Материал курса

Коммутативная алгебра, 2025

Содержание

1. Основные понятия

1.1. Кольца и идеалы

Определение 1.1.1. (коммутативное кольцо): Кортеж $(A, +, \cdot, 0, 1)$ называется *коммутативным кольцом,* (или просто *кольцом*) если

$$+, \cdot : A \times A \to A, \quad 0, 1 : \{\varnothing\} \to A \quad (0, 1 \in A),$$

а также выполняются следующие свойства:

(1) $(A, +, 0)$ — абелева группа;
(то есть операция сложения $+$ коммутативна и ассоциативна, 0 есть её нейтральный элемент, а также каждый элемент $x \in A$ имеет единственный противоположный $-x \in A$)

(2) $(A, \cdot, 1)$ — коммутативная полугруппа;
(то есть умножение $\cdot$ коммутативно и ассоциативно, 1 есть её нейтральный элемент)

(3) $\forall x, y, z \in A : \ x(y + z) = xy + xz$ (свойство *дистрибутивности*)

Замечание 1.1.2. Может статься, что $0 = 1$ в кольце A. Тогда имеем $x = x \cdot 1 = x \cdot 0 = 0$ и $A = \{0\} =: 0$.

Определение 1.1.3. (гомоморфизм колец): Отображение $f : A \to B$ между кольцами A и B называется *гомоморфизмом,* если оно является горморфизмом абелевых групп по сложению и полугрупп по умножению, то есть

(1) $f(x +_A y) = f(x) +_B f(y)$, $f(x \cdot_A y) = f(x) \cdot_B f(y)$;

(2) $f(0_A) = 0_B$, $f(1_A) = 1_B$.

Определение 1.1.4. (подкольца и идеалы):

(1) Подмножество $S \subset A$ называется *подкольцом,* если $(S, +, \cdot, 0, 1)$ есть кольцо.

(2) Подмножество $\mathfrak{a} \subset A$ называется *идеалом,* если $\mathfrak{a} \underset{\mathrm{Ab}}{\leq} A$, а также $A\mathfrak{a} \subset \mathfrak{a}$;

(3) Для любого $x \in A$, множество $xA = \{xy \mid y \in A\}$ образует идеал, который обозначается (x).

Определение 1.1.5. (факторкольцо): Пусть $\mathfrak{a} \leq A$. Тогда имеем $(A/\mathfrak{a}, +, \cdot, 0 + \mathfrak{a}, 1 + \mathfrak{a}) \in \mathrm{Ring}$, где

$$(x + \mathfrak{a}) +_{\mathfrak{a}} (y + \mathfrak{a}) = (x + y) + \mathfrak{a}, \quad (x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = xy + \mathfrak{a}.$$

(Пусть $\mathfrak{a}$ — идеал в кольце A. Тогда абелева группа $A/\mathfrak{a}$ однозначно снабжается умножением, индуцированным с умножения в кольце A, что превращает её в кольцо, называемое *факторкольцом* $A/\mathfrak{a}$)
Отображение $\varphi : A \to A/\mathfrak{a}$, $\varphi(x) = x + \mathfrak{a}$, называется *канонической проекцией.*

Утверждение 1.1.6. *Существует биекция*

$$\tilde{\varphi} : \{\mathfrak{b} \leq A \mid \mathfrak{a} \subset \mathfrak{b}\} \leftrightarrow \left\{\overline{\mathfrak{b}} \leq A/\mathfrak{a}\right\},$$

сохраняющая включение.

Доказательство: Упражнение. ∎

Определение 1.1.7. (делители нуля, нильпотенты, единицы):

(1) Пусть $x \in A$. Если найдётся $y \neq 0$, что $xy = 0$, то x называется *делителем нуля.* $(x \mid 0)$

(2) Кольцо $A \neq 0$, не имеющее ненулевых делителей нуля, называется *областью целостности.*

(3) Элемент $x \in A$ называется *нильпотентом,* если $x^n = 0$ для некоторого $n \geq 1$. Всякий нильпотент является делителем нуля, но не всегда наоборот.

(4) Пусть $x \in A$. Если для некоторого $y \in A$ выполняется $xy = 1$, то x называется *обратимым* $(x \mid 1)$. Обратимые элементы кольца A образуют абелеву группу по умножению.

