{Z}\,,\,\omega^2+\omega+1=0\,\}$

являются евклидовыми относительно высоты $\nu(z)=|z|^2$.

Элементы q и r, о которых идёт речь во втором свойстве (9-11), называются, соответственно, *неполным частным* и *остатком* от деления a на b. Подчеркнём, что их единственности (для данных a и b) не предполагается.

Упражнение 9.6. Покажите, что в любом евклидовом кольце равенство $\nu(ab)=\nu(a)$ в свойстве (9-11) равносильно тому, что элемент b обратим (решение можно подглядеть в сноске ([2])).

[1] здесь мы используем единственность разложения на неприводимые множители в кольце $\mathbb{F}_p[x]$

[2] Решение: если $\exists\,b^{-1}$, то $\nu(ab)\leqslant\nu(abb^{-1})=\nu(a)$; наоборот, если $\nu(ab)=\nu(a)$, то деля a на ab с остатком, получаем $a=abq+r$, где либо $\nu(r)<\nu(ab)=\nu(a)$, либо $r=0$; из равенства $r=a(1-bq)$ вытекает, что либо $\nu(r)\geqslant\nu(a)$, либо $1-bq=0$; с учётом предыдущего, такое возможно только при $1-bq=0$ или $r=0$; во втором случае $a(1-bq)=0$, что тоже влечёт $1-bq=0$; следовательно $bq=1$ и b обратим

Покажем, что в любом евклидовом кольце K всякий идеал $I \subset K$ является главным. Выберем в I какой-нибудь ненулевой элемент $d \in I$ наименьшей высоты. Тогда всякий элемент $a \in I$ делится на d. Действительно, деля a на d с остатком, получаем $a = dq + r$, где $r = a - dq \in I$, поскольку $a, d \in I$. При этом либо $\nu(r) < \nu(d)$, что невозможно по выбору d, либо $r = 0$, что и утверждается. Таким образом, $I \subset (d)$. Так как $d \in I$, мы имеем равенство $I = (d)$.

Итак, все евклидовы кольца являются кольцами главных идеалов[1]. В частности, кольцами главных идеалов являются $\mathbb{Z}$, $\Bbbk[x]$, где $\Bbbk$ — поле, а также кольца $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$ из упр. 9.5.

9.4.2. НОД и взаимная простота. Любой набор элементов $a_1, a_2, \dots, a_n$ произвольного кольца главных идеалов K имеет наибольший общий делитель $d = \text{нод}(a_1, a_2, \dots, a_n)$, который можно представить в виде $d = x_1a_1 + x_2a_2 + \dots + x_na_n$. Это простая переформулировка того, что идеал, порождённый элементами $a_1, a_2, \dots, a_n$, является главным:

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

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

Из наличия представления $\text{нод}(a_1, a_2, \dots, a_n) = x_1a_1 + x_2a_2 + \dots + x_na_n$ вытекает, что в любом кольце главных идеалов отсутствие у элементов $a_1, a_2, \dots, a_n$ необратимых общих делителей влечёт за собой их взаимную простоту[2], т. е. возможность представить единицу кольца в виде

$$1 = x_1a_1 + x_2a_2 + \dots + x_na_n \quad \text{с некоторыми } x_i \in K \ .$$

Упражнение 9.7. Покажите, что если элементы $a_1, a_2, \dots, a_m$ кольца главных идеалов K таковы, что $\forall\, i \neq j$ $\text{нод}(a_i, a_j) = 1$, то $K/(a_1 \cdot a_2 \cdot \dots \cdot a_m) \simeq (K/(a_1)) \times (K/(a_2)) \times \cdots (K/(a_m))$.

