

Материал курса

Коммутативная алгебра, 2025

Содержание

1. Кольца и идеалы	2
1.1. Основные понятия	2
1.2. Нильрадикал и радикал Джекобсона	4
1.3. Операции над идеалами	6
1.4. Аннуляторы	8
1.5. Расширение и сужение	10
2. Модули	11
2.1. Основные понятия	11
2.2. Подмодули и фактормодули	11

1. Кольца и идеалы

1.1. Основные понятия

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

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

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*)

Категорию всех коммутативных колец мы будем обозначать Ring .

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 $f : A \rightarrow B$ между кольцами A и B называется *гомоморфизмом*, если оно является гомоморфизмом абелевых групп по сложению и полугрупп по умножению, то есть

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

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

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 $\mathfrak{a} \leq A$, а также $A\mathfrak{a} \subset \mathfrak{a}$;

(3) Для любого $x \in A$, множество $x\mathfrak{a} = \{xy \mid y \in \mathfrak{a}\}$ образует идеал, который обозначается (x) .
Идеалы вида (x) называются *главными*.

Определение 1.1.5. (факторкольцо): Пусть $\mathfrak{a} \leq A$. Тогда имеем $(A/\mathfrak{a}, +, \cdot, 0 + \mathfrak{a}, 1 + \mathfrak{a}) \in \text{Ring}$, 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 $\varphi : A \rightarrow A/\mathfrak{a}$, $\varphi(x) = x + \mathfrak{a}$, называется *канонической проекцией*.

Утверждение 1.1.6. Существует биекция

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

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) $f : A \rightarrow B, g : B \rightarrow C \text{ homo} \implies (g \circ f) : A \rightarrow C \text{ homo}$;
(композиция гомоморфизмов — гомоморфизм)
- (3) $f : A \rightarrow B$ — инъекция $\iff \ker f = 0$;
- (4) $x \mid 0 \implies x \nmid 1$. (всякий делитель нуля необратим)

Утверждение 1.1.9. Пусть A — ненулевое кольцо. Следующие условия равносильны:

- (1) A — поле;
- (2) $\mathfrak{a} \leq A \implies \mathfrak{a} = 0 = \{0\} \vee \mathfrak{a} = (1) = A$; (в A нет идеалов, кроме $0 = \{0\}$ и (1))
- (3) $\forall B \neq 0, \forall f : A \rightarrow B : f$ — ин. (всякий гомоморфизм из A в ненулевое кольцо инъективен)

Доказательство:

- (1) \implies (2): Если $\mathfrak{a} \leq A$ и $\mathfrak{a} \neq 0$, то \mathfrak{a} содержит некий обратимый элемент $x \in A$. Тогда $1 = xy \in \mathfrak{a}$ для некоторого y , а значит $\forall z \in A : z = z \cdot 1 \in \mathfrak{a}$, и $\mathfrak{a} = (1)$.
- (2) \implies (3): Если $B \neq 0$, то для гомоморфизма $f : A \rightarrow B$ имеем $f(1) = 1$, а значит $\ker f \neq A$. Следовательно, $\ker f = 0$, и f инъективен.
- (3) \implies (1): Пусть $x \in A, x \neq 0$. Рассмотрим каноническую проекцию $\varphi : A \rightarrow A/(x)$. Так как $\varphi(0) = \varphi(x) = (x)$, мы заключаем, что φ не инъективен. 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 $x \in \mathfrak{p}$ 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 $\iff A/\mathfrak{p}$ — область целостности;
- (2) Идеал $\mathfrak{m} \subset A$ максимальный $\iff A/\mathfrak{m}$ — 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, \leq) — 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 $\{a_\alpha\}_{\alpha \in \mathcal{J}}$ — некоторое линейно упорядоченное подмножество Σ . Рассмотрим объединение

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

Очевидно, что \mathfrak{b} — идеал (упражнение), и кроме того $1 \notin \mathfrak{b}$, так как $1 \notin a_\alpha$ при всех $\alpha \in \mathcal{J}$.

Следовательно, $\mathfrak{b} \in \Sigma$, а значит \mathfrak{b} является мажорантой множества $\{a_\alpha\}_{\alpha \in \mathcal{J}}$.

