

5. ЛЕКЦИЯ 5. ИДЕАЛЫ, ТЕОРЕМА О ГОМОМОРФИЗМАХ, ЕВКЛИДОВЫ И
ФАКТОРИАЛЬНЫЕ КОЛЬЦА.

5.1. **Идеалы и фактор-кольца.** Пусть R – коммутативное кольцо с единицей.

Определение 5.1. Идеал $I \subset R$ – это такое подкольцо в R , что $a \cdot b \in I \forall a \in R, b \in I$.

Ясно, что идеал задаёт отношение эквивалентности на R , а значит и разбиение кольца R на классы эквивалентности. Обозначим множество классов эквивалентности через R/I , а класс $x \in R$ будем обозначать через $[x]$.

Пример 5.2. $I = n\mathbb{Z} \subset \mathbb{Z}$ – идеал. Классы эквивалентности выглядят так:

$$\begin{aligned} &\{\dots, -n, 0, n, \dots\} \\ &\{\dots, -n+1, 1, n+1, \dots\} \\ &\dots \\ &\{\dots, -1, n-1, 2n-1, \dots\} \end{aligned}$$

Предложение 5.3. R/I – коммутативное кольцо с единицей:

$$\begin{aligned} [x] + [y] &:= [x + y] \\ [x] \cdot [y] &:= [xy] \end{aligned}$$

Доказательство. Если $[x_1] = [x_2]$ и $[y_1] = [y_2]$, то $x_1 = x_2 + i_1, y_1 = y_2 + i_2$ и

$$\begin{aligned} [x_1] + [y_1] &= [x_2 + y_2 + i_1 + i_2] = [x_2 + y_2] = [x_2] + [y_2] \\ [x_1][y_1] &= [x_2y_2 + i_1y_2 + i_2y_1 + i_1i_2] = [x_2y_2] = [x_2][y_2] \end{aligned}$$

□

Пример 5.4. Пусть $f \in R[x]$. Тогда $(f) = \{fg \mid g \in \mathbb{k}[x]\}$ – идеал и определено кольцо $R[x]/(f)$. В случае $R = \mathbb{k}$ это кольцо изоморфно кольцу остатков по модулю f .

5.2. **Теорема о гомоморфизме.**

Предложение 5.5. Пусть $\varphi : R \rightarrow S$ – гомоморфизм колец. Тогда

- (1) $\text{Im } \varphi$ подкольцо в S ;
- (2) $\text{Ker } \varphi$ – идеал в R ;
- (3) $R/\text{ker } \varphi \simeq \text{Im } \varphi$

Доказательство. (1) Если $y_1 = f(x_1)$ и $y_2 = f(x_2)$, то $y_1 + y_2 = f(x_1) + f(x_2) = f(x_1 + x_2)$ и $y_1y_2 = f(x_1)f(x_2) = f(x_1x_2)$.

(2) Если $f(x_1) = f(x_2) = 0$, то $f(x_1 + x_2) = f(x_1) + f(x_2) = 0$. Если $f(x_1) = 0$ и $r \in R_1$, то $f(rx_1) = f(r)f(x_1) = 0$.

(3) Определим отображение

$$f : R/\text{ker } \varphi \rightarrow \text{Im } \varphi, [x] \mapsto f(x)$$

Это отображение корректно определено: если $[x_1] = [x_2]$, то $x_1 = x_2 + r$, где $r \in \text{ker } \varphi$. Тогда $f(x_2) = f(x_1 + r) = f(x_1) + f(r) = f(x_1)$.

Является гомоморфизмом: $f([x_1] + [x_2]) = f([x_1 + x_2]) = f(x_1) + f(x_2) = f([x_1]) + f([x_2])$. Аналогично для умножения.

Является биекцией: Если $f([x_1]) = 0$, то $x_1 \in \text{ker } \varphi$, а значит $[x_1] = 0$ в $R/\text{ker } \varphi$. Если $y \in \text{Im } \varphi$, то существует $x \in R_1$ такой, что $f(x) = y$, а значит $f([x]) = y$.

