§ 2. Коммутативные кольца

В этом параграфе слово „кольцо" будет означать „коммутативное кольцо".

Пусть A — кольцо. *Простой* идеал в A — это такой идеал $\mathfrak{p} \neq A$, что кольцо $A/\mathfrak{p}$ — целостное. Эквивалентным образом мы могли бы сказать, что это такой идеал $\mathfrak{p} \neq A$, для которого из условий x, $y \in A$ и $xy \in \mathfrak{p}$ всегда следует, что $x \in \mathfrak{p}$ или $y \in \mathfrak{p}$.

Пусть $\mathfrak{m}$ — идеал. Мы говорим, что $\mathfrak{m}$ — *максимальный* идеал, если $\mathfrak{m} \neq A$ и если не существует идеала $\mathfrak{a} \neq A$, содержащего $\mathfrak{m}$ и $\neq \mathfrak{m}$.

Всякий максимальный идеал — простой. Доказательство. Пусть $\mathfrak{m}$ — максимальный идеал, и пусть x, $y \in A$ таковы, что $xy \in \mathfrak{m}$. Предположим, что $x \notin \mathfrak{m}$. Тогда $\mathfrak{m} + Ax$ — идеал, строго содержащий $\mathfrak{m}$ и, стало быть, равный A. Следовательно, мы можем написать

$$1 = u + ax,$$

где $u \in \mathfrak{m}$ и $a \in A$. Умножая на y, получаем

$$y = yu + axy,$$

откуда $y \in \mathfrak{m}$ и $\mathfrak{m}$, таким образом, простой.

Пусть A — кольцо. Всякий его идеал $\mathfrak{a} \neq A$ содержится в некотором максимальном идеале $\mathfrak{m}$. Доказательство. Множество идеалов, содержащих $\mathfrak{a}$ и $\neq A$, индуктивно упорядочено по включению. Действительно, если $\{\mathfrak{b}_i\}$ — линейно упорядоченное множество таких идеалов, то $1 \notin \mathfrak{b}_i$ ни для какого i и, следовательно, 1 не лежит в идеале $\mathfrak{b} = \bigcup \mathfrak{b}_i$, который и мажорирует все $\mathfrak{b}_i$. Пусть $\mathfrak{m}$ — некоторый максимальный элемент в нашем множестве. Тогда $\mathfrak{m} \neq A$ и $\mathfrak{m}$ является максимальным идеалом, что и требовалось установить.

Пусть A — кольцо. Тогда $\{0\}$ является простым идеалом в том и только в том случае, если A — целостное. (Доказательство очевидно.)

Мы определили *поле* K как такое кольцо, в котором $1 \neq 0$ и мультипликативный моноид отличных от нуля элементов является группой (т. е. если $x \in K$ и $x \neq 0$, то для x существует обратный). Отметим, что единственные идеалы поля K — это само K и нулевой идеал.

Если A — кольцо и $\mathfrak{m}$ — максимальный идеал, то $A/\mathfrak{m}$ — поле. Доказательство. Для $x \in A$ обозначаем через $\bar{x}$ класс вычетов элемента x по модулю $\mathfrak{m}$. Так как $\mathfrak{m} \neq A$, то в $A/\mathfrak{m}$ имеется единичный элемент $\neq 0$. Всякий ненулевой элемент из $A/\mathfrak{m}$ может быть записан как $\bar{x}$ для некоторого $x \in A$, $x \notin \mathfrak{m}$. Чтобы найти его обратный, заметим, что $\mathfrak{m}+Ax$ есть идеал в A, строго содержащий $\mathfrak{m}$ и, стало быть, равный A. Следовательно, мы можем написать

$$1 = u + yx,$$

где $u \in \mathfrak{m}$ и $y \in A$. Это означает, что $\bar{y}\bar{x}=1$ (т. е. $\bar{1}$) и, таким образом, $\bar{x}$ имеет обратный, что и требовалось установить.

Мы предоставляем читателю в качестве упражнения доказать, что и обратно, *если A — кольцо и $\mathfrak{m}$ — такой идеал, что $A/\mathfrak{m}$ — поле, то $\mathfrak{m}$ максимален.*

Пусть f: $A \to A'$ — гомоморфизм (коммутативных колец, согласно действующему соглашению). Пусть $\mathfrak{p}'$ — простой идеал в A' и $\mathfrak{p} = f^{-1}(\mathfrak{p}')$. Тогда идеал $\mathfrak{p}$ простой.