(5) Ненулевое кольцо A, в котором каждый ненулевой элемент обратим, называется *полем.*

Упражнение 1.1.8. Докажите следующие простые свойства кольца:
(1) $x \cdot 0 = 0$;
(2) $f : A \to B,\ g : B \to C$ homo $\Longrightarrow (g \circ f) : A \to C$ homo;
(композиция гомоморфизмов — гомоморфизм)
(3) $f : A \to B$ — инъекция $\Longleftrightarrow \ker f = 0$;
(4) $x \mid 0 \Longrightarrow x \nmid 1$. (всякий делитель нуля необратим)

Утверждение 1.1.9. *Пусть A — ненулевое кольцо. Следующие условия равносильны:*
(1) A — поле;
(2) $\mathfrak{a} \leq A \Longrightarrow \mathfrak{a} = 0 = \{0\} \vee \mathfrak{a} = (1) = A$; *(В A нет идеалов, кроме $0 = \{0\}$ и (1))*
(3) $\forall B \neq 0, \forall f : A \to B : \quad f$ — ин. *(всякий гомоморфизм из A в ненулевое кольцо инъективен)*

Доказательство:
(1) $\Longrightarrow$ (2): Если $\mathfrak{a} \leq A$ и $\mathfrak{a} \neq 0$, то $\mathfrak{a}$ содержит некий обратимый элемент $x \in A$. Тогда $1 = xy \in A$ для некоторого y, а значит $\forall z \in A : \ z = z \cdot 1 \in \mathfrak{a}$, и $\mathfrak{a} = (1)$.
(2) $\Longrightarrow$ (3): Если $B \neq 0$, то для гомоморфизма $f : A \to B$ имеем $f(1) = 1$, а значит $\ker f \neq A$. Следовательно, $\ker f = 0$, и f инъективно.
(3) $\Longrightarrow$ (1): Пусть $x \in A, x \neq 0$. Рассмотрим каноническую проекцию $\varphi : A \to A/(x)$. Так как $\varphi(0) = \varphi(x) = (x)$, мы заключаем, что φ не инъективно. Тогда $A/(x) = 0$, а значит $(x) = A$, и $1 = xy$ для некоторого $y \in A$. ■

Определение 1.1.10. (простые и максимальные идеалы):
(1) Идеал $\mathfrak{p} \subset A$ называется *простым,* если $\mathfrak{p} \neq A$ и включение $xy \in \mathfrak{p}$ влечёт $x \in \mathfrak{a}$ либо $y \in \mathfrak{p}$.
(2) Идеал $\mathfrak{m} \subset A$ называется *максимальным,* если $\mathfrak{m} \neq A$ и не существует идеала $\mathfrak{b}$, такого что $\mathfrak{m} \subsetneq \mathfrak{b} \subsetneq A$.

Утверждение 1.1.11. *Пусть A — кольцо.*
(1) Идеал $\mathfrak{p} \subset A$ простой $\Longleftrightarrow A/\mathfrak{p}$ — область целостности;
(2) Идеал $\mathfrak{m} \subset A$ максимальный $\Longleftrightarrow A/\mathfrak{m}$ — поле.

Доказательство: Упражнение. ■

Следствие 1.1.12. *Всякий максимальный идеал прост.*

Теорема 1.1.13. *В каждом кольце $A \neq 0$ есть максимальный идеал.*

Доказательство: Для доказательства сформулируем *лемму Цорна:*

Предложение 1.1.14. (Лемма Цорна): *Пусть $(P, \leqslant)$ — непустое частично упорядоченное множество. Тогда если каждое линейно упорядоченное подмножество в P имеет мажоранту, то в P существует по крайней мере один максимальный элемент.*

Это утверждение мы оставим без доказательства, отметив только, что оно эквивалентно *аксиоме выбора.*

Далее, рассмотрим множество Σ всех собственных идеалов в A, частично упорядоченное по включению. Это множество непусто, так как содержит нулевой идеал 0.
Теперь пусть $\{\mathfrak{a}_\alpha\}_{\alpha \in \mathcal{J}}$ — некое линейно упорядоченное подмножество Σ. Рассмотрим объединение

$$\mathfrak{b} = \bigcup_{\alpha \in \mathcal{J}} \mathfrak{a}_\alpha.$$

Очевидно, что $\mathfrak{b}$ — идеал (упражнение), и кроме того $1 \notin \mathfrak{b}$, так как $1 \notin \mathfrak{a}_\alpha$ при всех $\alpha \in \mathcal{J}$. Следовательно, $\mathfrak{b} \in \Sigma$, а значит $\mathfrak{b}$ является мажорантой множества $\{\mathfrak{a}_\alpha\}_{\alpha \in \mathcal{J}}$.

