В этой лекции рассматриваются только коммутативные кольца.

Часть 1. Идеалы

Пусть A — коммутативное кольцо.

Определение 1.1. Элемент $a \in A$ называется делитетем нуля, если $a \neq 0$ и существует $0 \neq b \in A$, так что $ab = 0$. Кольцо A называется целостным (областью целостности), если в нем нет делителей нуля и $1 \neq 0$.

Примеры 1.2. 1. Всякое поле является целостным кольцом.
2. Кольца $\mathbb{Z}$ и $K[x]$ — целостные.
3. Кольцо $\mathbb{Z}/n\mathbb{Z}$ — целостное тогда и только тогда, когда n — простое число.

Определение 1.3. Идеал $\mathfrak{p} \subset A$ называется простым, если кольцо $A/\mathfrak{p}$ — целостное.

Пример 1.4. Идеал $n\mathbb{Z} \subset \mathbb{Z}$ — простой, тогда и только тогда, когда n — простое число.

Лемма 1.5. *Идеал $\mathfrak{p} \subset A$ — простой $\iff \mathfrak{p} \neq A$ и $\forall x, y \in A$, если $xy \in \mathfrak{p}$, то либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$.*

Доказательство: обозначим через $\bar{x}$ образ элемента $x \in A$ в кольце $A/\mathfrak{p}$. Если $\mathfrak{p}$ — простой, и $xy \in \mathfrak{p}$, то $\bar{x}\bar{y} = 0$, следовательно либо $\bar{x} = 0$, либо $\bar{y} = 0$ (так как $A/\mathfrak{p}$ — целостное), значит либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$. Аналогично доказывается обратное утверждение. $\square$

Следствие 1.6. *Кольцо A — целостное $\iff \{0\} \subset A$ — простой идеал.*

Определение 1.7. Идеал $\mathfrak{m} \subset A$ называется максимальным, если $\mathfrak{m} \neq A$ и не существует идеала $\mathfrak{m} \subset \mathfrak{a} \subset A$, такого что $\mathfrak{m} \neq \mathfrak{a} \neq A$.

Лемма 1.8. *Идеал $\mathfrak{m} \subset A$ — максимальный $\iff A/\mathfrak{m}$ — поле.*

Доказательство: пусть $f : A \to A/\mathfrak{m}$ — каноническая проекция. Если $\mathfrak{a} \subset A$ — идеал, такой что $\mathfrak{m} \subset \mathfrak{a}$, то $\mathfrak{a}/\mathfrak{m} = f(\mathfrak{a}) \subset A/\mathfrak{m}$ — идеал. Аналогично, если $\mathfrak{b} \subset A/\mathfrak{m}$ — идеал, то $\mathfrak{a} = f^{-1}(\mathfrak{b}) \subset A$ — идеал, такой что $\mathfrak{m} \subset \mathfrak{a}$. Поэтому $\mathfrak{m}$ — максимальный $\iff A/\mathfrak{m}$ не имеет нетривиальных идеалов. Покажем, что это выполнено тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

Если $A/\mathfrak{m}$ — поле, то всякий элемент $0 \neq x \in A/\mathfrak{m}$ обратим, следовательно любой ненулевой идеал в $A/\mathfrak{m}$ совпадает с $A/\mathfrak{m}$. Обратно, пусть кольцо $B = A/\mathfrak{m}$ не имеет нетривиальных идеалов. Возьмем произвольный $0 \neq x \in B$. Тогда идеал $xB \subset B$ — ненулевой, следовательно $xB = B$, то есть $1_B \in xB$, то есть $\exists y \in B$, так что $xy = 1_B$. Значит x — обратим и B — поле. $\square$

Следствие 1.9. *Всякий максимальный идеал является простым.*

Пример 1.10. В кольце $\mathbb{Z}$ имеем $n\mathbb{Z} \subset m\mathbb{Z} \iff m|n$. Поэтому $n\mathbb{Z}$ — максимальный $\iff n$ — простое число.

Лемма 1.11. *Пусть $\mathfrak{a} \neq A$ — идеал. Тогда существует максимальный идеал $\mathfrak{a} \subset \mathfrak{m} \subset A$.*

Доказательство: по лемме Цорна достаточно проверить, что для всякой цепочки идеалов $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset A$, в которой $\forall i\ \mathfrak{a}_i \neq A$, существует идеал $\mathfrak{a} \neq A$, такой что $\forall i\ \mathfrak{a}_i \subset \mathfrak{a}$. Возьмем $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$. Нам надо проверить, что 1) $\mathfrak{a}$ — идеал; 2) $\mathfrak{a} \neq A$. Действительно, если $x, y \in \mathfrak{a}$, то $x \in \mathfrak{a}_i$, $y \in \mathfrak{a}_j$ для каких-то i, j, следовательно $x, y \in \mathfrak{a}_k$, где $k = \max(i, j)$, следовательно $x + y \in \mathfrak{a}_k \subset \mathfrak{a}$. Аналогично проверяется, что $ax \in \mathfrak{a}\ \forall a \in A$. Стало быть, $\mathfrak{a}$ — идеал. Теперь предположим, что $\mathfrak{a} = A$. Тогда $1 \in \mathfrak{a}$, следовательно $\exists i$, так что $1 \in \mathfrak{a}_i$, значит $\mathfrak{a}_i = A$ — противоречие. $\square$

Следствие 1.12. *Всякий необратимый элемент кольца содержится в некотором максимальном идеале.*

Пусть A — целостное кольцо. Рассмотрим множество классов эквивалентности пар (a, s), $a \in A$, $s \in A \setminus \{0\}$, где $(a, s) \sim (b, t) \iff at = bs$. Обозначим класс пары (a, s) через a/s и будем называть его дробью.