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 $\mathfrak{a} < A$ 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, $xy = 1 - t \in 1 + \mathfrak{m}$, 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 $(x + y)^{n+m}$ 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 $k \in \mathbb{N}$

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

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

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

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

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

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. $x \in \mathfrak{R} \iff 1 - xy$ обратим в кольце A для всех $y \in A$.

Доказательство:

\implies : 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.

\impliedby : 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 семейства идеалов $\{\mathfrak{a}_\alpha\}_{\alpha \in J}$, можно определить сумму $\sum_{\alpha \in J} \mathfrak{a}_\alpha$ как идеал всевозможных *конечных* сумм элементов из \mathfrak{a}_α ;
- (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} , таким, что $\mathfrak{a} \not\subset \mathfrak{p}$?

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

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

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

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

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

формулой $\varphi(x) = (x + \mathfrak{a}_1, x + \mathfrak{a}_2, \dots, x + \mathfrak{a}_n)$. Тогда:

- (1) Если идеалы \mathfrak{a}_i и \mathfrak{a}_j взаимно просты при $i \neq j$, то $\prod \mathfrak{a}_k = \bigcap \mathfrak{a}_k$;
- (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 $\mathfrak{a}, \mathfrak{b} \leq A$, что $\mathfrak{a} + \mathfrak{b} = (1)$. Очевидно, $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Обратно, имеем

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

- Переход: $n - 1 \rightarrow n$. Пусть $n \geq 3$, и для идеалов $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_{n-1}$ 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,

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

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

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

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

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

Тогда имеем $x \in 1 + \mathfrak{a}_1$ и $x \in \mathfrak{a}_2$, откуда $\mathfrak{a}_1 + \mathfrak{a}_2 = (1)$.

\Leftarrow : Достаточно показать, что для некоторого $x \in A$ выполняется

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

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

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

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

что и требовалось. ■

Утверждение 1.3.8.

- (1) Пусть $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n$ — простые идеалы, \mathfrak{a} — идеал, содержащийся в $\bigcup_{k=1}^n \mathfrak{p}_k$. Тогда $\mathfrak{a} \subset \mathfrak{p}_k$ для некоторого k .
- (2) Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ — некоторые идеалы, \mathfrak{p} — простой идеал, содержащий $\bigcap_{k=1}^n \mathfrak{a}_k$. Тогда \mathfrak{p} содержит некоторый \mathfrak{a}_k . Если $\mathfrak{p} = \bigcap \mathfrak{a}_k$, то $\mathfrak{p} = \mathfrak{a}_k$ для некоторого k .

Доказательство:

- (1) Проведём доказательство индукцией по n в следующей форме:

$$(\forall k : \mathfrak{a} \not\subset \mathfrak{p}_k) \Rightarrow \mathfrak{a} \not\subset \bigcup_{k=1}^n \mathfrak{p}_k.$$

- База: $n = 1$. Очевидно.
- Переход: $n - 1 \rightarrow n$. Тогда для каждого k существует такой элемент $x_k \in \mathfrak{a}$, что $x_k \notin \mathfrak{p}_i$ при каждом $i \neq k$. Если для некоторого k ещё $x_k \notin \mathfrak{p}_k$, то всё доказано. В противном случае рассмотрим элемент

$$y = \sum_{k=1}^n x_1 x_2 \dots x_{k-1} x_{k+1} \dots x_n.$$

Имеем $y \in \mathfrak{a}$. При всех k , так как $x_k \in \mathfrak{p}_k$, имеем $y \notin \mathfrak{p}_k$. Следовательно, $x \notin \bigcup_{k=1}^n \mathfrak{p}_k$.

- (2) Предположим, что $\mathfrak{a}_k \not\subset \mathfrak{p}$ при всех k . Тогда найдутся элементы $x_k \in \mathfrak{a}_k, x_k \notin \mathfrak{p}$. Заметим, что $\prod x_k \in \prod \mathfrak{a}_k \subset \bigcap \mathfrak{a}_k$. При этом $\prod x_k \notin \mathfrak{p}$ (поскольку \mathfrak{p} прост). Следовательно, имеем $\bigcap \mathfrak{a}_k \not\subset \mathfrak{p}$, противоречие. Наконец, если $\mathfrak{p} = \bigcap \mathfrak{a}_k$, то $\mathfrak{p} \subset \mathfrak{a}_k$, а значит $\mathfrak{p} = \mathfrak{a}_k$ для некоторого k .

