Идеалы коммутативных колец

В рамках этой лекции все кольца предполагаются коммутативными с единицей. Некоммутативный случай будет рассмотрен на следующей лекции.

Определение 1. Пусть $f : K_1 \to K_2$ — отображение колец.
Ядро (kernel) отображения f — множество $\mathrm{Ker}(f) = \{x \in K_1 | f(x) = 0\} \subset K_1$.
Образ (image) отображения f — множество $\mathrm{Im}(f) = \{f(x) \in K_2 | x \in K_1\} \subset K_2$.

Ясно, что ядро и образ — подкольца. При этом любое подкольцо может быть образом отображения (вложения подкольца в кольцо), но ядро обладает следующими дополнительными свойствами.

Определение 2. *Идеал* $I \subset K$ — подмножество со следующими свойствами:
1) I — подгруппа по сложению (достаточно проверить, что если a, $b \in I$, то $a - b \in I$),
2) если $a \in I$, $x \in K$, то $ax \in I$.

Определение 3. Пусть $I \subset K$ — идеал. *Факторкольцо* K/I (quotient ring) — кольцо классов эквивалентности элементов K по отношению $x \sim y$, если $x - y \in I$.

Корректность сложения при этом следует из аксиомы 1) определения идеала, корректность умножения — из аксиомы 2). Аксиомы кольца наследуются для факторкольца из исходного кольца.

При этом любой идеал I является ядром естественной проекции $K \to K/I$, сопоставляющей каждому элементу его класс.

Пример. Кольцо $\mathbb{Z}/n\mathbb{Z}$ является факторкольцом $\mathbb{Z}$ по идеалу $n\mathbb{Z}$.

Заметим, что идеалы частично упорядочены по вложению.

Определение 4. Идеал, не совпадающий со всем кольцом называется *собственным.* Максимальный по вложению среди собственных идеалов называется *максимальным.*

Следующее определение будет встречаться довольно часто для разных объектов.

Определение 5. Идеал, *порождённый* множеством X — минимальный (по вложению) идеал, содержащий M.

Ясно, что в нашей общности коммутативных колец с единицей такой идеал состоит из элементов вида $x_1a_1 + \cdots + x_ma_m$, где $a_i \in X$, $x_i, \in K$.

Предложение 1 *Идеал, порождённый множеством X существует и единственен. Уравнение $a_1x_1 + \cdots + a_nx_n = c$ разрешимо в кольце K тогда и только тогда c принадлежит идеалу, порождённому $a_1, \ldots, a_n$.*

Определение 6. Идеал, порождённый конечным набором элементов $a_1, \ldots, a_n$, будем называть *конечнопорождённым* и обозначать $(a_1, \ldots, a_n)$. Идеал (a), порожденный одним элементом, называется *главным.*

Предложение 2 *В евклидовом кольце всякий идеал главный.*

Доказательство: Рассмотрим ненулевой элемент идеала с минимальной нормой. Тогда всякий другой элемент идеала на него делится с нулевым остатком.

Теперь мы можем доказать, что некоторые кольца не евклидовы.

Упражнение 1 *Докажите, что идеал $(x, y) \subset \mathbb{C}[x, y]$ не является главным.*

Тем не менее, кольцо $\mathbb{C}[x, y]$ факториально. Докажем это. Пусть кольцо K факториально. Тогда в нём определены наибольший общий делитель и наименьшее общее кратное любого конечного набора элементов: для этого у каждого простого множителя берётся соответственно минимальная и максимальная степень и рассматривается класс произведения этих степеней. Для простоты записи будем обозначать символом 1 также класс обратимых элементов, если это не приводит к разночтениям.

Определение 7. Пусть $P \in K[x]$. Определим *содержание многочлена* $\mathrm{cnt}(P)$ как наибольший общий делитель коэффициентов P.

Лемма 1 *Если P прост в $K[x]$, то либо $\mathrm{cnt}(P) = 1$, либо $\deg P = 0$.*

Доказательство: В противном случае многочлен представим произведением необратимой константы и многочлена положительной степени.

Лемма 2 *Имеет место равенство $\mathrm{cnt}(PQ) = \mathrm{cnt}(P) \cdot \mathrm{cnt}(Q)$.*

Доказательство: Ясно, что $\mathrm{cnt}(PQ)$ делится на $\mathrm{cnt}(P) \cdot \mathrm{cnt}(Q)$. Сокращая на общие делители, достаточно доказать равенство для случая $\mathrm{cnt}(P) = \mathrm{cnt}(Q) = 1$. Предположим, $\mathrm{cnt}(PQ)$ содержит класс элемента $n \neq 1$, пусть p — простой делитель n. Тогда пусть a_i — первый коэффициент $P(x) = a_n x^n + \cdots + a_0$, не делящийся на p (то есть $p | a_k$ при $k < i$), аналогично пусть b_j — первый коэффициент $Q(x)$, не делящийся на p. Тогда $i + j$–тый коэффициент PQ не делится на p, что противоречит предположению.

Ключевой момент доказательства факториальности $K[x]$ — переход от $K[x]$ к большему кольцу $F(K)[x]$, где $F(K)$ — поле частных K. Другими словами, мы разрешаем делить многочлены на элементы K.

Лемма 3 *Если $P \in K[x]$ прост, $\deg(P) > 0$, то P прост и в $F(K)[x]$.*

Доказательство: Предположим, $P = R_1 R_2$ в $F(K)[x]$, где $\deg(R_i) > 1$, $i = 1, 2$. Тогда $R_i = \frac{m_i}{n_i} P_i$, где $P_i \in K[x]$ и $\mathrm{cnt}(P_i) = 1$. Значит, в $K[x]$ выполнено равенство $n_1 n_2 P = m_1 m_2 P_1 P_2$. Сравнивая содержания левой и правой части по Лемме 2, получим $n_1 n_2 \sim m_1 m_2$ и P отличается от $P_1 P_2$ на обратимый множитель.

