§ 4. Кольца главных идеалов

И в этом параграфе „кольцо" означает „коммутативное кольцо".

Пусть A — целостное кольцо. Элемент $a \neq 0$ называется *неприводимым*, если он не является единицей и если из равенства $a = bc$ с $b \in A$ и $c \in A$ следует, что b или c — единица.

Пусть $a \neq 0$ — некоторый элемент в A, и пусть главный идеал (a) простой. Тогда a неприводим. Действительно, если $a = bc$, то один из множителей, скажем b, лежит в (a). Тогда мы можем написать $b = ad$, где d — некоторый элемент из A и, следовательно, $a = acd$. Поскольку A целостное, отсюда следует, что $cd = 1$, другими словами, что c — единица.

Утверждение, обратное предыдущему, верно не всегда. Мы обсудим, при каких условиях оно верно. Говорят, что элемент $a \in A$, $a \neq 0$, обладает *однозначным разложением на неприводимые элементы*, если в A существуют единица u и неприводимые элементы p_i $(i = 1, \ldots, r)$, такие, что

$$a = u \prod_{i=1}^{r} p_i,$$

причем для двух таких разложений на неприводимые элементы

$$a = u \prod_{i=1}^{r} p_i = u' \prod_{j=1}^{s} q_j,$$

мы имеем $r = s$ и после перестановки индексов i $p_i = u_i q_i$, где u_i — некоторые единицы в A, $i = 1, \ldots, r$.

Отметим, что если p — неприводимый элемент и u — единица, то up — тоже неприводимый элемент, так что при разложении на множители мы должны допускать умножение на единицы. В кольце целых чисел $\mathbf{Z}$ отношение порядка позволяет нам выделить один неприводимый элемент (положительное простое число) из двух возможных (а именно, $\pm p$), отличающихся друг от друга на множитель, являющийся единицей. В более общих кольцах это, конечно, невозможно.

Допуская в предыдущем равенстве $r = 0$, мы принимаем соглашение, что всякая единица кольца A имеет разложение на неприводимые элементы.

Кольцо называется *факториальным* (или кольцом с однозначным разложением на множители), если оно целостное и если всякий элемент $\neq 0$ имеет однозначное разложение на неприводимые элементы. Мы докажем ниже, что всякое целостное кольцо главных идеалов факториально.

Пусть A — целостное кольцо и $a, b \in A$, $ab \neq 0$. Мы говорим, что *a делит b*, и пишем $a \mid b$, если существует элемент $c \in A$, для

которого $ac=b$. Мы говорим, что элемент $d\in A$, $d\neq 0$, является *наибольшим общим делителем* (сокращенно н. о. д.) элементов a и b, если $d\mid a$, $d\mid b$ и если любой элемент e из A, $e\neq 0$, делящий и a, и b, делит также d.

Предложение 2. *Пусть A — целостное кольцо главных идеалов и $a, b\in A$, $a, b\neq 0$. Если $(a, b)=(c)$, то c — наибольший общий делитель элементов a и b.*

Доказательство. Так как b лежит в идеале (c), то $b=xc$ для некоторого $x\in A$, или, что то же самое, $c\mid b$. Аналогично $c\mid a$. Пусть d делит и a, и b, т. е. $a=dy$, $b=dz$, где $y, z\in A$. Так как c лежит в (a, b), то

$$c=wa+tb$$

с некоторыми $w, t\in A$. Тогда $c=w\,dy+t\,dz=d(wy+tz)$, откуда $d\mid c$ и наше предложение доказано.

Теорема 1. *Всякое целостное кольцо A главных идеалов факториально.*

Доказательство. Мы докажем сначала, что всякий ненулевой элемент в A имеет разложение на неприводимые элементы. Обозначим через S — множество главных идеалов $\neq 0$, образующие которых не имеют разложения на неприводимые элементы; предположим, что S не пусто. Пусть (a_1) лежит в S. Рассмотрим произвольную возрастающую цепочку

$$(a_1)\subsetneqq(a_2)\subsetneqq\ \ldots\subsetneqq(a_n)\subsetneqq\ \ldots$$

идеалов из S. Мы утверждаем, что она не может быть бесконечной. Действительно, объединение идеалов такой цепочки будет идеалом в A, причем главным, равным, скажем (a). Образующая a должна лежать в некотором элементе цепочки, скажем в (a_n), а тогда

$$(a_n)\subset(a)\subset(a_n),$$

откуда вытекает, что цепочка обрывается на (a_n). Следовательно любой идеал в A, содержащий (a_n) и $\neq(a_n)$, имеет образующую допускающую разложение на неприводимые множители.

Заметим теперь, что элемент a_n не может быть неприводимым (иначе он имел бы разложение) и, следовательно, $a_n=bc$, где ни b, ни c не являются единицей. Но тогда $(b)\neq(a_n)$ и $(c)\neq(a_n)$, а потому и b, и c обладают разложениями на неприводимые множители. Произведение этих разложений будет разложением для a_n вопреки предположению, что S не пусто.

Чтобы доказать единственность, заметим сначала, что если p — неприводимый элемент в A, $a, b\in A$, $p\mid ab$, то $p\mid a$ или $p\mid b$. Дока-

зательство. Если $p \nmid a$, то н. о. д. элементов p и a равен 1 и, следовательно,

$$1 = xp + ya$$

для некоторых $x, y \in A$. Тогда $b = bxp + yab$, а поскольку $p \mid ab$, мы заключаем, что $p \mid b$.