Лемма 1.13. *Множество дробей* $F(A) = \{\, a/s \,\}$ *с операциями* $a/s + b/t = (at+bs)/st$, $(a/s)\cdot(b/t) = (ab)/(st)$ *является полем. Отображение* $\varphi : A \to F(A)$, $a \mapsto a/1$ *является мономорфизмом.*

Доказательство: непосредственная проверка.

Поле $F(A)$ называется полем частных кольца A.

Следствие 1.14. *Идеал* $\mathfrak{a} \subset A$ *— простой* $\iff$ $\mathfrak{a} = \operatorname{Ker} f$, *где* f *— гомоморфизм из* A *в некоторое поле.*

Часть 2. Кольца главных идеалов

Определение 2.1. Идеал $I \subset A$ называется главным, если $I = aA$, $a \in A$. Коммутативное кольцо A называется кольцом главных идеалов, если $1 \neq 0$ и всякий идеал в A — главный.

Говорят, что в кольце A возможно деление с остатком, если существует функция $\varphi : A \to \mathbb{Z}_{\geqslant 0}$, такая что $\varphi^{-1}(0) = \{\, 0 \,\}$ и для любых $a, b \in A$, $b \neq 0$ $\exists q, r \in A$ $a = bq + r$ и $\varphi(r) < \varphi(b)$.

Пример 2.2. В кольцах $\mathbb{Z}$ и $K[x]$ возможно деление с остатком: достаточно взять $\varphi(n) = |n|$ для $n \in \mathbb{Z}$ и $\varphi(p(x)) = \deg p(x) + 1$ для $p(x) \in K[x]$ (если положить $\deg 0 = -1$).

Лемма 2.3. *Если в кольце* A *возможно деление с остатком, то* A *— кольцо главных идеалов.*

Доказательство: пусть $I \subset A$ — идеал. Если $I = 0$, то I — главный. Предположим, что $I \neq 0$. Пусть $b \in I$ таков, что $\varphi(b) = \min\{\, \varphi(x) \mid 0 \neq x \in I \,\}$. Покажем, что $I = bA$. Действительно, пусть $a \in I$. Тогда $a = bq + r$, $\varphi(r) < \varphi(b)$. Но $r \in I$, значит $r = 0$ и $a \in bA$. □

Следствие 2.4. *Кольца* $\mathbb{Z}$ *и* $K[x]$ *являются кольцами главных идеалов.*

Определение 2.5. Пусть A — целостное кольцо. Элемент $d \in A$ называется делителем элемента $a \in A$, если $a = dc$ (обозначается $d|a$). Элемент $d \in A$ называется наибольшим общим делителем элементов $a, b \in A$, если $d|a$, $d|b$ и $\forall d' \in A$ $d'|a$, $d'|b \Longrightarrow d'|d$.

Ясно, что если наибольший общий делитель существует, то определен однозначно с точностью до умножения на обратимый элемент. Будем через НОД(a, b) обозначать любой из наибольших общих делителей.

Лемма 2.6. *Если* A *— кольцо главных идеалов,* $a, b \in A$, *то существует* НОД(a, b).

Доказательство: рассмотрим идеал $I = aA + bA$. Так как A — кольцо главных идеалов, то $I = dA$, $d \in A$. Покажем, что $d =$ НОД(a, b). Во-первых, $a \in aA \subset I = dA$, поэтому $d|a$. Аналогично, $d|b$. Далее, если $d'|a$ и $d'|b$, то $aA \subset d'A$, $bA \subset d'A$, поэтому $d \in dA = I = aA + bA \subset d'A$, значит $d'|d$. □

Замечание 2.7. Из доказательства леммы видно, что если $d =$ НОД(a, b), то существуют $x, y \in A$ такие что $d = ax + by$.

Еще одним важным свойством колец главных идеалов является нётеровость.

Лемма 2.8. *Если* A *— кольцо главных идеалов, то* A *— нётерово: всякая возрастающая цепочка идеалов* $I_1 \subset I_2 \subset \cdots \subset A$ стабилизируется, *то есть* $\exists n$ *такое что* $I_k = I_n$ *при* $k \geqslant n$.

Доказательство: возьмем $I = \bigcup_i I_i$. Как было показано выше I — идеал, следовательно $I = aA$. Так как $a \in I$, то $a \in I_n$ для некоторого n, значит $I = aA \subset I_n$, значит $I_n = I$, значит $I_k = I_n$ при $k \geqslant n$. □

Часть 3. Факториальность

Определение 3.1. Элемент $u \in A$ называется единицей, если он обратим. Элемент $a \in A$ называется неприводимым, если a не единица, но из равенства $a = bc$ следует, что либо b, либо c — единица в A.