9.4.3. ПРЕДЛОЖЕНИЕ. *В любом кольце главных идеалов K следующие свойства элемента $p \in K$ попарно эквивалентны друг другу:*

(1) *$K/(p)$ является полем;*

(2) *в $K/(p)$ нет делителей нуля;*

(3) *p неприводим, т. е. $p = ab \Rightarrow a$ или b обратим в K .*

Доказательство. Импликация (1) $\Rightarrow$ (2) уже была доказана нами для любого поля в (n° 7.2). Покажем, что в любом целостном кольце K (не обязательно являющемся кольцом главных идеалов) имеет место импликация (2) $\Rightarrow$ (3). Из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и если в $K/(p)$ нет делителей нуля, то один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, и значит, $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим. Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Если p неприводим, то $\forall\, b \notin (p)$ $\text{нод}(p, b) = 1$, а значит, $\exists\, x, y \in K : px + by = 1$, откуда $[b][y] = 1$ в $K/(p)$. Тем самым, любой класс $[b] \neq [0]$ обратим в $K/(p)$, т. е. $K/(p)$ — поле. □

9.4.4. Однозначность разложения на неприводимые множители. Целостное кольцо называется *факториальным*, если каждый его необратимый элемент a является произведением конечного числа неприводимых элементов $a = p_1p_2 \cdots p_m$, причём любое другое такое разложение $a = q_1q_2 \cdots q_k$ состоит из того числа сомножителей $k = m$, и после надлежащей перенумерации каждый q_ν будет ассоциирован[3] с p_ν.

Упражнение 9.8. Покажите, что в произвольном кольце главных идеалов K любые два неприводимых элемента p, q либо взаимно просты (т. е. $px + qy = 1$ для некоторых $x, y \in K$), либо ассоциированы (т. е. $p = qs$ для некоторого обратимого $s \in K$).

9.4.5. ПРЕДЛОЖЕНИЕ. *Всякое кольцо главных идеалов факториально.*

[1] отметим, что обратное неверно, но контрпримеры приходят из достаточно глубокой теории чисел и алгебраической геометрии, так что для их полноценного понимания требуется техника, которой мы пока ещё не владеем; впрочем, заинтересовавшийся читатель может обратиться к замечанию 3 на стр. 365 книги Э. Б. Винберга «*Курс алгебры*» (цит. по изданию М. «Факториал» (1999))

[2] иначе взаимную простоту $a_1, a_2, \dots, a_n$ можно охарактеризовать как равенство $(a_1, a_2, \dots, a_n) = K$

[3] т. е. $q_\nu = s_\nu \cdot p_\nu$ для некоторых обратимых $s_\nu \in K$, см. (n° 7.7)

Доказательство. Докажем сначала существование разложения произвольного элемента a в произведение конечного числа неприводимых множителей. Если a неприводим, то доказывать нечего. Если нет, запишем его в виде произведения необратимых элементов. Каждый приводимый сомножитель этого произведения снова запишем в виде произведения необратимых элементов и т. д. Этот процесс не кончится через конечное число шагов построением требуемого разложения, только если в K существует бесконечная последовательность элементов $\{a_i\}$, в которой a_{i+1} делит a_i, но a_i не делит a_{i+1}, т. е. $(a_i) \subsetneq (a_{i+1})$.

Упражнение 9.9. Убедитесь, что для любой цепочки вложенных идеалов $\cdots \subset I_\nu \subset I_{\nu+1} \subset \cdots$ произвольного коммутативного кольца объединение $I = \bigcup\limits_\nu I_\nu$ также является идеалом.

Поскольку все идеалы в K главные, $\bigcup\limits_\nu (a_\nu) = (d)$ для некоторого $d \in \bigcup\limits_\nu (a_\nu)$. Коль скоро d лежит в объединении, $\exists\, i : d \in (a_i)$. А тогда $(d) = \bigcup\limits_\nu (a_\nu) = (a_i)$. В частности, $\forall\, k > 0\ (a_{i+k}) = (a_i)$ вопреки предположению о том, что $(a_i) \subsetneq (a_{i+1})$. Тем самым, процесс разложения не может продолжаться бесконечно.