Для доказательства возьмем x, $y \in A$ с условием $xy \in \mathfrak{p}$. Предположим, что $x \notin \mathfrak{p}$. Тогда $f(x) \notin \mathfrak{p}'$. Но $f(x)f(y) = f(xy) \in \mathfrak{p}'$. Следовательно, $f(y) \in \mathfrak{p}'$, что и требовалось установить.

В качестве упражнения докажите, что если гомоморфизм f сюръективен и $\mathfrak{m}'$ — максимальный идеал в A', то идеал $f^{-1}(\mathfrak{m}')$ максимален в A.

Пример. Пусть $\mathbf{Z}$ — кольцо целых чисел. Мы уже отмечали, что всякий идеал в этом кольце главный и имеет вид $n\mathbf{Z}$ для некоторого целого $n \geqslant 0$ (однозначно определенного идеалом). Пусть $\mathfrak{p}$ — простой идеал (отличный от 0), $\mathfrak{p} = n\mathbf{Z}$. Тогда n должно быть простым числом, что по существу непосредственно вытекает из определения простого идеала. Обратно, если p — простое число, то $p\mathbf{Z}$ — простой идеал (тривиальное упражнение). Кроме того, $p\mathbf{Z}$ — максимальный идеал. Действительно, предположим, что $p\mathbf{Z}$ содержится в некотором идеале $n\mathbf{Z}$. Тогда $p = nm$ для некоторого целого m, откуда $n = p$ или $n = 1$, что и доказывает максимальность $p\mathbf{Z}$.

Пусть n — целое число. Факторкольцо $\mathbf{Z}/n\mathbf{Z}$ называется *кольцом целых чисел по модулю n*. Если n равно простому числу p, то кольцо целых чисел по модулю p является в действительности полем, обозначаемым символом $\mathbf{F}_p$. В частности, мультипликативная группа поля $\mathbf{F}_p$ называется группой отличных от нуля целых чисел по модулю p. Из элементарных свойств групп получаем следующий стандартный факт элементарной теории чисел. Если x — целое число $\not\equiv 0 \pmod{p}$, то $x^{p-1} \equiv 1 \pmod{p}$. (Для простоты обычно пишут mod p вместо mod $p\mathbf{Z}$ и аналогично пишут mod n вместо mod $n\mathbf{Z}$ для любого целого n.) Если, далее, дано целое число $n > 1$, то обратимые элементы кольца $\mathbf{Z}/n\mathbf{Z}$ состоят из тех классов вычетов mod $n\mathbf{Z}$, которые представляются целыми числами $m \neq 0$, взаимно простыми с n. Порядок группы единиц (обратимых элементов) кольца $\mathbf{Z}/n\mathbf{Z}$

обозначается через $\varphi(n)$ (где φ известна как *эйлерова фи-функция*). Следовательно, если x — целое число, взаимно простое с n, то $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Китайская теорема об остатках. *Пусть A — кольцо и $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — такие идеалы, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ при всех $i \neq j$. Для любого семейства элементов $x_1, \ldots, x_n$ кольца A существует такой элемент $x \in A$, что $x \equiv x_i \pmod{\mathfrak{a}_i}$ при всех i.*

Доказательство — по индукции. Если $n = 2$, то имеем

$$1 = a_1 + a_2$$

для некоторых элементов $a_i \in \mathfrak{a}_i$ и можно положить $x = x_2 a_1 + x_1 a_2$.

Предположим, что теорема доказана для семейства из $n-1$ идеалов. Для каждого $i \geqslant 2$ мы можем найти элементы $a_i \in \mathfrak{a}_1$ и $b_i \in \mathfrak{a}_i$, такие, что

$$a_i + b_i = 1, \qquad i \geqslant 2.$$

Произведение $\prod_{i=2}^{n} (a_i + b_i)$ равно 1 и лежит в $\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i$, т. е. в $\mathfrak{a}_1 + \mathfrak{a}_2 \ldots \mathfrak{a}_n$. Следовательно,

$$\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i = A.$$

В силу справедливости теоремы при $n = 2$ мы можем найти такой элемент $y_1 \in A$, что

$$y_1 \equiv 1 \pmod{\mathfrak{a}_1},$$
$$y_1 \equiv 0 \left(\operatorname{mod} \prod_{i=2}^{n} \mathfrak{a}_i\right).$$

Аналогично найдутся такие элементы $y_2, \ldots, y_n$, что $y_j \equiv 1 \pmod{\mathfrak{a}_j}$ и $y_j \equiv 0 \pmod{\mathfrak{a}_i}$ при $i \neq j$. Тогда элемент $x = x_1 y_1 + \ldots + x_n y_n$ удовлетворяет нашим требованиям.