Пример 3.2. В кольце $\mathbb{Z}$ единицами являются числа ± 1, а неприводимыми — числа $\pm p$, где p — простое.

Лемма 3.3. *Пусть* A *— целостное кольцо. Тогда* $aA = bA \iff a = bu$, *где* u *— единица.*

Доказательство: $a \in aA = bA$, поэтому $a = bu$. Аналогично $b = av$. Значит $a = avu$, следовательно $vu = 1$, то есть u — единица. $\square$

Лемма 3.4. *Если A — кольцо главных идеалов, p — неприводим и $p|ab$, то либо $p|a$, либо $p|b$.*

Доказательство: если $p \nmid a$, то НОД$(p, a) = 1$, следовательно $1 = px + ay$, значит $b = p(xb) + (ab)y$. Ясно, что p делит оба слагаемых в правой части равенства, поэтому $p|b$. $\square$

Лемма 3.5. *Если A — целостное и главный идеал $aA \subset A$ прост, то $a \in A$ — неприводим.*

Доказательство: если $0 \neq a = bc$, то $bc \in aA$, значит либо $b \in aA$, либо $c \in aA$. Если $b \in aA$, то $b = ad$, следовательно $a = adc$, следовательно $dc = 1$ и c — единица. $\square$

В кольце $\mathbb{Z}$ верно и обратное утверждение, однако в более общих кольцах это уже не так.

Определение 3.6. Элемент $0 \neq a \in A$ обладает однозначным разложением на неприводимые множители, если $a = u\prod_{i=1}^n p_i$, где u — единица, а p_i — неприводимы, и для любого другого такого разложения $a = u'\prod_{i=1}^m p'_i$ имеем $n = m$ и $p_i = u_i p'_i$, где u_i — единицы. Кольцо A называется факториальным, если оно целостное и всякий ненулевой элемент обладает однозначным разложением на неприводимые множители.

Пример 3.7. Хорошо известно, что в кольце $\mathbb{Z}$ всякий элемент обладает однозначным разложением на простые множители, то есть кольцо $\mathbb{Z}$ факториально. Примером не факториального кольца является кольцо $\mathbb{Z}[\sqrt{-5}] = \{\, a + b\sqrt{-5} \in \mathbb{C} \mid a, b \in \mathbb{Z} \,\}$. В этом кольце $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Теорема 3.8. *Если A — целостное кольцо главных идеалов, то A факториально.*

Доказательство: покажем вначале, что если $a \in A$ не является единицей, то a имеет неприводимый делитель. Преположим противное. Тогда существует разложение $a = a_1 b_1$, так что a_1 и b_1 — не единицы. Следовательно $aA \subset a_1 A$, причем по лемме 3.3 вложение строгое. Далее, если a_1 — неприводим, то все доказано, иначе же существует разложение $a_1 = a_2 b_2$, так что a_2 и b_2 — не единицы. Продолжая подобным образом, мы либо в конце концов найдем неприводимый делитель, либо построим нестабилизирующуся возрастающую цепочку идеалов $aA \subset a_1 A \subset a_2 A \subset \ldots$. Однако, из-зи нётеровости кольца A последнее невозможно. Следовательно, неприводимый делитель существует.

Докажем теперь, что a допускает разложение на неприводимые множители. Во-первых, a имеет неприводимый делитель, поэтому $a = a_1 p_1$, где p_1 неприводим. Далее, либо a_1 — единица, либо имеет неприводимый делитель, то есть $a_1 = a_2 p_2$. Продолжая подобным образом, мы либо в конце концов найдем разложение на неприводимые множители, либо построим нестабилизирующуся возрастающую цепочку идеалов $aA \subset a_1 A \subset a_2 A \subset \ldots$. Однако, из-зи нётеровости кольца A последнее невозможно. Следовательно, разложение на неприводимые множители существует.

Докажем теперь, что разложение единственно. Предположим, что $up_1 \ldots p_n = u' p'_1 \ldots p'_m$. Так как p_1 делит левую часть, то p_1 делит и правую часть, следовательно по лемме 3.4 он делит один из сомножителей правой части. Ясно, что $p_1 \nmid u'$, поэтому $p_1 | p'_i$. Переставляя в правой части сомножители, можно считать, что $p_1 | p'_1$. Следовательно, $p'_1 = p_1 u_1$, где u_1 — единица. Сокращая на p_1 получаем равенство $up_2 \ldots p_n = (u'u_1)p'_2 \ldots p'_m$. Далее единственность следует по индукции. $\square$

Следствие 3.9. *Кольца $\mathbb{Z}$ и $K[x]$ — факториальны.*

Замечание 3.10. Впоследствии мы докажем, что кольца $\mathbb{Z}[x]$ и $K[x_1, \ldots, x_n]$ факториальны, хотя и не являются кольцами главных идеалов.