Коммутативная алгебра

Часть 1. Идеалы

Пусть A — коммутативное кольцо. Напомним, что идеалом в A называется подгруппа (относительно сложения) $\mathfrak{a} \subset A$, такая что $A\mathfrak{a} = \mathfrak{a}$.

Определение 1.1. Суммой идеалов $\mathfrak{a} + \mathfrak{b}$ называется множество элементов кольца A вида $a + b$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Произведением идеалов $\mathfrak{a}\mathfrak{b}$ называется множество элементов кольца A вида $\sum a_i b_i$, где $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$.

Лемма 1.2. *Сумма, произведение и пересечение идеалов — идеалы. Все указанные операции коммутативны и ассоциативны, а произведение — билинейно:* $(\mathfrak{a}_1+\mathfrak{a}_2)\mathfrak{b} = \mathfrak{a}_1\mathfrak{b}+\mathfrak{a}_2\mathfrak{b}$. *Наконец,* $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{a}, \mathfrak{b} \subset \mathfrak{a}+\mathfrak{b}$.

Если $a \in A$, то идеал $(a) = aA := \{\, x = ay \mid y \in A \,\}$ называется главным идеалом. Идеал $(a_1) + \cdots + (a_m)$ обозначается также $(a_1, \dots, a_m)$. Заметим, что $(a) = A \iff a$ обратим.

Идеал $\mathfrak{m} \subset A$ — максимальный, если для всякого идеала $\mathfrak{a} \subset A$, такого что $\mathfrak{m} \subset \mathfrak{a} \subset A$, имеем либо $\mathfrak{a} = \mathfrak{m}$, либо $\mathfrak{a} = A$. Идеал $\mathfrak{p} \subset A$ — простой, если $\forall x, y \in A$, $x \notin \mathfrak{p}$, $y \notin \mathfrak{p} \Longrightarrow xy \notin \mathfrak{p}$. Идеал $\mathfrak{m} \subset A$ максимален $\iff$ $A/\mathfrak{m}$ — поле. Идеал $\mathfrak{p} \subset A$ прост $\iff A/\mathfrak{p}$ — целостное кольцо. Макисмальный идеал прост.

Напомним, что прообраз простого идеала при гомоморфизме колец всегда прост, а прообраз максимального идеала максимален, если дополнительно предположить, что гомоморфизм сюрьективен.

Лемма 1.3. *Всякое кольцо обладает максимальным идеалом.*

Доказательство: если $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset A$ — возрастающая цепочка идеалов $\mathfrak{a}_i \neq A$, то идеал $\mathfrak{a} = \bigcup_i \mathfrak{a}_i \subset A$ нетривиален: $\mathfrak{a} = A \Longrightarrow 1 \in \mathfrak{a} \Longrightarrow 1 \in \mathfrak{a}_i \Longrightarrow \mathfrak{a}_i = A$ для некоторого i. Остается применить лемму Цорна. □

Рассматривая прообразы максимальных идеалов в $A/\mathfrak{a}$ относительно проекции $A \to A/\mathfrak{a}$, заключаем, что всякий нетривиальный идеал содержится в максимальном идеале. Рассматривая $\mathfrak{a} = (a)$, заключаем, что всякий необратимый элемент кольца A содержится в максимальном идеале.

Часть 2. Радикалы

Напомним, что $x \in A$ называется нильпотентом, если $x^n = 0$ для некоторого n.

Лемма 2.1. *Множество всех нильпотентов в A является идеалом.*

Доказательство: $x^n = y^m = 0 \Longrightarrow (x+y)^{n+m} = \sum \binom{n+m}{k} x^k y^{n+m-k} = 0$; $(ax)^n = a^n x^n = 0$. □

Идеал $\mathfrak{N}$, образованный всеми нильпотентами кольца A называется нильрадикалом.