Наконец, по лемме Цорна мы заключаем, что множество Σ имеет максимальный элемент $\mathfrak{m}$, то есть максимальный идеал в кольце A. ■

Следствие 1.1.15. *Каждый собственный идеал $\mathfrak{a} \subset A$ содержится в некотором максимальном идеале, и всякий необратимый элемент содержится в некотором максимальном идеале.*

Доказательство: Достаточно рассмотреть кольцо $A/\mathfrak{a}$ и применить предыдущую теорему. ■

Определение 1.1.16. Кольцо A, имеющее всего один максимальный идеал, называется *локальным.* Если множество максимальных идеалов кольца A конечно, то кольцо A называется *полулокальным.*

Утверждение 1.1.17. *Пусть A — некоторое кольцо.*

(1) Если $\mathfrak{a}$ — такой собственный идеал, что всякий элемент $x \in A \setminus \mathfrak{a}$ обратим, то кольцо A локально, и $\mathfrak{a}$ — его максимальный идеал.

(2) Если $\mathfrak{m}$ — максимальный идеал в A, и всякий элемент $1 + x \in 1 + \mathfrak{m}$ обратим, то A является локальным.

Доказательство:

(1) Пусть $\mathfrak{m}$ — некий максимальный идеал. Тогда если $x \in \mathfrak{m}$, то x необратим и следовательно $x \in \mathfrak{a}$. Тогда $\mathfrak{m} \subset \mathfrak{a}$, а значит $\mathfrak{m} = \mathfrak{a}$, так как идеал $\mathfrak{m}$ максимальный. Итого, все максимальные идеалы в A совпадают с $\mathfrak{a}$, ч.т.д.

(2) Допустим, что $x \in A \setminus \mathfrak{m}$. Так как $\mathfrak{m}$ максимален, идеал, порождённый $\mathfrak{m}$ и x, совпадает со всем кольцом A. Поэтому найдутся такие элементы $y \in A, t \in \mathfrak{m}$, что $xy + t = 1$. Следовательно, $xy = 1 - t \in 1 + m$, а значит xy обратим. Тогда x обратим. Остаётся только воспользоваться утверждением (1).

■

1.2. Нильрадикал и радикал Джекобсона

Утверждение 1.2.1. *Множество $\mathfrak{N}$ всех нильпотентов кольца A является идеалом. В кольце $A/\mathfrak{N}$ нет ненулевых нильпотентов.*

Доказательство: Очевидно, что если $x \in \mathfrak{N}$, то $ax \in \mathfrak{N}$ для любого $a \in A$. Теперь рассмотрим два элемента $x, y \in \mathfrak{N}$, причём $x^n = 0$ и $y^m = 0$. Тогда выражение $(x+y)^{m+n}$ по теореме Ньютона раскрывается следующим образом:

$$(x+y)^{n+m} = \sum_{i+j=n+m} a_{ij} x^i y^j.$$

При этом для каждой пары (i, j), либо $i \geq n$, либо $j \geq m$. Следовательно, каждое слагаемое $a_{ij} x^i y^j$ равно нулю, а значит $(x+y)^{n+m} = 0$, и $x + y \in \mathfrak{N}$.
Далее, рассмотрим элемент $x + \mathfrak{N} \in A/\mathfrak{N}$ и допустим, что $(x + \mathfrak{N})^n = \mathfrak{N}$. Это означает, что $x^n \in \mathfrak{N}$, и для некоторого $k \in \mathbb{N}$

$$x^{nk} = (x^n)^k = 0 \Longrightarrow x \in \mathfrak{N} \Longrightarrow x + \mathfrak{N} = \mathfrak{N}.$$

■

Определение 1.2.2. Идеал $\mathfrak{N}$ называется *нильрадикалом* кольца A.

Теорема 1.2.3. *Нильрадикал кольца A совпадает с пересечением всех его простых идеалов.*

Доказательство: Пусть P — пересечение всех простых идеалов кольца A.
Во-первых, очевидно, что всякий нильпотент лежит во всяком простом идеале (упражнение), так что $\mathfrak{N} \subset P$.