■

1.4. Аннуляторы

Определение 1.4.1. Пусть $\mathfrak{a}, \mathfrak{b}$ — идеалы в кольце A . Тогда их *частным* называется множество

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subset \mathfrak{a}\},$$

которое само является идеалом (упражнение). В частности, частное $(0 : \mathfrak{b})$ называется *аннулятором* идеала \mathfrak{b} и обозначается $\text{Ann}(\mathfrak{b})$. Множество всех делителей нуля в кольце A можно представить как

$$D = \bigcup_{x \neq 0} \text{Ann}((x)).$$

Если $\mathfrak{b} = (x)$ — главный идеал, то мы будем писать $(\mathfrak{a} : x)$ вместо $(\mathfrak{a} : (x))$.

Пример 1.4.2. Пусть $A = \mathbb{Z}, \mathfrak{a} = (m), \mathfrak{b} = (n)$. Тогда $(\mathfrak{a} : \mathfrak{b}) = (q)$, где $q = m / \gcd(m, n)$, где $\gcd(m, n)$ — наибольший общий делитель m и n .

Доказательство: Пусть

$$n = \prod_i p_i^{\alpha_i}, \quad m = \prod_i p_i^{\beta_i}.$$

Условие $x \in (\mathfrak{a} : \mathfrak{b})$ равносильно $x\mathfrak{b} \subset \mathfrak{a} \iff xn \in \mathfrak{a} \iff xn : m$. Если положить

$$x = \prod_i p_i^{\chi_i},$$

то последнее условие означает, что $\chi_i + \alpha_i \geq \beta_i$. Порождающий элемент $(\mathfrak{a} : \mathfrak{b})$ — это минимальное число x , обладающее этим свойством. Тогда это число x содержит p_i в минимальных степенях $\chi_i = \max(0, \beta_i - \alpha_i)$, то есть

$$x = \prod_i p_i^{\max(0, \beta_i - \alpha_i)} = \prod_i p_i^{\beta_i - \min(\alpha_i, \beta_i)} = m / \gcd(m, n).$$

■

Упражнение 1.4.3. Покажите, что в кольце A

- (1) $\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$;
- (2) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$;
- (3) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$;
- (4) $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.

Определение 1.4.4. Пусть $\mathfrak{a} \leq A$ — произвольный идеал. Его *радикалом* называется множество

$$r(\mathfrak{a}) = \{x \in A \mid \exists n \in \mathbb{N}, x^n \in \mathfrak{a}\}.$$

Имеем $r(\mathfrak{a}) = \varphi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$, так что $r(\mathfrak{a})$ — идеал в кольце A .

Упражнение 1.4.5. Пусть $\mathfrak{a}, \mathfrak{b}$ — идеалы в кольце A . Тогда

- (1) $r(r(\mathfrak{a})) = r(\mathfrak{a})$;
- (2) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$;
- (3) $r\left(\bigcup_{\alpha} \mathfrak{a}_{\alpha}\right) = \bigcup_{\alpha} r(\mathfrak{a}_{\alpha})$;
- (4) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$;
- (5) $r(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$;
- (6) Если \mathfrak{p} простой, то $r(\mathfrak{p}^n) = r(\mathfrak{p})$

Упражнение 1.4.6. Пусть $f : A \rightarrow B$ — сюръективный гомоморфизм колец. Покажите, что идеал $\mathfrak{b} \leq B$ прост тогда и только тогда, когда прост $f^{-1}(\mathfrak{b}) \leq A$.

Утверждение 1.4.7. Пусть A — кольцо, $\mathfrak{a} \leq A$. Тогда радикал $r(\mathfrak{a})$ совпадает с пересечением всех простых идеалов, содержащих \mathfrak{a} .

$$r(\mathfrak{a}) = \bigcap \{\mathfrak{p} \leq A \mid \mathfrak{p} \text{ простой, } \mathfrak{p} \supset \mathfrak{a}\}.$$

Доказательство: Применим теорему 1.2.3 к A/\mathfrak{a} . Имеем

$$\begin{aligned} r(\mathfrak{a}) &= \varphi^{-1}(\mathfrak{N}_{A/\mathfrak{a}}) = \varphi^{-1}\left(\bigcap \{\mathfrak{p} \leq A/\mathfrak{a} \mid \mathfrak{p} \text{ прост в } A/\mathfrak{a}\}\right) = \bigcap \{\varphi^{-1}(\mathfrak{p}) \mid \mathfrak{p} \text{ прост}\} = \\ &= \bigcap \{\mathfrak{p} \leq A \mid \mathfrak{p} \text{ прост и } \mathfrak{p} \subset \mathfrak{a}\}, \end{aligned}$$