Лемма 2.2. *Нильрадикал равен пересечению всех простых идеалов.*

Доказательство: пусть $x \in A$ — нильпотент, а $\mathfrak{p} \subset A$ — простой идеал. Если $x \notin \mathfrak{p}$, то по индукции $x^n \notin \mathfrak{p}$, но $x^n = 0 \in \mathfrak{p}$, значит $x \in \mathfrak{p}$, то есть $\mathfrak{N} \subset \bigcap \mathfrak{p}$. Обратно, предположим, что x — не нильпотент и рассмотрим множество идеалов, не пересекающихся с множеством $\{\, x^n \,\}_{n\in\mathbb{N}}$. Согласно лемме Цорна в множестве таких идеалов найдется макисмальный идеал $\mathfrak{p}$. Покажем, что $\mathfrak{p}$ — простой. Пусть $y, z \notin \mathfrak{p}$. Тогда по построению $\mathfrak{p}$ имеем $x^k \in \mathfrak{p} + (y)$, $x^l \in \mathfrak{p} + (z)$. Перемножая, получаем $x^{k+l} \in \mathfrak{p} + (yz)$. Если $yz \in \mathfrak{p}$, то $\mathfrak{p} + (yz) = \mathfrak{p}$, то есть $x^{k+l} \in \mathfrak{p}$, что противоречит выбору $\mathfrak{p}$. Значит $yz \notin \mathfrak{p}$ и $\mathfrak{p}$ — прост. □

Определение 2.3. Радикалом идеала $\mathfrak{a} \subset A$ называется множество $\mathfrak{r}(\mathfrak{a}) := \{\, x \in A \mid x^n \in \mathfrak{a}$ для некотого $n \,\}$.

Лемма 2.4. *Если $\pi : A \to A/\mathfrak{a}$ — канонический эпиморфизм, то $\mathfrak{r}(\mathfrak{a}) = \pi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$.*

Доказательство: $x^n \in \mathfrak{a} \iff \pi(x)^n = 0$ в $A/\mathfrak{a}$. □

Следствие 2.5. *Радикал* $\mathfrak{r}(\mathfrak{a})$ *является идеалом,* $\mathfrak{a} \subset \mathfrak{r}(\mathfrak{a})$*, и* $\mathfrak{r}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.

Следствие 2.6. *Имеем* $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$.

Доказательство: $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \bigcap_{\mathfrak{p} \supset \mathfrak{r}(\mathfrak{a})} \mathfrak{p} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p} = \mathfrak{r}(\mathfrak{a})$. □

Определение 2.7. Идеал $\mathfrak{a} \subset A$ называется радикальным, если $\mathfrak{a} = \mathfrak{r}(\mathfrak{a})$.

Предыдущее следствие показывает, что радикал идеала является радикальным идеалом.

Следствие 2.8. *Идеал* $\mathfrak{a}$ *— радикальный* $\iff$ *кольцо* $A/\mathfrak{a}$ *не имеет нетривиальных нильпотентов.*

Следствие 2.9. *Простой идеал радикален.*

Часть 3. Алгебраические многообразия

Коммутативная алгебра очень тесно связана с геометрией алгебраических многообразий. Пусть k — алгебраически замкнутое поле. Обозначим через $\mathbb{A}^n = \mathsf{k}^n$ — n-мерное аффинное пространство с координатами $x_1, \dots, x_n$, и пусть $X \subset \mathbb{A}^n$ — аффинное алгебраическое многообразиенад полем k, то есть множество, заданное полиномиальными уравнениями: $X = \{\, x = (x_1, \dots, x_n) \in \mathbb{A}^n \mid f_1(x_1, \dots, x_n) = \dots = f_m(x_1, \dots, x_n) = 0 \,\}$, где $f_1, \dots, f_m \in \mathsf{k}[x_1, \dots, x_n]$. Тогда $A_X := \mathsf{k}[x_1, \dots, x_n]/(f_1, \dots, f_m)$ — типичное коммутативное кольцо. Точнее говоря, k-алгебра A называется конечно порожденной над полем k, если найдется конечный набор элементов $a_1, \dots, a_n \in A$, такой что всякий элемент из A представляется в виде многочлена от a_i с коэффицентами в k.