Докажем теперь единственность разложения. Пусть мы имеем равенство $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$, в котором все множители неприводимы. Заметим, что p_i не может быть взаимно прост с каждым из q_i, поскольку в этом случае он будет взаимно прост и с их произведением (см. n° 7.6), т. е. найдутся $x, y \in K : 1 = xp_1 + yq_1 q_2 \cdots q_m = xp_1 + yp_1 p_2 \cdots p_k = p_1(x + yp_2 \cdots p_k)$, что невозможно, поскольку p_1 необратим. Тем самым, в правой части существует множитель, скажем q_1, который не взаимно прост с p_1, а значит (см. упр. 9.8) $q_1 = sp_1$ для некоторого обратимого $s \in K$. Тогда $p_1(p_2 \cdots p_k - sq_2 \cdots q_m) = 0$, откуда следует более короткое равенство $p_2 p_3 \cdots p_k = (sq_2) q_3 \cdots q_m$, к которому применимо предыдущее рассуждение. □

9.4.6. Некоторые предостережения. Разумеется, не все кольца являются кольцами главных идеалов. Например, идеалы $(2, x) \subset \mathbb{Z}[x]$ и $(x, y) \subset \mathbb{Q}[x, y]$ не являются главными.

Упражнение 9.10. Докажите это.

Через некоторое время мы покажем, что кольца $\mathbb{Z}[x]$ и $\mathbb{Q}[x, y]$ факториальны. Таким образом, факториальность является существенно более слабым ограничением на кольцо, чем свойство быть кольцом главных идеалов.

Пример нефакториального целостного кольца доставляет кольцо алгебраических чисел

$$\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2 - 5)\ ,$$

в котором есть такие два различных разложения на неприводимые множители:

$$2 \cdot 2 = \left(\sqrt{5} + 1\right) \cdot \left(\sqrt{5} - 1\right)\ .$$

Упражнение 9.11. Докажите, что 2, $\sqrt{5} + 1$, $\sqrt{5} - 1$ неприводимы и попарно неассоциированы.

9.4.7. Пример: простые и неприводимые элементы. Ключевым местом в доказательстве единственности разложения из предложения (n° 9.4.5) была такая импликация: если произведение $q_1 q_2 \cdots q_m$ делится на p_1, то хотя бы один из сомножителей делится на p_1.

Необратимый элемент p произвольного целостного кольца K называется *простым*, если для любых $a, b \in K$ из того, что произведение ab делится на p, вытекает, что a или b делится на p. Иначе можно сказать, что простота элемента p означает, что в кольце $K/(p)$ нет делителей нуля.

В доказательстве предложения (n° 9.4.3) мы видели, что в любом целостном кольце все простые элементы автоматически неприводимы. Мы видели также, что в кольце главных идеалов справедливо и обратное: всякий неприводимый элемент прост. Именно в этом и заключается причина факториальности колец главных идеалов.

Упражнение 9.12. Пусть в целостном кольце K всякий элемент является произведением конечного числа неприводимых. Покажите, что K факториально тогда и только тогда, когда все неприводимые элементы в K просты.

Для общего целостного кольца K простота является строго более сильным свойством, чем неприводимость. Так, в уже упоминавшемся выше кольце алгебраических чисел $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2 - 5)$ число 2 неприводимо, но не просто, поскольку в фактор кольце

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

имеется очевидный делитель нуля $(x + 1) \pmod{(2, x^2 + 1)}$ (на языке алгебраических чисел это означает, что $\sqrt{5} + 1$ не делится на 2 в $\mathbb{Z}[\sqrt{5}]$, а $(\sqrt{5} + 1)^2 = 6 + 2\sqrt{5}$ — делится), хотя двойка при этом неприводима.

9.4.8. Пример: гауссовы целые числа (продолжение примера n° 6.4.1). Согласно упр. 9.5, 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. Для этого заметим, что разложение любого целого вещественного $n \in \mathbb{Z}$, будучи инвариантным относительно комплексного сопряжения, должно вместе с каждым неприводимым множителем $a + ib \in \mathbb{C} \smallsetminus \mathbb{R}$ содержать и сопряжённый ему множитель $a - ib$. В частности, если простое $p \in \mathbb{Z}$ перестаёт быть неприводимым в $\mathbb{Z}[i]$, то оно представляется в виде $p = (a + ib)(a - ib) = a^2 + b^2$ с ненулевыми $a, b \in \mathbb{Z}$. Таким образом, простое $p \in \mathbb{Z}$ тогда и только тогда приводимо в $\mathbb{Z}[i]$, когда p является суммой двух квадратов. Чтобы явно описать все такие p, вспомним, что неприводимость $p \in \mathbb{Z}[i]$ равносильна тому, что фактор кольцо $\mathbb{Z}[i]/(p)$ является полем[1], и посмотрим на это фактор кольцо как на фактор кольца многочленов $\mathbb{Z}[x]$ по идеалу $(p, x^2+1) \subset \mathbb{Z}[x]$, порождённому элементами p и $(x^2 + 1)$:

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2 + 1) \simeq \mathbb{F}_p[x]/(x^2 + 1)\ .$$

Самое правое кольцо является полем тогда и только тогда, когда многочлен $x^2 + 1$ неприводим над $\mathbb{F}_p$, что равносильно отсутствию у него корней в $\mathbb{F}_p$. Таким образом, простое $p \in \mathbb{Z}$ является суммой двух квадратов, если и только если -1 квадратичный вычет по модулю p. Как мы видели в примере (n° 8.5.6), это происходит в точности тогда, когда $(p - 1)/2$ чётно, т. е. для простых $p = 4k + 1$ и $p = 2$.

9.4.9. Пример: взаимно простые идеалы. Два идеала I, J произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если существуют $x \in I$ и $y \in J$, такие что $x+y = 1$. Это условие равносильно тому, что идеал $I + J \overset{\text{def}}{=} (I, J) = \{x + y \mid x \in I\ ,\ y \in J\}$, порождённый их объединением и состоящий из всевозможных сумм, совпадает со всем кольцом. Свойства взаимно простых идеалов обобщают свойства взаимно простых чисел.

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

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

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

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

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

$$K/\bigcap\limits_\nu I_\nu \xrightarrow[\sim]{a\mapsto(a \,(\mathrm{mod}\ I_1),\, a\,(\mathrm{mod}\ I_2),\, \dots ,\, a\,(\mathrm{mod}\ I_n))} (K/I_1) \times (K/I_2) \times \ \cdots \ \times (K/I_n)\ . \tag{9-13}$$

Доказательство. Отображение $K \xrightarrow[\sim]{a\mapsto(a \,(\mathrm{mod}\ I_1),\, a\,(\mathrm{mod}\ I_2),\, \dots ,\, a\,(\mathrm{mod}\ I_n))} (K/I_1) \times (K/I_2) \times \ \cdots \ \times (K/I_n)$ является гомоморфизмом колец с ядром $\bigcap\limits_\nu I_\nu$. Поэтому нам достаточно доказать его сюрьективность. По предыдущей лемме I_k взаимно прост с $\bigcap\limits_{\nu\neq k} I_\nu$ для каждого k. Поэтому найдутся $x_k \in I_k$ и $y_k \in \bigcap\limits_{\nu\neq k} I_\nu$, такие что $x_k + y_k = 1$. Это означает, что

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

и в качестве элемента $a \in K$, отображающегося в произвольно заданный набор классов $[a_k] \in K/I_k$, мы можем взять $a = \sum\limits_{k=1}^{n} y_k a_k$. □

Упражнение 9.13. Выведите из предложения (n° 9.4.11) предыдущие версии китайской теоремы об остатках, доказанные нами в примерах (n° 7.6.1) и (n° 8.5.3).

[1] см. предложение (n° 9.4.3)

[2] убедитесь, что пересечение идеалов тоже является идеалом

9.5. Характеристика. Для любого кольца с единицей K имеется канонический гомоморфизм

$$\mathbb{Z} \xrightarrow{\varkappa} K\,,$$

переводящий единицу в единицу и действующий на произвольное целое число по правилу

$$\varkappa(\pm n) = \pm(\underbrace{1+1+\,\cdots\,+1}_{n}) \quad \text{для} \;\; n \in \mathbb{N}\,.$$

Если $\varkappa$ инъективен, то говорят, что K имеет *характеристику нуль*, в противном случае *характеристикой* называют наименьшее натуральное число p, для которого

$$\underbrace{1+1+\,\cdots\,+1}_{p} = 0\,.$$

Иначе это можно сказать так: поскольку в $\mathbb{Z}$ все идеалы главные, $\ker(\varkappa) = (p)$ для некоторого целого неотрицательного p, которое и называется *характеристикой* кольца K. Характеристика обозначается $\mathrm{char}(K)$. Если кольцо K целостное, то его подкольцо $\mathbb{Z}/(p) \simeq \mathrm{im}\,(\varkappa) \subset K$ также не будет иметь делителей нуля. Таким образом, характеристика целостного кольца или равна нулю или является простым числом.

