§8. Напоминание про коммутативные кольца, гомоморфизмы и идеалы.

8.1. 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:

$$\begin{aligned} f(a_1 + a_2) &= f(a_1) + f(a_2) \\ f(a_1 a_2) &= f(a_1) f(a_2)\,. \end{aligned} \tag{8-1}$$

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, присущими гомоморфизму групп. Например, из первого соотношения (8-1) 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 $b \in A$) :

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

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*).

8.1.1. 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. □

8.1.2. 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, в произвольном кольце из равенства $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ вытекает 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.

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

$$a_1, a_2 \in I \quad \Rightarrow \quad a_1 \pm a_2 \in I \tag{8-2}$$

$$a \in I \quad \Rightarrow \quad \forall\, b \in K \;\; ab \in I \tag{8-3}$$

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

$$(a) = \{ka \mid k \in K\}, \tag{8-4}$$

состоящие из всех элементов, кратных фиксированному элементу $a \in K$. Идеалы вида (8-4) называются *главными*. Мы встречались с ними при построении колец вычетов $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов

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

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

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

$$(a_1, a_2, \ldots, a_m) \stackrel{\text{def}}{=} \{k_1a_1 + k_2a_2 + \cdots + k_ma_m \mid k_1, k_2, \ldots, k_m \in K\} \tag{8-5}$$

тоже является идеалом. Он называется *идеалом, порождённым* $a_1, a_2, \ldots, a_m$.

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

Упражнение 8.1. 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.

8.2.1. 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 (8-3). 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. □

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

$$K = \bigsqcup_{x \in X} K_x\,, \tag{8-6}$$

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

$$K \xrightarrow{x} X\,, \tag{8-7}$$

сопоставляющее каждому элементу $a \in K$ номер $x(a)$ того подмножества разбиения (8-6), 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 (8-6) формулами

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

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 (8-8) 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 $[a_1b_1]=[a_2b_2]$. 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 $a_2+b_2=a_1b_1+(\alpha b_1+\beta a_1+\alpha\beta)$, 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

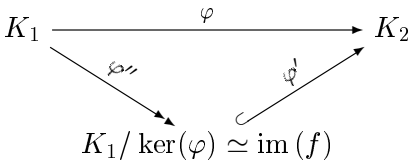
$$[a]\cdot([b]+[c])=[a]\cdot[b+c]=[a(b+c)]=[ab+bc]=[ab]+[bc]=[a]\cdot[b]+[a]\cdot[c]\,.$$

Упражнение 8.2. Проверьте аналогичным образом выполнение всех остальных аксиом.

Наоборот, если формулы (8-8) корректно задают на X структуру кольца, то отображение (8-7) 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.

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

8.3.2. 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 $K_1/\ker(\varphi)\simeq\operatorname{im}(\varphi)\xhookrightarrow{\ \varphi'\ }K_2$ и эпиморфизма факторизации $K_1\xrightarrow{\ \varphi''\ }K_1/\ker(\varphi)\simeq\operatorname{im}(\varphi)$, т. е. мы имеем коммутативную диаграмму



(8-9)

8.3.3. Пример: редукция целочисленных многочленов по модулю n. Рассмотрим в кольце $\mathbb{Z}[x]$ главный идеал (n), где $n\neq1$ — 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

$$\begin{gathered}\varrho_n:\mathbb{Z}[x]\xrightarrow{\ f\mapsto[f]_n\ }\big(\mathbb{Z}/(n)\big)[x]\,,\quad\text{где}\\ \big[a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0\big]_n\overset{\text{def}}{=}[a_m]_n\,x^m+[a_{m-1}]_n\,x^{m-1}+\ \cdots\ +[a_1]_n\,x+[a_0]_n\ ,\end{gathered}\tag{8-10}$$

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

Гомоморфизм (8-10) 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 8.3. Перечислите все неприводимые многочлены степени $\leqslant3$ 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. 8.3, 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 8.4 (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 $\mathbb{Z}[x]$.