Обратно, пусть элемент $f \in A$ не является нильрадикалом. Нам нужно показать, что он не содержится в каком-либо простом идеале. Рассмотрим множество Σ всех идеалов $\mathfrak{a}$ со свойством

$$\forall n \in \mathbb{N}: \ f^n \notin \mathfrak{a}.$$

Множество Σ непусто, поскольку $0 \in \Sigma$. Рассуждение из теоремы 1.2.3 показывает применимость леммы Цорна ко множеству Σ, в результате чего получаем максимальный элемент $\mathfrak{p} \in \Sigma$. Покажем, что $\mathfrak{p}$ — простой идеал.
Пусть $x, y \notin \mathfrak{p}$. Тогда идеалы $\mathfrak{p} + (x)$ и $\mathfrak{p} + (y)$ строго содержат $\mathfrak{p}$, и следовательно, не принадлежат Σ. Иначе говоря, имеем

$$f^m \in \mathfrak{p} + (x), \qquad f^n \in \mathfrak{p} + (y),$$

для некоторых $m, n \in \mathbb{N}$. отсюда следует, что

$$f^{m+n} \in \mathfrak{p} + (xy) \Longrightarrow p + (xy) \notin \Sigma \Longrightarrow xy \notin \mathfrak{p}.$$

Тем самым, мы построили простой идеал, не содержащий f, и потому $f \notin P$. ■

Определение 1.2.4. Пересечение $\mathfrak{R}$ всех максимальных идеалов кольца A называется *радикалом Джекобсона.*

Утверждение 1.2.5. *$x \in \mathfrak{R} \Longleftrightarrow 1 - xy$ обратим в кольце A для всех $y \in A$.*

Доказательство:
$\Longrightarrow$: Допустим, что элемент $1 - xy$ необратим. Тогда, по следствию 1.1.15, этот элемент содержится в некотором максимальном идеале $\mathfrak{m}$. Но $x \in \mathfrak{R} \subset \mathfrak{m}$, а значит $1 = (1 - xy) + y \cdot x \in \mathfrak{m}$, противоречие.
$\Longleftarrow$: Предположим, что $x \notin \mathfrak{m}$ для некоторого максимального идеала $\mathfrak{m}$. Тогда имеем $A = \mathfrak{m} + (x)$, а потому $1 = u + xy$ для некоторых $u \in \mathfrak{m}$ и $y \in A$. Следовательно, $1 - xy = u \in \mathfrak{m}$, что невозможно, так как $1 - xy$ обратим. ■

1.3. Операции над идеалами

Определение 1.3.1.

(1) Пусть $\mathfrak{a}, \mathfrak{b}$ — идеалы в кольце A. Тогда $\mathfrak{a} + \mathfrak{b}$ — идеал, состоящий из сумм $x + y$, где $x \in \mathfrak{a}, y \in \mathfrak{b}$. Это наименьший идеал, содержащий $\mathfrak{a}$ и $\mathfrak{b}$. Он называется *суммой* $\mathfrak{a}$ и $\mathfrak{b}$.
(2) Также, для любого семейсва идеалов $\{\mathfrak{a}_\alpha\}_{\alpha \in \mathcal{J}}$, можно определить сумму $\sum\limits_{\alpha \in \mathcal{J}} \mathfrak{a}_\alpha$ как идеал всевозможных *конечных* сумм элементов из $\mathfrak{a}_\alpha$;
(3) *Пересечение* любого семейства идеалов является идеалом. Таким образом, идеалы кольца A образуют полную структуру по включению;
(4) Возникает определение *идеала, порождённого множеством:* если $S \subset A$, то $\langle S \rangle$ определяется как пересечение всех идеалов, содержащих S.
(5) *Произведением* двух идеалов $\mathfrak{a}$ и $\mathfrak{b}$ называется идеал, порождённый всевозможными произведениями xy, где $x \in \mathfrak{a}$, $y \in \mathfrak{b}$:

$$\mathfrak{a} \cdot \mathfrak{b} = \langle \{xy \mid x \in \mathfrak{a}, y \in \mathfrak{b}\} \rangle = \left\{ \sum_{i=1}^{n} x_i y_i \mid x_i \in \mathfrak{a}, y_i \in \mathfrak{b} \right\}.$$

Замечание 1.3.2. Все три операции коммутативны и ассоциативны (упражнение). Кроме того, справедлив дистрибутивный закон:

$$\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}$$

Определение 1.3.3. Если $\mathfrak{a} + \mathfrak{b} = (1)$, то идеалы $\mathfrak{a}$ и $\mathfrak{b}$ называются *взаимно простыми.*

Замечание 1.3.4. В кольце $\mathbb{Z}$, идеалы (n) и (m) взаимно просты тогда и только тогда, когда числа n и m взаимно просты.