Предположим теперь, что a имеет два разложения

$$a = p_1 \ldots p_r = q_1 \ldots q_s$$

на неприводимые элементы. Так как p_1 делит произведение, стоящее справа, то p_1 делит один из его сомножителей, причем после их перенумерации мы можем считать, что это q_1. Тогда найдется единица u_1, для которой $q_1 = u_1 p_1$. Сокращая оба разложения на p_1, получаем

$$p_2 \ldots p_r = u_1 q_2 \ldots q_s.$$

Доказательство завершается по индукции.

Можно было бы называть два элемента $a, b \in A$ эквивалентными, если существует единица u, такая, что $a = bu$. Выберем по одному элементу p из каждого класса эквивалентности, состоящего из неприводимых элементов, и обозначим через P множество таких представителей. Пусть $a \in A$, $a \neq 0$. Тогда существуют единица u и целые числа $\nu(p) \geqslant 0$, равные 0 для почти всех $p \in P$, такие, что

$$a = u \prod_{p \in P} p^{\nu(p)}.$$

При этом единица u и целые числа $\nu(p)$ однозначно определены элементом a. Мы называем $\nu(p)$ *порядком* элемента a в p, обозначая его также символом $\operatorname{ord}_p a$.

Если A — факториальное кольцо, то всякий неприводимый элемент p порождает простой идеал (p). Поэтому в факториальном кольце неприводимые элементы будут также называться *простыми*.

Заметим, что можно обычным способом определить понятие *наименьшего общего кратного* (н. о. к.) конечного числа ненулевых элементов кольца A. Именно, мы полагаем н. о. к. элементов $a_1, \ldots, a_n \in A$ равным любому элементу $c \in A$, удовлетворяющему условию

$$\operatorname{ord}_p c = \max_i \operatorname{ord}_p a_i$$

для всех простых элементов p из A. Такой элемент c определен однозначно с точностью до множителя, являющегося единицей.

Мы говорим, что ненулевые элементы $a, b \in A$ *взаимно просты*, если $(a, b) = (1)$. Это означает, что н. о. д. элементов a и b есть единица.

Пример Кольцо целых чисел $\mathbf{Z}$ факториально. Его группа единиц состоит из 1 и -1. Естественно брать в качестве представителя класса

эквивалентности данного простого элемента положительный простой элемент (называемый простым числом) при возможном выборе из двух элементов p и $-p$. Аналогично, как мы покажем позднее, кольцо многочленов от одной переменной над полем факториально, и в качестве представителей простых элементов в этом кольце обычно выбирают неприводимые многочлены со старшим коэффициентом 1.

УПРАЖНЕНИЯ

Все кольца предполагаются коммутативными

1. Пусть A — кольцо с $1 \neq 0$, S — его мультипликативное подмножество, не содержащее 0. Пусть, далее, $\mathfrak{p}$ — максимальный элемент в множестве идеалов кольца A, пересечение которых с S пусто. Показать, что $\mathfrak{p}$ — простой.

2. Пусть $f\colon A \to A'$ — сюръективный гомоморфизм колец. Показать, что если кольцо A — локальное, то и кольцо A' — локальное.

3. Пусть A — кольцо и $\mathfrak{p}$ — простой идеал. Показать, что $A_{\mathfrak{p}}$ имеет единственный максимальный идеал, состоящий из всех элементов вида a/s, где $a \in \mathfrak{p}$ и $s \notin \mathfrak{p}$.

4. Пусть A — кольцо главных идеалов и S — его мультипликативное подмножество. Показать, что $S^{-1}A$ — кольцо главных идеалов.

5. Пусть A — факториальное кольцо и S — его мультипликативное подмножество. Показать, что $S^{-1}A$ факториально и что простые элементы в $S^{-1}A$ — это те простые p из A, для которых $(p) \cap S$ пусто.

6. Пусть A — кольцо главных идеалов, $a_1, \ldots, a_n$ — ненулевые элементы из A и $(a_1, \ldots, a_n) = (d)$. Показать, что d — наибольший общий делитель для a_i $(i = 1, \ldots, n)$.

7. Пусть p — простое число, A — кольцо $\mathbf{Z}/p^r\mathbf{Z}$ (r — целое число $\geqslant 1$). Пусть $G = A^*$ — группа единиц в A, т. е. группа классов вычетов по модулю p^r, взаимно простых с модулем. Показать, что G — циклическая, за исключением случая, когда

$$p = 2, \quad r \geqslant 3;$$

в этом случае она является группой типа $(2, 2^{r-2})$.

[*Указание*: в общем случае показать, что G — произведение циклической группы, порожденной элементом $1 + p$, на циклическую группу порядка $p - 1$. В исключительном случае показать, что G — произведение группы $\{\pm 1\}$ на циклическую группу, порожденную классом вычетов числа 5 по модулю 2^r.]

8. Пусть i — комплексное число $\sqrt{-1}$. Показать, что $\mathbf{Z}[i]$ — кольцо главных идеалов и, следовательно, факториально. Каковы в нем единицы?

9. Пусть A — кольцо целых функций на комплексной плоскости. Показать, что всякий конечно порожденный идеал в A является главным. Каковы главные простые идеалы в A? Каковы единицы в A? Показать, что A не факториально.