Еще одно замечание в том же духе: если $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — такие идеалы в A, что

$$\mathfrak{a}_1 + \ldots + \mathfrak{a}_n = A,$$

и если $\nu_1, \ldots, \nu_n$ — положительные целые числа, то

$$\mathfrak{a}_1^{\nu_1} + \ldots + \mathfrak{a}_n^{\nu_n} = A.$$

Доказательство тривиально и предоставляется читателю в качестве упражнения.

Следствие. *Пусть A — кольцо и $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — идеалы в A. Предположим, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ при $i \neq j$. Пусть*

$$f\colon A \to \prod_{i=1}^{n} A/\mathfrak{a}_i = (A/\mathfrak{a}_1) \times \ldots \times (A/\mathfrak{a}_n)$$

— отображение кольца A в написанное произведение, индуцированное каноническими отображениями A на $A/\mathfrak{a}_i$ для каждого множителя. Тогда ядро отображения f есть $\bigcap_{i=1}^{n} \mathfrak{a}_i$ и f сюръективно, что приводит, таким образом, к изоморфизму

$$A/\bigcap \mathfrak{a}_i \xrightarrow{\approx} \prod A/\mathfrak{a}_i.$$

Доказательство. Утверждение о ядре очевидно. Сюръективность вытекает из предыдущей теоремы.

Теорема и ее следствие часто применяются к кольцу целых чисел $\mathbf{Z}$ и к попарно различным простым идеалам $(p_1), \ldots, (p_n)$. Они удовлетворяют предпосылкам теоремы, поскольку являются максимальными. Аналогично можно взять целые числа $m_1, \ldots, m_n$, попарно взаимно простые, и применить теорему к главным идеалам $(m_1) = m_1\mathbf{Z}, \ldots, (m_n) = m_n\mathbf{Z}$. Это ультраклассический случай китайской теоремы об остатках.

Пусть, в частности, m — целое число > 1 и

$$m = \prod_i p_i^{r_i}$$

— разложение m на простые сомножители с показателями $r_i \geqslant 1$. Тогда имеем изоморфизм колец

$$\mathbf{Z}/m\mathbf{Z} \approx \prod_i \mathbf{Z}/p_i^{r_i}\mathbf{Z}.$$

Если A — кольцо, то обозначаем, как обычно, через A^* мультипликативную группу обратимых элементов в A. Мы предоставляем следующее утверждение читателю в качестве упражнения.

Предыдущий кольцевой изоморфизм $\mathbf{Z}/m\mathbf{Z}$ на произведение индуцирует изоморфизм групп

$$(\mathbf{Z}/m\mathbf{Z})^* \approx \prod_i \left(\mathbf{Z}/p_i^{r_i}\mathbf{Z}\right)^*.$$

В силу этого изоморфизма имеем

$$\varphi(m) = \prod_i \varphi\left(p_i^{r_i}\right).$$

Если p — простое число и r — целое число $\geqslant 1$, то

$$\varphi(p^r) = (p-1)\,p^{r-1}.$$

Последняя формула доказывается по индукции. Если $r=1$, то $\mathbf{Z}/p\mathbf{Z}$ — поле и мультипликативная группа этого поля имеет порядок $p-1$. При $r \geqslant 1$ рассмотрим канонический гомоморфизм колец

$$\mathbf{Z}/p^{r+1}\mathbf{Z} \to \mathbf{Z}/p^r\mathbf{Z},$$

порожденный включением идеалов $(p^{r+1}) \subset (p^r)$. Индуцированный им гомоморфизм групп

$$\lambda\colon\ (\mathbf{Z}/p^{r+1}\mathbf{Z})^* \to (\mathbf{Z}/p^r\mathbf{Z})^*$$