что и требовалось. ■

Утверждение 1.4.8.

$$D = \{x \in A \mid \exists y \neq 0, xy = 0\} = \bigcup_{x \neq 0} r(\text{Ann}(x)).$$

Доказательство: Очевидно, что если $x^n \in D$, то $x \in D$, поэтому $D = r(D)$. Тогда мы имеем

$$D = r(D) = r\left(\bigcup_{x \neq 0} \text{Ann}(x)\right) = \bigcup_{x \neq 0} r(\text{Ann}(x)),$$

что и требовалось доказать. ■

Пример 1.4.9. Пусть $A = \mathbb{Z}$, $\mathfrak{a} = (m)$. Разложим m на простые множители:

$$m = \prod_{i=1}^k p_i^{\alpha_i}.$$

Для каждого i имеем $r((p_i)) = (p_i)$ (упражнение). Тогда

$$r(\mathfrak{a}) = r\left(\left(\prod_{i=1}^k p_i^{\alpha_i}\right)\right) = r\left(\prod_{i=1}^k (p_i^{\alpha_i})\right) = \bigcap_{i=1}^k r((p_i)^{\alpha_i}) = \bigcap_{i=1}^k (p_i).$$

Утверждение 1.4.10. Если радикалы $r(\mathfrak{a}), r(\mathfrak{b})$ идеалов $\mathfrak{a}, \mathfrak{b}$ в кольце A взаимно просты, то \mathfrak{a} и \mathfrak{b} взаимно просты.

Доказательство: Имеем

$$r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) = r(1) = (1) \implies \mathfrak{a} + \mathfrak{b} = (1),$$

что и требовалось. ■

1.5. Расширение и сужение

Определение 1.5.1. Пусть $f : A \rightarrow B$ — некий гомоморфизм колец. Если $\mathfrak{a} \leq A$ — идеал, то множество $f(\mathfrak{a})$, вообще говоря, не обязано быть идеалом в B (приведите соответствующий пример).

Расширением \mathfrak{a}^e идеала \mathfrak{a} называется идеал $\langle f(\mathfrak{a}) \rangle = Bf(\mathfrak{a}) \leq B$, порождённый образом $f(\mathfrak{a})$. Допускается представление

$$\mathfrak{a}^e = \left\{ \sum_i y_i f(x_i) \mid x_i \in A, y_i \in B \right\}$$

Пусть теперь $\mathfrak{b} \leq B$ — некоторый идеал в B . Тогда $f^{-1}(\mathfrak{b})$ — идеал в A , который называется сужением \mathfrak{b} и обозначается \mathfrak{b}^c .

Замечание 1.5.2. Если \mathfrak{b} прост, то \mathfrak{b}^c тоже прост. Если \mathfrak{a} прост, то \mathfrak{a}^e не обязательно прост (например, $f : \mathbb{Z} \rightarrow \mathbb{Q}$, $\mathfrak{a} = (2)$).

Утверждение 1.5.3. Пусть $f : A \rightarrow B$ — гомоморфизм, $\mathfrak{a} \leq A$, $\mathfrak{b} \leq B$. Тогда

- (1) $\mathfrak{a} \subset \mathfrak{a}^{ec}$, $\mathfrak{b} \supset \mathfrak{b}^{ce}$;
- (2) $\mathfrak{a}^e = \mathfrak{a}^{ece}$, $\mathfrak{b}^c = \mathfrak{b}^{cec}$;
- (3) Если C — множество идеалов в A , которые являются сужениями, а E — множество всех идеалов в B , которые являются расширениями, то

$$C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}, \quad E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\},$$

и $\mathfrak{a} \mapsto \mathfrak{a}^e$ — биективное отображение C на E , обратное к которому — $\mathfrak{b} \mapsto \mathfrak{b}^c$.

Доказательство: Пункт (1) тривиален:

$$\mathfrak{a} \subset f^{-1}(f(\mathfrak{a})) \subset f^{-1}(Bf(\mathfrak{a})) = \mathfrak{a}^{ec}, \quad \mathfrak{b}^{ce} = Bf(f^{-1}(\mathfrak{b})) \subset B\mathfrak{b} = \mathfrak{b}.$$

Пункт (2) остаётся читателю как упражнение.