Теорема 1 *Если кольцо K факториально, то и $K[x]$ факториально.*

Доказательство: Существование разложения доказывается по индукции аналогично евклидовому случаю, используя понижение степени или содержания. Кроме того, по Лемме 1 и Лемме 2 это представление имеет вид $P = p_1 \dots p_s \cdot P_1 \dots P_n$, где $p_i \in K$, $p_1 \dots p_s$ эквивалентно $\mathrm{cnt}(P)$, и $\deg(P_i) > 0$, $\mathrm{cnt}(P_i) = 1$. В силу факториальности K классы p_i определены однозначно, поэтому достаточно доказать единственность разложения для случая $\mathrm{cnt}(P) = 1$.

Пусть такой P разлагается на простые множители в $K[x]$ двумя способами, то есть $P = P_1 \dots P_n = Q_1 \dots Q_m$ где P_i, $Q_i \in K[x]$ — простые элементы ненулевой степени. Докажем, что они эквивалентны с точностью до перестановки.

Вспомним, что $F(K)[x]$ факториально, значит по Лемме 3 выполнено $m = n$ и Q_i отличаются от соответствующих P_j множителями из $F(K)$, то есть $pQ_i = qP_j$, где $p, q \in K$. Но так как $\mathrm{cnt}(P_j) = \mathrm{cnt}(Q_i) = 1$, имеем $p \sim q$ в K и $Q_i \sim P_j$ в $K[x]$.

Следствие 1 *Если K факториально, то $K[x_1, \dots, x_n]$ тоже факториально.*

Определение 8. *Пересечение* идеалов $I_1 \cap I_2$ — пересечение соответствующих множеств.

Сумма идеалов $I_1 + I_2$ — идеал, порождённый $I_1 \cup I_2$. Он состоит из элементов $a + b$, где $a \in I_1$, $b \in I_2$.

Произведение идеалов $I_1 I_2$ — идеал, порождённый элементами ab, где $a \in I_1$, $b \in I_2$.

Упражнение 2 *Идеалы с операциями сложения и умножения образуют полукольцо.*

Упражнение 3 *В евклидовом кольце сумма идеалов соответствует НОД образующих, произведение — произведению, пересечение — НОК.*

Определение 9. Определим *декартово произведение* колец/групп $K_1 \times K_2$ как множество пар (a, b), $a \in K_1$, $b \in K_2$ с операциями

$$(a, b) + (a', b') = (a + a', b + b'), \qquad (a, b) \cdot (a', b') = (a \cdot a', b \cdot b').$$

Предложение 3 *Пусть K — коммутативно, I_1, $I_2 \subset K$ — идеалы. Пусть $I_1 + I_2 = K$, тогда $K/(I_1 \cap I_2) \cong K/I_1 \times K/I_2$.*

Доказательство: Пара естественных проекций задаёт отображение $K \to K/I_1 \times K/I_2$. Ядро этого отображения совпадает с $I_1 \cap I_2$. А чтобы убедиться, что это отображение — наложение, достаточно решить уравнение $r + x = s + y$ относительно переменных $x \in I_1$ и $y \in I_2$ при произвольных r, $s \in K$, что возможно в силу $I_1 + I_2 = K$.

Следствие 2 Китайская теорема об остатках *Пусть K евклидово, a, $b \in K$ взаимно просты. Тогда $K/abK \cong K/aK \times K/bK$.*

Определение 10. Пусть K — коммутативное кольцо. Идеал I называется *простым*, если он отличен от нуля и K, и из $ab \in I$ следует $a \in I$ или $b \in I$.

Упражнение 4 *Идеал прост тогда и только тогда факторкольцо не имеет делителей нуля.*

Пример. Рассмотрим кольцо $K = Z[\sqrt{-5}]$. Оно не является факториальным так как

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 - \sqrt{-5}),$$

и простота этих сомножителей доказывается аналогичным вычислением комплексной нормы. Но при этом

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}), \qquad (3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}),$$

и идеал (6) разложился в произведение этих четырёх простых идеалов.

Определение 11. Целостное кольцо, в котором идеалы однозначно распадаются в произведение простых, называется *дедекиндовым.*

Пример. Кольцо $K = Z[\sqrt{-3}]$ не является ни факториальным, ни дедекиндовым, так как идеал (2) содержится только в идеале $(2, 1+\sqrt{-3})$ и не является его степенью. Тем не менее, добавление чисел виде $(a + b\sqrt{-3})/2$ с нечётными a и b делает это кольцо евклидовым.

Предложение 4 *Всякое простое поле изоморфно $\mathbb{Q}$ или $\mathbb{Z}/p\mathbb{Z}$ для простого $p \in \mathbb{N}$.*

Доказательство: Рассматривая элементы $\pm(1+\cdots+1)$, получим отображение колец $\iota : \mathbb{Z} \to F$. Так как в F нет делителей нуля, либо ядро ι равно нулю, либо оно является простым идеалом в $\mathbb{Z}$. В первом случае ι продолжается до вложения соответствующего поля частных $\mathbb{Q}$ в F, во втором случае оно является вложением $\mathbb{Z}/p\mathbb{Z}$ в F. В силу простоты F, это вложение является изоморфизмом.

Определение 12. *Характеристика (characteristic)* поля — целое число, полагаемое равным нулю, если простое подполе изоморфно $\mathbb{Z}$, и равным p, если оно изоморфно $\mathbb{Z}/p\mathbb{Z}$.