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

Параллелизм в свойствах колец $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, объясняется именно тем, что оба этих кольца являются кольцами главных идеалов. Доказательство этого факта основано на возможности деления с остатком. Возможность деления с остатком в абстрактном коммутативном кольце можно описать аксиоматически следующим образом.

8.4.1. 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:

$$\nu(ab) \geqslant \nu(a) \tag{8-11}$$

$$\exists\, q, r \in K \,:\; a = bq + r \ \text{ и либо } \nu(r) < \nu(b)\,, \text{ либо } r = 0\,. \tag{8-12}$$

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 8.5. Покажите, что кольца

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

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

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

Элементы q и r, о которых идёт речь во втором свойстве (8-11), называются, соответственно, *неполным частным* и *остатком* от деления a на b. Подчеркнём, что их единственности (для данных a и b) не предполагается.

Упражнение 8.6. Покажите, что в любом евклидовом кольце равенство $\nu(ab) = \nu(a)$ в свойстве (8-11) равносильно тому, что элемент b обратим (решение можно подглядеть в сноске ([2])).

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[3]. 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. 8.5.

---

[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 делим 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

[3] 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))

8.4.2. НОД. 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 $d = x_1a_1 + x_2a_2 + \cdots + x_na_n$. Это простая переформулировка того, что идеал, порождённый элементами $a_1, a_2, \dots, a_n$, является главным:

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

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.

Отметим, что образующая главного идеала определяется по идеалу не однозначно: равенство $(d_1) = (d_2)$ равносильно тому, что $d_1 = sd_2$, где s — обратим. В самом деле, $d_1 \in (d_2) \Rightarrow d_1 = s_2d_2$ для некоторого s_2. Аналогично, $d_2 \in (d_1) \Rightarrow d_2 = s_1d_1$ для некоторого s_1. Но тогда $d_2 = s_1s_2d_2$ и $d_2(1 - s_1s_2) = 0$. Поскольку делителей нуля в кольце главных идеалов, по определению, нет, мы заключаем, что $s_1s_2 = 1$, т. е. оба эти элемента обратимы.

Элементы, порождающие один и тот же главный идеал (т. е. отличающиеся друг от друга на обратимый множитель), называются *ассоциированными*. Таким образом, любые два наибольших общих делителя заданного набора элементов кольца ассоциированы друг с другом, т. е. различаются на обратимый множитель.

8.5. Взаимная простота. Сделаем несколько важных замечаний о делимости, относящихся к произвольному коммутативному кольцу K с единицей. Элементы $a, b \in K$ называются *взаимно простыми*, если

$$ax + by = 1 \quad \text{для некоторых } x, y \in K . \tag{8-13}$$

Если элементы a и b взаимно просты, то произведение mb с произвольным $m \in K$ делится на a только тогда, когда m делится на a. В самом деле, умножая равенство (8-13) на m, мы получаем

$$m = amx + bmy , \tag{8-14}$$

и если mb делится на a, то и m делится на a. Это же вычисление показывает, что если m делится на a и на b, то m делится и на произведение ab (поскольку оба слагаемых в правой части (8-14) делятся в этом случае на ab).

Далее, если элемент $a \in K$ взаимно прост с каждым из элементов $b_1, b_2, \dots, b_n$, то он взаимно прост и с их произведением. В самом деле, если для каждого i мы можем подобрать такие $x_i, y_i \in K$, что $ax_i + b_iy_i = 1$, то, перемножив все эти равенства, мы получим равенство вида[1]

$$a \cdot x + (b_1b_2 \cdots b_n) \cdot (y_1y_2 \cdots y_n) = 1 ,$$

устанавливающее взаимную простоту a и $b_1b_2 \cdots b_n$.