Лемма 3.1. *Если* k*-алгебра* A *— конечно порождена над* k*, то* $A \cong \mathsf{k}[x_1, \dots, x_n]/I$*. Более того, если* A *не имеет нетривиальных нильпотентов, то идеал* I *— радикальный.*

Доказательство: если $a_1, \dots, a_n$ порождают A, то отображение $f : \mathsf{k}[x_1, \dots, x_n] \to A$, $f(x_1, \dots, x_n) \mapsto f(a_1, \dots, a_n)$ является эпиморфизмом, значит $A \cong \mathsf{k}[x_1, \dots, x_n]/\operatorname{Ker} f$. Остается применить следствие 2.8. □

Позднее мы покажем, что всякий идеал $I \subset \mathsf{k}[x_1, \dots, x_n]$ представляется в виде $I = (f_1, \dots, f_m)$ (теорема Гильберта о базисе).

Всякому идеалу $\mathfrak{a} \subset A_X$ сопоставим подмножество $V(\mathfrak{a}) = \{\, x \in X \mid \forall f \in \mathfrak{a}\ f(x) = 0 \,\}$. Подмножества вида $V(\mathfrak{a}) \subset X$ называются алгебраическими подмногообразиями. Обратно, всякому подмножеству $Y \subset X$ сопоставим идеал $I_Y := \{\, f \in A_X \mid f_{|Y} \equiv 0 \,\} \subset A_X$.

Лемма 3.2. *Обе конструкции монотонны по отношению к включению: если* $\mathfrak{a} \subset \mathfrak{b}$*, то* $V(\mathfrak{b}) \subset V(\mathfrak{a})$*, а если* $Y \subset Z$*, то* $I_Z \subset I_Y$.

Доказательство: если $\mathfrak{a} \subset \mathfrak{b}$ и $x \in V(\mathfrak{b})$, то всякая функция из $\mathfrak{a}$ лежит в $\mathfrak{b}$, следовательно зануляется на $V(\mathfrak{b})$, значит $x \in V(\mathfrak{a})$, значит $V(\mathfrak{b}) \subset V(\mathfrak{a})$. Если $Y \subset Z$ и $f \in I_Z$, то f зануляется на Z, а значит и на Y, значит $f \in I_Y$, значит $I_Z \subset I_Y$. □

Лемма 3.3. *Операции сложения, умножения и пересечения идеалов соответствуют пересечению и объединению подмногообразий. Иначе говоря,* $V(\mathfrak{a}_1 + \mathfrak{a}_2) = V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2)$, $V(\mathfrak{a}_1\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2) = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$.

Доказательство: если $x \in V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2)$, то $\forall f \in \mathfrak{a}_1, g \in \mathfrak{a}_2$ имеем $f(x) = g(x) = 0$, значит $(f+g)(x) = 0$, то есть $V(\mathfrak{a}_1 + \mathfrak{a}_2) \supset V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2)$. Далее, $V(\mathfrak{a}_1 + \mathfrak{a}_2) \subset V(\mathfrak{a}_1), V(\mathfrak{a}_2) \subset V(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subset V(\mathfrak{a}_1\mathfrak{a}_2)$, так как $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2 \subset \mathfrak{a}_1, \mathfrak{a}_2 \subset \mathfrak{a}_1 + \mathfrak{a}_2$. Остается проверить, что $V(\mathfrak{a}_1\mathfrak{a}_2) \subset V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$. Действительно, если $x \in V(\mathfrak{a}_1\mathfrak{a}_2) \setminus V(\mathfrak{a}_1)$, то $\exists f \in \mathfrak{a}_1$, так что $f(x) \neq 0$. Значит $\forall g \in \mathfrak{a}_2$ имеем $fg \in \mathfrak{a}_1\mathfrak{a}_2 \implies (fg)(x) = 0 \implies g(x) = 0$, т.е. $x \in V(\mathfrak{a}_2)$. □

Одним из основных результатов в коммутативной алгебре является

Теорема 3.4. *Имеем* $I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a})$.