Упражнение 9.14. Докажите это непосредственно, пользуясь равенством

$$\underbrace{1+1+\,\cdots\,+1}_{mn} = (\underbrace{1+1+\,\cdots\,+1}_{m})(\underbrace{1+1+\,\cdots\,+1}_{n})$$

9.5.1. Простое подполе. Пусть $\Bbbk$ — поле. Наименьшее по включению подполе в $\Bbbk$, содержащее 1 и 0, называется *простым подполем* в $\Bbbk$. Простое подполе, таким образом, содержит $\mathrm{im}\,(\varkappa)$.

Если $\mathrm{char}(\Bbbk) = p > 0$, то $\mathrm{im}\,(\varkappa) \simeq \mathbb{F}_p$ и будет простым подполем поля $\Bbbk$.

Если $\mathrm{char}(\Bbbk) = 0$, т. е. $\varkappa(q) \neq 0$ при $q \neq 0$, то гомоморфизм $\varkappa$ можно продолжить до (автоматически инъективного по n° 9.1.1) гомоморфизма полей

$$\varkappa : \mathbb{Q} \xhookrightarrow{\frac{p}{q} \mapsto \frac{\varkappa(p)}{\varkappa(q)}} \Bbbk\,.$$

Следовательно, в этом случае простое подполе в $\Bbbk$ изоморфно полю рациональных чисел $\mathbb{Q}$.

Таким образом, всякое поле является либо расширением поля $\mathbb{Q}$, либо расширением одного из полей $\mathbb{F}_p$ с простым $p \in \mathbb{N}$, причём никаких ненулевых гомоморфизмов между полями разных характеристик нет.

9.5.2. Гомоморфизм Фробениуса. Если $\mathrm{char}(\Bbbk) = p > 0$, тоже самое вычисление, что и в (n° 7.9), показывает, что

$$\forall\, a, b \in \Bbbk \quad (a+b)^p = a^p + \sum_{k=1}^{p-1} (\underbrace{1+1+\,\cdots\,+1}_{\binom{p}{k}}) a^k b^{p-k} + b^p = a^p + b^p\,.$$

Тем самым, отображение возведения в p-тую степень $F_p : \Bbbk \xrightarrow{x \mapsto x^p} \Bbbk$ является гомоморфизмом из поля $\Bbbk$ в себя. Он называется *гомоморфизмом Фробениуса*. Согласно малой теореме Ферма[1] гомоморфизм Фробениуса тождественно действует на простом подполе $\mathbb{F}_p \subset \Bbbk$. Например, для $\Bbbk = \mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$ гомоморфизм Фробениуса $\mathbb{F}_4 \xrightarrow{F_2} \mathbb{F}_4$ является автоморфизмом, аналогичным комплексному сопряжению: он тождественно действует на подполе $\mathbb{F}_2 = \{0, 1\}$ и переводит друг в друга элементы $\omega = [x]$ и ω^2, являющиеся корнями многочлена $x^2 + x + 1$.

Упражнение 9.15. Опишите действие Фробениуса F_3 на поле $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$.

9.6. Кольца функций. Пусть K — коммутативное кольцо, а X — произвольное множество. Множество всех функций $X \longrightarrow K$ обозначается K^X и образует кольцо относительно операций поточечного сложения и умножения значений функций:

$$f + g : x \mapsto f(x) + g(x) \qquad fg : x \mapsto f(x)g(x)\,.$$

[1] см. (n° 7.9) и (n° 7.3.2)

Тождественно нулевая функция является в K^X нулём, а тождественно единичная (если в K есть единица) — единицей.