Элементы $a_1, a_2, \dots, a_n$ произвольного коммутативного кольца K с единицей называются *взаимно простыми в совокупности*, если $(a_1, a_2, \dots, a_n) = K = (1)$, что равносильно существованию таких $x_1, x_2, \dots, x_n \in K$ что $1 = x_1a_1 + x_2a_2 + \cdots + x_na_n$. Из сказанного в предыдущем разделе (n° 8.4.2) вытекает, что в кольце главных идеалов взаимная простота элементов $a_1, a_2, \dots, a_n$ равносильна условию $\text{НОД}(a_1, a_2, \dots, a_n) = 1$, т. е. отсутствию у элементов $a_1, a_2, \dots, a_n$ необратимых общих делителей.

8.5.1. Отступление: 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 $I + J \stackrel{\text{def}}{=} (I, J) = \{x + y \mid x \in I\,,\ y \in J\}$, порождённый их объединением и состоящий из всевозможных сумм, совпадает со всем кольцом. Свойства взаимно простых идеалов обобщают свойства взаимно простых чисел.

[1] в первом слагаемом собраны все члены, содержащие сомножитель a, во втором — единственный член не содержащий такого сомножителя

8.5.2. 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*[1].

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 $\bigcap\limits_\nu J_\nu$. □

8.5.3. 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*

$$K/\bigcap_\nu I_\nu \xrightarrow[\sim]{a \mapsto (a \pmod{I_1}, a \pmod{I_2}, \dots, a \pmod{I_n})} (K/I_1) \times (K/I_2) \times \cdots \times (K/I_n) . \tag{8-15}$$

Доказательство. Отображение $K \xrightarrow[\sim]{a \mapsto (a \pmod{I_1}, a \pmod{I_2}, \dots, a \pmod{I_n})} (K/I_1) \times (K/I_2) \times \cdots \times (K/I_n)$ является гомоморфизмом колец с ядром $\bigcap\limits_\nu I_\nu$. Поэтому нам достаточно доказать его сюръективность. 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 8.7. Выведите из предложения (n° 8.5.3) все известные Вам версии китайской теоремы об остатках. В частности, 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 $K/(a_1 \cdot a_2 \cdot \cdots \cdot a_m) \simeq (K/(a_1)) \times (K/(a_2)) \times \cdots (K/(a_m))$.

8.6. Факториальность. Целостное кольцо называется *факториальным*, если каждый его необратимый элемент a является произведением конечного числа неприводимых элементов $a = p_1 p_2 \cdots p_m$, причём любое другое такое разложение $a = q_1 q_2 \cdots q_k$ состоит из того числа сомножителей $k = m$, и после надлежащей перенумерации каждый q_ν будет ассоциирован[2] с p_ν.

Упражнение 8.8. 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 $s \in K$).

8.6.1. ЛЕММА. *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) очевидна: если $ab = 0$ и $a \neq 0$, то, умножая обе части на a^{-1}, получаем $b = 0$.

Импликация (2) $\Rightarrow$ (3) имеет место в любом целостном кольце K (не обязательно являющемся кольцом главных идеалов). В самом деле, 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.

[1] убедитесь, что пересечение идеалов тоже является идеалом

[2] т. е. $q_\nu = s_\nu \cdot p_\nu$ для некоторых обратимых $s_\nu \in K$

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. □

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

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 8.9. 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° 8.5), 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. 8.8) $q_1 = sp_1$ 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. □

8.6.3. Некоторые предостережения. 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 8.10. Докажите это.

Ниже, в (n° 8.7), мы увидим, что кольца $\mathbb{Z}[x]$ и $\mathbb{Q}[x, y]$ факториальны. Таким образом, не все факториальные кольца являются кольцами 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 8.11. Докажите, что 2, $\sqrt{5} + 1$, $\sqrt{5} - 1$ неприводимы и попарно неассоциированы.

8.6.4. Простые и неприводимые элементы. Ключевым местом в доказательстве единственности разложения из предложения (n° 8.6.2) 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° 8.6.1) 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 8.12. 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.