Эта теорема известна как Теорема Гильберта о нулях (Hilbert Nullstellensatz). Ее мы докажем позднее, а пока выведем из нее следствия.

Следствие 3.5. *Если* $Y \subset X$ *— алгебраическое подмногообразие, то идеал* I_Y *радикален, а* $Y = V(I_Y)$.

Доказательство: Y по определению подмногообразия имеет вид $Y = V(\mathfrak{a})$, поэтому $I_Y = I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a})$ — радикальный идеал, а $V(I_Y) = V(\mathfrak{r}(\mathfrak{a})) = V(\mathfrak{a}) = Y$. □

Следствие 3.6. *Соответствия $\mathfrak{a} \mapsto V(\mathfrak{a})$, $Y \mapsto I_Y$ задают биекцию между множеством всех подмногообразий $Y \subset X$ и множеством всех радикальных идеалов $\mathfrak{a} \subset A_X$.*

Доказательство: если $\mathfrak{a}$ радикален, то $I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a}) = \mathfrak{a}$, а все остальное доказано выше. □

Следствие 3.7. *Всякий максимальный идеал в кольце $A = A_X$ имеет вид $\mathfrak{m} = I_x$, где $x \in X$.*

Доказательство: $I_{V(\mathfrak{m})} = \mathfrak{r}(\mathfrak{m}) = \mathfrak{m}$. Так как $I_\emptyset = A$, то $V(\mathfrak{m}) \neq \emptyset$. Если $x \in V(\mathfrak{m})$, то $\mathfrak{m} = I_{V(\mathfrak{m})} \subset I_x \neq A$. Но $\mathfrak{m}$ максимальный, значит $\mathfrak{m} = I_x$. □

Таким образом, точки многообразия находятся во взаимно-однозначном соответствии с максимальными идеалами кольца.

Определение 3.8. Подмножество $Y \subset X$ называется неприводимым, если $Y \subset V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) \Longrightarrow Y \subset V(\mathfrak{a}_1)$ или $Y \subset V(\mathfrak{a}_2)$.

Лемма 3.9. *Подмногообразие Y — неприводимо $\Longleftrightarrow$ идеал I_Y прост.*

Доказательство: ($\Longrightarrow$) $Y = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) \Longrightarrow Y = V(\mathfrak{a}_1\mathfrak{a}_2)$. Если $\mathfrak{a}_1 \not\subset I_Y$, то найдется $f \in \mathfrak{a}_1 \setminus I_Y$. Тогда для всякого $g \in \mathfrak{a}_2$ имеем $fg \in \mathfrak{a}_1\mathfrak{a}_2 \Longrightarrow fg \in I_Y \Longrightarrow g \in I_Y$, то есть $\mathfrak{a}_2 \subset I_Y \Longrightarrow Y \subset V(\mathfrak{a}_2)$. Иначе $\mathfrak{a}_1 \subset I_Y \Longrightarrow Y \subset V(\mathfrak{a}_1)$. ($\Longleftarrow$) Пусть I_Y — не прост. Тогда найдутся $f_1, f_2 \notin I_Y$, так что $f_1f_2 \in I_Y$. Тогда $I_Y + (f_1f_2) = I_Y$ и $Y = V(I_Y) = V(I_Y + (f_1f_2)) = V((I_Y + (f_1))(I_Y + (f_2))) = V(I_Y + (f_1)) \cup V(I_Y + (f_2))$, но $Y \not\subset V(I_Y + (f_i))$, так как $f_i \notin I_Y$. □

Следствие 3.10. *Многообразие X неприводимо $\Longleftrightarrow$ кольцо A_X целостное.*

Таким образом, неприводимые подмногообразия в X находятся во взаимно-однозначном соответствии с простыми идеалами кольца A_X. При этом точки, лежащие на подмногообразии $V(\mathfrak{p})$ соответствуют максимальным идеалам, содержащим идеал $\mathfrak{p}$.