Иначе K^X можно воспринимать как *прямое произведение*[1] одинаковых копий кольца K, занумерованных элементами $x \in X$. Если множество X состоит из n элементов, то вместо K^X обычно пишут K^n и изображают элементы такого кольца строчками[2] $(a_1, a_2, \dots, a_n)$.

Поскольку произведение любых двух функций с непересекающимися носителями[3] равно нулю, в кольце K^X много делителей нуля, даже если K — поле. Обратимыми элементами K^X являются функции, принимающие обратимое значение в каждой точке.

9.6.1. Гомоморфизмы подъёма. С каждым отображением множеств $X \xrightarrow{\varphi} Y$ связан гомоморфизм *подъёма*[4] вдоль φ

$$\varphi^* \,:\, K^Y \xrightarrow{f \mapsto f \circ \varphi} K^X\,,$$

который переводит функции на Y в их композиции с φ, являющиеся функциями на X, и тем самым, действует в противоположном к φ направлении. На языке некоммутативной алгебры подъём есть не что иное, как правое умножение всех отображений из $\mathrm{Hom}(Y, K)$ на отображение $\varphi \in \mathrm{Hom}(X, Y)$:

$$\mathrm{Hom}(Y, K) \xrightarrow{f \mapsto f\varphi} \mathrm{Hom}(X, K)$$

Отметим, что хотя кольца функций и не целостные, гомоморфизм подъёма всегда переводит единицу кольца K^Y в единицу кольца K^X.

Упражнение 9.16. Из каких функций состоит ядро гомоморфизма подъёма?

В геометрии и анализе множества X и Y обычно наделяются той или иной дополнительной структурой: мерой, метрикой, топологиейи т. п. Соответственно и функции рассматриваются не любые, а согласованные с этой структурой: интегрируемые, непрерывные, гладкие, аналитическиеи т. п. Такие специальные функции образуют в кольце всех функций подкольцо, которое в алгебре принято обозначать $K[X] \subset K^X$ и называть *структурным кольцом* (или *кольцом регулярных функций*) соответствующей теории.

Отображения между множествами с дополнительной структурой тоже рассматриваются не произвольные, а согласованные со структурой, скажем, непрерывные или дифференцируемые. В алгебре такие отображения тоже называются *регулярными*. Как только зафиксирована теория, т. е. в кольце функций каждого рассматриваемого в этой теории множества X выделено подкольцо регулярных функций $K[X]$, регулярные отображения между множествами теории можно определить уже чисто алгебраически, а именно, как такие отображения $X \xrightarrow{\varphi} Y$, подъём вдоль переводит регулярные функции на Y в регулярные функции на X , т. е. является гомоморфизмом не только между кольцами всех функций, но и между ме́ньшими подкольцами:

$$K[Y] \xrightarrow{\varphi^*} K[X]\,.$$

Упражнение 9.17* (для тех, кто знаком с непрерывностью). Обозначим кольцо непрерывных функций $[0,1] \longrightarrow \mathbb{R}$ через $C \subset \mathbb{R}^{[0,1]}$. Покажите, что

а) отображение $[0,1] \xrightarrow{\varphi} [0,1]$ непрерывно тогда и только тогда, когда $\varphi^*(C) \subset C$;

б) для непрерывного φ инъективность гомоморфизма $C \xrightarrow{\varphi^*} C$ равносильна сюрьективности φ.

9.6.2. Гомоморфизмы вычисления. В случае, когда $X = \{*\}$ состоит из одной точки, гомоморфизм поднятия, отвечающий вложению $\{*\} \xhookrightarrow{y} Y$ этой точки в качестве некой точки $y \in Y$, называется *вычислением в точке* y и обозначается[5] ev_y. Поскольку $K^{\{*\}} = K$,

$$\mathrm{ev}_y \,:\, K^Y \xrightarrow{f \mapsto f(y)} K$$

---

[1]см. (n° 7.5)

[2]напомним (см. n° 7.5), что сложение и умножение таких строк производится покомпонентно

[3]напомним, что *носителем* функции $X \xrightarrow{f} K$ называется множество $\mathrm{Supp}(f) = \{x \in X \mid f(x) \neq 0\}$.