Доказательство: Упражнение. ■

Упражнение 1.3.5. Правда ли, что всякий простой идеал $\mathfrak{p}$ взаимно прост с любым другим идеалом $\mathfrak{a} \neq (0)$?

Определение 1.3.6. Пусть $A_1, A_2, ..., A_n$ — некоторые кольца. Их *прямым произведением*

$$A = \prod_{k=1}^{n} A_k$$

называется множество $A_1 \times A_2 \times ... \times A_n$ с поточечными операциями. Проекции $p_k : A \to A_k$ являются гомоморфизмами колец.

Теорема 1.3.7. *Пусть A — кольцо, $\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_n$ — его идеалы. Определим гомоморфизм*

$$\varphi : A \to \prod_{k=1}^{n} (A/\mathfrak{a}_k)$$

формулой $\varphi(x) = (x + \mathfrak{a}_1, x + \mathfrak{a}_2, ..., x + \mathfrak{a}_n)$. Тогда:
(1) Если идеалы $\mathfrak{a}_i$ и $\mathfrak{a}_j$ взаимно просты при $i \neq j$, то $\prod a_k = \bigcap a_k$;
(2) Гомоморфизм φ сюръективен $\iff \mathfrak{a}_i, \mathfrak{a}_j$ взаимно просты при $i \neq j$;
(3) Гомоморфизм φ инъективен $\iff \bigcap \mathfrak{a}_k = (0)$.

Доказательство:
(1) Первый пункт доказывается индукцией по n:
- База: $n = 2$. Имеем такие идеалы $\mathfrak{a}, \mathfrak{b} \leqslant A$, что $\mathfrak{a} + \mathfrak{b} = (1)$. Очевидно, $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Обратно, имеем

$$\mathfrak{a} \cap \mathfrak{b} = (1) \cdot (\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{ab} + \mathfrak{ba} = \mathfrak{ab}.$$

- Переход: $n - 1 \to n$. Пусть $n \geq 3$, и для идеалов $\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_{n-1}$ результат верен. Положим

$$\mathfrak{b} = \bigcap_{k=1}^{n-1} \mathfrak{a}_k.$$

  Так как $\mathfrak{a}_i + \mathfrak{a}_n = (1)$, имеем $x_k + y_k = 1$ для некоторых $x_k \in \mathfrak{a}_k, y_k \in \mathfrak{a}_n$. Следовательно,

$$\prod_{k=1}^{n-1} x_i = \prod_{k=1}^{n-1} (1 - y_k) \in 1 + \mathfrak{a}_n.$$

  Тогда $\mathfrak{a}_n + \mathfrak{b} = (1)$, а значит

$$\prod_{k=1}^{n} \mathfrak{a}_k = \mathfrak{b} a_n = b \cap \mathfrak{a}_n = \bigcap_{k=1}^{n} \mathfrak{a}_n.$$

(2) $\Longrightarrow$: Покажем, что $\mathfrak{a}_1$ и $\mathfrak{a}_2$ взаимно просты. Поскольку φ сюръективно, найдётся такой элемент $x \in A$, что

$$\varphi(x) = (1 + \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, ..., \mathfrak{a}_n).$$

Тогда имеем $x \in 1 + \mathfrak{a}_1$ и $x \in \mathfrak{a}_2$, откуда $\mathfrak{a}_1 + \mathfrak{a}_2 = (1)$.
$\Longleftarrow$: Достаточно показать, что для некоторого $x \in A$ выполняется

$$\varphi(x) = (1 + \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, ..., \mathfrak{a}_n).$$

Так как $\mathfrak{a}_1$ и $\mathfrak{a}_k$ взаимно просты при $k \geq 2$, найдутся элементы $u_k \in \mathfrak{a}_1$ и $v_k \in \mathfrak{a}_k$ со свойством $1 = u_k + v_k$. Тогда положим $x = \prod v_i$. Имеем

$$x = \prod (1 - u_k) \in 1 + \mathfrak{a}_1 \quad \text{и} \quad x \in \mathfrak{a}_k \Longrightarrow \varphi(x) = (1 + \mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_n).$$

(3) Очевидно, поскольку $\bigcap \mathfrak{a}_k = \ker \varphi$,

что и требовалось. ■