8.7. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Выберем в каждом классе ассоциированных неприводимых элементов по представителю и определим *наибольший общий делитель* $\text{НОД}(a_1, a_2, \ldots, a_n)$ набора элементов $a_1, a_2, \ldots, a_n \in K$ как класс элементов, ассоциированных с произведением представителей всех неприводимых элементов кольца K, которые делят каждый из элементов a_i. Этот класс, очевидно, не зависит от сделанного нами выбора представителей.

Назовём *содержанием* многочлена $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$ наибольший общий делитель его коэффициентов:

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

Обозначим через Q_K поле частных кольца K. Кольцо многочленов $K[x]$ является подкольцом в кольце многочленов $Q_K[x]$. Всякий многочлен $f(x) \in Q_K[x]$ можно записать в виде

$$f(x) = \frac{a}{b} \cdot \widetilde{f}(x)\,, \tag{8-16}$$

где $\widetilde{f}(x) \in K[x]$ имеет $\operatorname{cont}(f) = 1$, а $a, b \in K$ имеют $\text{НОД}(a, b) = 1$.

Отметим, что в этой записи a, b и $\widetilde{f}(x)$ определяются по f однозначно с точностью до умножения на обратимые элементы из K. В самом деле, равенство

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

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

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

$$\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)\,. \tag{8-17}$$

Доказательство. Достаточно для каждого неприводимого $q \in K$ показать, что q делит левую часть (8-17), если и только если он делит правую. Для этого применим к равенству (8-17) гомоморфизм редукции по модулю q

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

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

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

Доказательство. Если в $Q_K[x]$ выполняется равенство $\operatorname{cont}(f)\widetilde{f}(x) = f(x) = g(x) \cdot h(x) = g(x) \cdot \frac{c}{d} \cdot \widetilde{h}(x)$, где $\widetilde{f}, \widetilde{h} \in K[x]$, $c, d \in K$, $\operatorname{cont}\widetilde{f} = \operatorname{cont}(\widetilde{h}) = \text{НОД}(c, d) = 1$, то $\operatorname{cont}(g\widetilde{h}) = 1$, и в силу единственности представления (8-16) мы должны иметь $\operatorname{cont}(f) = c$ и $d = 1$ (с точностью до умножения на обратимые элементы из K). □

Упражнение 8.13. Пусть многочлен $f \in K[x]$ раскладывается в $Q_K[x]$ в произведение двух многочленов. Покажите, что тогда и в $K[x]$ многочлен f можно разложить в произведение двух многочленов, причём тех же самых степеней, что и в $Q_K[x]$.

Упражнение 8.14. Покажите, что множество неприводимых элементов кольца $K[x]$ состоит из неприводимых констант и многочленов содержания 1, неприводимых в $Q_K[x]$.

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

Доказательство. Область главных идеалов $Q_K[x]$ факториальна. Всякий многочлен $f \in Q_K[x]$ раскладывается в $Q_K[x]$ на неприводимые множители, которые можно записать в виде (8-16). Поэтому

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

где $\widetilde{f}_\nu \in K[x]$ неприводимы в $Q_K[x]$ (а тем более в $K[x]$) и $\operatorname{cont}(\widetilde{f}_\nu) = \text{НОД}(a,b) = 1$. Поскольку $\operatorname{cont}(\prod \widetilde{f}_\nu) = 1$, в силу единственности представления (8-16) мы получаем $b = 1$ и $f = a\prod \widetilde{f}_\nu$ (с точностью до умножения на обратимые константы из K). Раскладывая $a \in K$ в произведение неприводимых констант, получаем разложение f в произведение неприводимых множителей в кольце $K[x]$. Единственность такого разложения следует из упр. 8.14, единственности представления (8-16) и единственности разложений на неприводимые множители в K и в $Q_K[x]$. □

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