[4]по-английски он называется *pull back homomorphism*; по-русски подъёмы тоже иногда называют *обратными образами*, и их ни в коем случае не следует путать с *прообразами*

[5]от английского *evaluation*

сопоставляет каждой функции $Y \xrightarrow{f} K$ её значение $\mathrm{ev}_y(f) = f(y)$ в точке y. Гомоморфизм вычисления ev_y эпиморфен, а его ядро состоит из функций, обращающихся в нуль в точке y.

Гомоморфизмы вычисления позволяют для любого абстрактно заданного кольца $R \supset K$ с единицей построить множество $X[R]$, для которого R естественным образом отождествится с некоторым подкольцом в $K^{X[R]}$. А именно, назовём *K-точкой* кольца R произвольный гомоморфизм $R \xrightarrow{p} K$, тождественно действующий на подкольце $K \subset R$, и положим $X[R]$ равным множеству всех K-точек кольца R. Каждый элемент $f \in R$ может восприниматься как функция на $X[R] \xrightarrow{f} K$, значение которой на K-точке $R \xrightarrow{p} K$, по определению, равно $p(f) \in K$. Подкольцо $K \subset R$ при этом превращается в множество постоянных функций.

Упражнение 9.18*. Имеется ли биекция между точками отрезка $[0,1]$ и $\mathbb{R}$-точками кольца непрерывных функций $[0,1] \longrightarrow \mathbb{R}$? Изменится ли ответ, если заменить отрезок на полуинтервал? Изменятся ли ответы, если заменить непрерывные функции на а) дифференцируемые б) полиномиальные?

Таким образом, как только зафиксировано кольцо констант K, например $K = \mathbb{R}$, и выбран некоторый класс колец R, содержащих K в качестве подкольца, так сразу же возникает геометрическая теория, пространствами в которой будут множества $X[R]$, описанные выше, а кольцами регулярных функций на этих пространствах будут подкольца $R \subset K^{X[R]}$, вложенные в $K^{X[R]}$ так, как это объяснялось выше. Замечательно, что всякий гомоморфизм колец

$$R_1 \xrightarrow{\varphi} R_2\,,$$

тождественно действующий на кольце констант K, может восприниматься при этом как гомоморфизм подъёма для отображения пространств, ассоциированных с этими кольцами

$$\varphi^* : X[R_2] \xrightarrow{p \mapsto p\circ\varphi} X[R_1]$$

(это отображение переводит K-точку $R_2 \xrightarrow{p} K$ в её подъём $R_1 \xrightarrow{\varphi} R_2 \xrightarrow{p} K$ вдоль φ).

Упражнение 9.19. Убедитесь, что $(\varphi^*)^* = \varphi$.

Таким образом, между точками и функциями имеется замечательная симметрия, играющая фундаментальную роль во всей математике (да и в природе). Причина её заключается в том, что выражение $f(x)$ на самом деле абсолютно симметрично по x и f — можно считать, что f вычисляется на x, а можно считать, что x вычисляется на f, и нет никакого естественного способа сделать этот выбор *a priori*. Точки точно также являются же функциями на пространстве функций, как функции — на пространстве точек.

Если в качестве кольца констант взять некоторое поле $\Bbbk$, а в качестве колец регулярных функций — конечные прямые произведения $\Bbbk^n$ (с произвольными $n \in \mathbb{N}$), то описанная выше конструкция выдаст геометрическую теорию, известную как *конечномерная линейная алгебра*, с которой мы вскоре начнём знакомиться. Следующий по сложности класс колец — кольца многочленов $\Bbbk[x_1, x_2, \dots, x_n]$ и их фактор кольца — приводит к теории, известной как *аффинная алгебраическая геометрия*, которую мы тоже через некоторое время изучим.

Описания классов колец, отвечающих за более сложные геометрические теории, возникающие в анализе, топологии и математической физике, можно отнести к наиболее ярким достижениям математики XX века.