□

Примеры. 1) Пусть $L \supset \mathbb{K}$, $\alpha \in L$ поля и $m_\alpha(x) \in \mathbb{K}[x]$ – минимальный многочлен элемента α . Рассмотрим отображение $f : \mathbb{K}[x] \rightarrow L, f(x) \mapsto f(\alpha)$. Ясно, что $\text{Im } f = \{f(\alpha) \mid f \in \mathbb{K}[x]\} := \mathbb{K}[\alpha] \subset L$. Более того, f – гомоморфизм. Тогда

$$\mathbb{K}[\alpha] \simeq \mathbb{K}[x]/(m_\alpha(x)).$$

В частности, $\mathbb{K}[\alpha]$ – поле, так как $m_\alpha(x)$ неприводим.

2) Рассмотрим отображение $f : \mathbb{Z} \rightarrow \mathbb{Z}[i]/(1+3i), n \mapsto [n]$. Ясно, что f – гомоморфизм. Более того, $i-3 \in (1+3i)$, значит, отображение f – сюръективно. При этом $N(1+3i) = 10$, а значит если $[n] = 0$, то $n = (1+3i)(a+bi)$ и $a^2+b^2 = 1$, а значит $n = 10k, k \in \mathbb{Z}$. Отсюда $\mathbb{Z}/(10) \simeq \mathbb{Z}[i]/(1+3i)$.

5.3. Евклидовы кольца и кольца главных идеалов. Цель данного раздела – формализовать понятия деления с остатком и выделить основное свойство, которое использовалось для доказательства факториальности.

Определение 5.6. Евклидово кольцо – это область целостности R в которой задана функция: $N : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ так, что для любых $a, b \in R$ существуют $q, r \in R$ такие, что

$$a = bq + r, \quad N(r) < N(b) \text{ или } r = 0$$

Примеры евклидовых колец это $\mathbb{Z}, \mathbb{K}[x], \mathbb{Z}[i]$. Пусть R – кольцо и $M \subset R$ – произвольное множество элементов.

Определение 5.7. Идеал порождённый множеством – это

$$\langle M \rangle = \{a_1r_1 + \dots + a_nr_n \mid r_i \in R, a_i \in M\}$$

Определение 5.8. Идеал $I \subset R$ называется конечно-порождённым, если существует конечное $M \subset R$ такое, что $I = \langle M \rangle$.

Определение 5.9. Кольцо называется нётеровым, если любой идеал в этом кольце конечно-порождён.

Предложение 5.10. Нётеровость эквивалентна условию, что не существует бесконечно-возрастающих цепочек идеалов.

Доказательство. Легко видеть, что объединение произвольного семейства идеалов является идеалом. Это означает, что нётеровость кольца влечёт невозможность бесконечной возрастающей цепочки: иначе сможем построить идеал, который не может быть порождён конечным числом элементов. Обратно, если в кольце нет бесконечно-возрастающих цепочек, то сможем в любом идеале выбрать конечный порождающий набор. $\square$

Примеры. 1) Любое евклидово кольцо нётерово (см. ниже).

2) $\mathbb{K}[x_1, \dots, x_n, \dots]$ – кольцо многочленов от бесконечного числа переменных не является нётеровым.

3) Кольцо $C[0, 1]$ непрерывных вещественнозначных функций на отрезке $[0, 1]$ не является нётеровым (упражнение).

Заметим, что в контексте разложения на неприводимые элементы условие нётеровости гарантирует *существование* разложения на неприводимые множители. Действительно, иначе получили бы бесконечную цепочку возрастающих идеалов.

Теорема Гильберта о базисе утверждает, что кольцо многочленов над нётеровым кольцом является нётеровым.

Определение 5.11. Идеал $I \subset R$ называется главным, если $I = \langle r \rangle := (r)$ для некоторого $r \in R$.

В терминах этих понятий, легко формализовать понятия неприводимого и простого элемента области целостности.

Определение 5.12. Элемент $a \in R$ неприводим, если идеал (a) является максимальным идеалом среди собственных главных.

Определение 5.13. Элемент $p \in R$ является простым, если $R/(p)$ – область целостности.

Определение 5.14. Идеал $I \subset R$ называется простым, если R/I – область целостности.

Определение 5.15. Идеал $I \subset R$ называется максимальным, если R/I – поле.

Предложение 5.16. Максимальный идеал является максимальным собственным идеалом в теоретико-множественном смысле.