Если $\mathfrak{a} \in C$, то $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec}$. Наоборот, если $\mathfrak{a} = \mathfrak{a}^{ec}$, то \mathfrak{a} — сужение \mathfrak{a}^e .

Рассуждение относительно E аналогично. ■

Упражнение 1.5.4. Пусть $f : A \rightarrow B$, $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2 \leq A$, $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2 \leq B$. Тогда

$$\begin{aligned} (\mathfrak{a}_1 + \mathfrak{a}_2)^e &= \mathfrak{a}_1^e + \mathfrak{a}_2^e, & (\mathfrak{b}_1 + \mathfrak{b}_2)^c &\supset \mathfrak{b}_1^c + \mathfrak{b}_2^c, \\ (\mathfrak{a}_1 \cap \mathfrak{a}_2)^e &\subset \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, & (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c &= \mathfrak{b}_1^c \cap \mathfrak{b}_2^c, \\ (\mathfrak{a}_1 \mathfrak{a}_2)^e &= \mathfrak{a}_1^e \mathfrak{a}_2^e, & (\mathfrak{b}_1 \mathfrak{b}_2)^c &\supset \mathfrak{b}_1^c \mathfrak{b}_2^c, \\ (\mathfrak{a}_1 : \mathfrak{a}_2)^e &\subset (\mathfrak{a}_1^e : \mathfrak{a}_2^e), & (\mathfrak{b}_1 : \mathfrak{b}_2)^c &\subset (\mathfrak{b}_1^c : \mathfrak{b}_2^c), \\ r(\mathfrak{a})^e &\subset r(\mathfrak{a}^e), & r(\mathfrak{b})^c &= r(\mathfrak{b}^c). \end{aligned}$$

2. Модули

2.1. Основные понятия

Определение 2.1.1. Пусть A — некоторое кольцо. A -модулем называется абелева группа $(M, +, 0)$ вместе с линейным действием A на M ,

$$\begin{aligned}\mu : A \times M &\longrightarrow M, \\ (\alpha, x) &\mapsto \mu(\alpha, x) =: \alpha x,\end{aligned}$$

причём выполняются следующие аксиомы:

$$\alpha(x + y) = \alpha x + \alpha y, \quad (\alpha + \beta)x = \alpha x + \beta x, \quad (\alpha\beta)x = \alpha(\beta x), \quad 1x = x.$$

Категория всех A -модулей обозначается $A - \text{Mod}$

Замечание 2.1.2. Есть равносильное определение A -модуля: абелева группа M вместе с гомоморфизмом колец $\mu : A \rightarrow \text{End}(M)$, где $\text{End}(M)$ — кольцо эндоморфизмов M как абелевой группы (упражнение).

Пример 2.1.3. Понятие модуля обобщает несколько хорошо известных понятий:

- (1) Любой идеал $\mathfrak{a} \leq A$ является A -модулем, в частности A есть A -модуль;
- (2) Если A есть поле F , то A -модуль есть векторное пространство над полем F ;
- (3) \mathbb{Z} -модули это абелевы группы ($nx = x + x + \dots + x$).

Определение 2.1.4. Пусть M, N — некоторые A -модули. Отображение $f : M \rightarrow N$ называется гомоморфизмом A -модулей, если

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$$

для всех $x, y \in M$ и $\alpha, \beta \in A$.

Множество $\text{Hom}(M, N)$ всех гомоморфизмов A -модулей M в N можно наделять структурой A -модуля, определив

$$(f + g)(x) = f(x) + g(x), \quad (\alpha f)(x) = \alpha f(x)$$

для всех $x \in M$.

Замечание 2.1.5. Для любого A -модуля M , имеется естественный изоморфизм $\text{Hom}(A, M) \cong M$: каждый гомоморфизм $f : A \rightarrow M$ однозначно задаётся элементом $f(1)$, который можно выбрать произвольно.

2.2. Подмодули и фактормодули

Определение 2.2.1. Пусть M — некоторый A -модуль. Подгруппа $M' \leq M$ называется подмодулем, если $AM' \subset M'$. Тогда на факторгруппу M/M' переносится структура A -модуля, если определить умножение формулой

$$\alpha(x + M') = \alpha x + M',$$

а модуль M/M' называется фактормодулем M по M' .