сюръективен, потому что любое целое число a, представляющее некоторый элемент из $\mathbf{Z}/p^r\mathbf{Z}$ и взаимно простое с p, будет представлять также некоторый элемент из $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$. Пусть a — целое число, представляющее такой элемент из $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$, что $\lambda(a)=1$. Тогда

$$a \equiv 1 \pmod{p^r\mathbf{Z}}$$

и, следовательно, мы можем написать

$$a \equiv 1 + xp^r \pmod{p^{r+1}\mathbf{Z}}$$

для некоторого $x \in \mathbf{Z}$. Значения $x = 0, 1, \ldots, p-1$ приводят к p различным элементам из $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$, которые все лежат в ядре λ. Но в качестве элемента x в предыдущем сравнении всегда может быть выбрано одно из этих p чисел, поскольку всякое целое число сравнимо с одним из них по модулю p. Следовательно, ядро λ имеет порядок p и наша формула доказана.

Отметим, что ядро λ изоморфно группе $\mathbf{Z}/p\mathbf{Z}$. (Доказательство?)

Пусть A — кольцо. Обозначим на минуту его единичный элемент через e. Отображение

$$\lambda\colon\ \mathbf{Z} \to A,$$

для которого $\lambda(n) = ne$, будет, очевидно, кольцевым гомоморфизмом с идеалом-ядром (n), порожденным некоторым целым числом $n \geqslant 0$. Канонический инъективный гомоморфизм $\mathbf{Z}/n\mathbf{Z} \to A$ является (кольцевым) изоморфизмом между $\mathbf{Z}/n\mathbf{Z}$ и некоторым подкольцом в A. Если A — целостное, то $n\mathbf{Z}$ — простой идеал и, следовательно, $n=0$ или $n=p$, где p — некоторое простое число. В первом случае A содержит в качестве подкольца кольцо, изоморфное $\mathbf{Z}$ и часто отождествляемое с $\mathbf{Z}$. В этом случае мы говорим, что A имеет *характеристику* 0. Если же $n=p$, то мы говорим, что A имеет *характеристику* p; в этом случае A содержит (изоморфный образ) $\mathbf{F}_p$ в качестве подкольца[1]).

[1]) В дальнейшем употребляется также краткое обозначение $\operatorname{char} A = 0$ или p. — *Прим. ред.*

Всякое поле K имеет характеристику 0 или $p > 0$. В первом случае K содержит в качестве подполя изоморфный образ поля рациональных чисел, а во втором случае оно содержит изоморфный образ поля $\mathbf{F}_p$. В обоих случаях это подполе будет называться *простым полем* (содержащимся в K). Так как это простое поле является наименьшим подполем в K, содержащим 1 и не имеющим автоморфизмов, кроме тождественного, его обычно отождествляют с $\mathbf{Q}$ или $\mathbf{F}_p$, в зависимости от того, какой случай имеет место.

Под *простым кольцом* (в K) мы будем понимать либо кольцо целых чисел $\mathbf{Z}$, если K имеет характеристику 0, либо $\mathbf{F}_p$, если K имеет характеристику p.

§ 3. Локализация

Мы продолжаем предполагать, что „кольцо“ означает „коммутативное кольцо“.

Пусть A — некоторое кольцо. Под *мультипликативным подмножеством* в A мы будем понимать подмоноид в кольце A (рассматриваемом как мультипликативный моноид согласно КО 2). Другими словами, это есть подмножество S, содержащее 1 и вместе с любыми двумя элементами x, y их произведение xy.

Мы построим сейчас *кольцо частных кольца A по S*, известное также под названием *кольца отношений кольца A по S*.

Рассмотрим пары (a, s), где $a \in A$ и $s \in S$. Определим отношение

$$(a, s) \sim (a', s')$$

между такими парами следующим условием: существует элемент $s_1 \in S$, для которого

$$s_1(s'a - sa') = 0.$$

Тривиально проверяется, что это будет отношение эквивалентности; класс эквивалентности, содержащий пару (a, s), обозначается через a/s. Множество классов эквивалентности обозначается символом $S^{-1}A$.

Отметим, что если $0 \in S$, то $S^{-1}A$ солержит ровно один элемент, а именно $0/1$.

Условием

$$(a/s)(a'/s) = aa'/ss'$$

в $S^{-1}A$ вводится умножение Тривиально проверяется, что это умножение правильно определено. Оно имеет единичный элемент, а именно $1/1$, и, очевидно, ассоциативно.