Доказательство. ($\Rightarrow$) Пусть R/I – поле. Докажем, что $\langle I, x \rangle = R$ для любого $x \in R$, отсюда будет следовать максимальность I . Действительно, существует $y \in R$ такое, что $[x] \cdot [y] = [1]$. Это означает, что существует $i \in I$ такой, что $xy = 1 + i$. Тогда $1 \in \langle I, x \rangle$, а, значит, $\langle I, x \rangle = R$.

($\Leftarrow$) Пусть I – максимальный. Тогда для любого $x \in R$ имеем $\langle x, I \rangle = R$, а значит существует $y \in R$ и $i \in I$ такие, что $xy + i = 1$, откуда $[x]^{-1} = [y]$. $\square$

Несложно видеть, что корректность определения НОД в евклидовом кольце R связана с тем, что для любых a, b идеал (a, b) порождён одним элементом.

Предложение 5.17. Евклидово кольцо является областью главных идеалов.

Доказательство. Пусть R – евклидово и $I \subset R$ – идеал. Пусть $x \in I$ – элемент минимальной нормы. Тогда $I = (x)$. Действительно, если существует $y \in I, y \notin (d)$, то $y = dq + r$, причём $N(r) < N(d)$ и $r \in I$ – противоречие. $\square$

Более того, можно обобщить определение НОД на кольца главных идеалов, а именно, $\text{НОД}(f, g) = d$, если $(f, g) = (d)$. Ясно, что НОД определён однозначно с точностью до умножения на обратимый элемент кольца. Далее, факториальность кольца эквивалентна лемме Евклида, то есть тому факту, что простота = неприводимость в R .

Предложение 5.18. В кольце главных идеалов простота неприводимый элемент прост.

Доказательство. a – неприводим $\implies (a)$ – максимальный среди главных $\implies (a)$ – максимальный $\implies R/(a)$ – поле $\implies R/(a)$ – область целостности $\implies a$ – простой. $\square$

Следствие 5.19. Кольцо главных идеалов факториально.

Подытожим вышесказанное, имеется следующая картинка:

$$\{\text{евклидовы кольца}\} \subset \{\text{области главных идеалов}\} \subset \{\text{факториальные кольца}\}$$

Все включения тут являются нестрогими: для первого, это, например, кольцо $\mathbb{R}[x, y]/(x^2 + y^2 + 1)$. Для второго $\mathbb{Z}[x]$.

5.4. Простые идеалы и системы полиномиальных уравнений. Пусть $\mathbb{k}$ – поле и рассмотрим систему полиномиальных уравнений

$$f_1(x_1, \dots, x_n) = \dots = f_k(x_1, \dots, x_n) = 0.$$

Определим $R = \mathbb{k}[x_1, \dots, x_n]/(f_1, \dots, f_n)$. Оказывается, имеется биекция между решениями системы и множеством простых идеалов кольца R .

Для того, чтобы придать этому строгий смысл потребуется дать несколько определений. Пусть $L \supset \mathbb{k}$ и имеется решение $\alpha_1, \dots, \alpha_n \in L$. Тогда определён гомоморфизм $f : R \rightarrow L$: им будет $[f] \rightarrow f(\alpha_1, \dots, \alpha_n)$. Отметим, что образ этого гомоморфизма – область целостности, а, значит, ядро – простой идеал. С другой стороны, любой гомоморфизм $f : R \rightarrow L$ задаёт решение системы: образы $[x_i]$.

Обратно, любой простой идеал I задаёт гомоморфизм $f : R \rightarrow R/I \rightarrow \text{fгac } R/I$, то есть гомоморфизм $f : R \rightarrow L$, где L – некоторое поле. Породим отношение эквивалентности на множестве решений: пусть $R \rightarrow L$ – соответствующий решению гомоморфизм, следующим образом. Будем говорить, что $f : R \rightarrow L_1$ эквивалентно $g : R \rightarrow L_2$ если $L_1 \subset L_2$ и $f = i \circ g$, где i – вложение $L_1 \rightarrow L_2$.

Предложение 5.20. Соответствие $\{ \text{класс эквивалентности решений системы} \} \rightarrow \ker f$, где $f : R \rightarrow L$ – соответствующий решению гомоморфизм, является биекцией.