Изучим теперь геометрический смысл факторизации.

Лемма 3.11. *Все (простые, максимальные) идеалы кольца $A/\mathfrak{a}$ находятся во взаимно-однозначном соответствии со всеми (простыми, максимальными) идеалами кольца A, содержащими $\mathfrak{a}$.*

Доказательство: если $\pi : A \to A/\mathfrak{a}$ — канонический эпиморфизм, а $\mathfrak{b} \subset A/\mathfrak{a}$ — идеал, то $\mathfrak{b} = \pi^{-1}(\mathfrak{a})/\mathfrak{a}$. Обратно, если $\mathfrak{c} \subset A$ — идеал и $\mathfrak{a} \subset \mathfrak{c}$, то $\mathfrak{c}/\mathfrak{a} \subset A/\mathfrak{a}$ — идеал и $\mathfrak{c} = \pi^{-1}(\mathfrak{c}/\mathfrak{a})$. Наконец, $(A/\mathfrak{a})/\mathfrak{b} = A/\pi^{-1}(\mathfrak{b})$, поэтому $\mathfrak{b}$ — прост (максимален) $\Longleftrightarrow \pi^{-1}(\mathfrak{b})$ — прост (максимален). □

Таким образом, точки многообразия, соответствующего кольцу $A/\mathfrak{a}$, это точки, лежащие на $V(\mathfrak{a})$. Иначе говоря, переход к факторкольцу соответствует переходу к подмногообразию.

Пусть $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ — алгебраические многообразия. Отображение $\phi : X \to Y$ называется алгебраическим, если оно имеет вид $\phi(x_1, \ldots, x_n) = (\phi_1(x_1, \ldots, x_n), \ldots, \phi_m(x_1, \ldots, x_n))$ и $\phi_1, \ldots, \phi_m \in \mathsf{k}[x_1, \ldots, x_n]$. Если $\phi : X \to Y$ — алгебраическое отображение и $f \in \mathsf{k}[y_1, \ldots, y_m]$, то $\phi^*(f) := f \circ \phi = f(\phi_1, \ldots, \phi_m) \in \mathsf{k}[x_1, \ldots, x_n]$. Более того, если $f_{|Y} = 0$, то $\phi^*(f)_{|X} = 0$, поэтому ϕ^* индуцирует отображение $A_Y \to A_X$, которое очевидно является гомоморфизмом.

Лемма 3.12. *Сопоставления $X \mapsto A_X$, $\phi \mapsto \phi^*$ задают контравариантный функтор из категории алгебраических многообразий над полем k в категорию конечно порожденных коммутативных k-алгебр.*

Обратно, пусть $\Phi : A_Y \to A_X$ — гомоморфизм колец. Каждая из переменных $y_1, \ldots, y_m$ является функцией на Y, поэтому $\Phi(y_i) \in A_X = \mathsf{k}[x_1, \ldots, x_n]/I_X$. Поднимая $\Phi(y_i)$ до многочленов $\phi_i(x) \in \mathsf{k}[x_1, \ldots, x_n]$, получаем отображение $\phi : X \to \mathbb{A}^m$. Ясно, что при этом $\phi^*(f)_{|X} = \Phi(f_{|Y})$, поэтому если $f \in I_Y$, то $f \circ \phi = 0$, значит $\phi(X) \subset Y$. Таким образом, всякий гомоморфизм колец индуцирован алгебраическим отображением многообразий. Наконец, вспоминая, что всякая конечно порожденная коммутативная алгебра без нильпотентов является алгеброй функций на аффинном многообразии, получаем.

Теорема 3.13. *Категория аффинных алгебраических многообразий над полем k эквивалентна категории конечно порожденных коммутативных k-алгебр без нильпотентов.*