Лекции по алгебраической геометрии

С. М. Львовский

НМУ, 1996/97 год, первый семестр

Лекция 1. Топология Зарисского

В этом курсе мы будем заниматься алгебраической геометрией над алгебраически замкнутым полем. Поэтому зафиксируем раз и навсегда алгебраически замкнутое поле k. Рассмотрим множество всех упорядоченных наборов $(x_1, \dots, x_n)$, где все x_j принадлежат k. В алгебраической геометрии это множество принято называть *n-мерным аффинным пространством* (над полем k) и обозначать $\mathbb{A}^n$. Точка $x = (x_1, \dots, x_n) \in \mathbb{A}^n$ называется *нулем* многочлена $f \in k[X_1, \dots, X_n]$, если $f(x_1, \dots, x_n) = 0$.

Определение 1.1. Подмножество $V \subset \mathbb{A}^n$ называется *замкнутым по Зарисскому,* если V — множество нулей семейства многочленов $f_\alpha \in k[X_1, \dots, X_n]$ с коэффициентами из k.

Очевидно, множество X не изменится, если к многочленам f_α добавить всевозможные многочлены вида $\sum g_\alpha f_\alpha$ — иными словами, X является также множеством общих нулей многочленов из идеала, порожденного $\{f_\alpha \dots\}$. Однако каждый идеал в кольце $k[X_0, \dots, X_n]$ конечно порожден — этот факт известен как «теорема Гильберта о базисе». Стало быть, всякое замкнутое по Зарисскому множество можно задать *конечным* числом уравнений. Доказательство теоремы Гильберта о базисе проще всего прочитать в книге С. Ленга «Алгебра», глава VI, §§1–2. Кстати, кольца, в которых всякий идеал конечно порожден, называются *нётеровыми.* Про их простейшие свойства можно прочитать в том же месте у Ленга.

Вернемся к замкнутым по Зарисскому множествам (оговорку «по Зарисскому» мы иногда будем опускать).

Предложение 1.2. *Объединение конечного числа замкнутых множеств замкнуто; пересечение любого семейства замкнутых множеств замкнуто.*

Доказательство. Если множества V и W заданы системами уравнений $f_\alpha = 0$ и $g_\beta = 0$ соответственно, то $V \cup W$ можно задать системой уравнений $f_\alpha g_\beta = 0$. Это доказывает первое утверждение. Второе утверждение очевидно. $\square$

Дополнения к замкнутым по Зарисскому множествам называются *открытыми* (опять же по Зарисскому). Доказанное выше предложение показывает, что открытые по Зарисскому множества задают на $\mathbb{A}^n$ топологию; она называется *топологией Зарисского.* Аналитическая интуиция применительно к топологии Зарисского работает плохо: например, эта топология не удовлетворяет аксиоме отделимости.

Теперь выясним, в каких случаях система полиномиальных уравнений имеет решения. В силу вышесказанного мы можем ограничиться случаем конечных систем.

Очевидно, многочлены $f_1, \ldots, f_m$ *не* имеют общих нулей, если для каких-то многочленов $g_1, \ldots, g_m$ верно тождество $\sum g_i f_i = 1$ («из системы следует уравнение $0 = 1$», или, на более научном языке, многочлены $f_1, \ldots, f_m$ порождают единичный идеал). Оказывается, над алгебраически замкнутыми полями других препятствий к существованию решения нет:

Предложение 1.3 (Теорема Гильберта о нулях, I). *Система уравнений $f_\alpha(x_1, \ldots, x_n) = 0$, где $f_\alpha \in k[X_1, \ldots, X_n]$ и k — алгебраически замкнутое поле, не имеет решений в $\mathbb{A}^n$ тогда и только тогда, когда эти многочлены порождают единичный идеал.*

Доказательство. Мы воспользуемся таким алгебраическим фактом:

Теорема 1.4. *Пусть $B = k[x_1, \ldots, x_n]$ — алгебра над полем k, порожденная своими элементами $x_1, \ldots, x_n$ (это означает, что всякий элемент из B представим в виде многочлена от x_i с коэффициентами из k; мы не предполагаем, что x_i алгебраически независимы над k). Если B является полем, то это поле является конечным расширением k.*

Доказательство алгебраического факта. При $n = 1$ теорема хорошо известна и очевидна (так как $B \ni x_1^{-1}$, то $x_1^{-1} = a_0 + a_1 x_1 + \cdots + a_r x^r$; избавляясь от знаменателя, получаем алгебраическое уравнение для x_1 над k). Теперь проведем индукцию по n. Пусть для $n-1$ образующих теорема доказана. Так как B — поле, то B содержит поле $k(x_n)$ и порождено над ним (как алгебра) элементами $x_1, \ldots, x_{n-1}$. По предположению индукции B является конечным расширением $k(x_n)$. Базис B над $k(x_n)$

(обозначим элементы этого базиса $\omega_1, \dots, \omega_N$) можно выбрать так, что он будет состоять из конечного числа произведений $\prod_{i=1}^{n-1} x_i^{a_i}$.

Нам достаточно показать, что x_n алгебраично над k. Предположим обратное; тогда $k(x_n)$ изоморфно полю рациональных функций от x_n. Пусть $\omega_i\omega_j = \sum c_{ij}^r \omega_r$, где $c_{ij}^r \in k(x_n)$, и пусть $p_1, \dots, p_M \in k[x_n]$ — конечное число неприводимых многочленов, на которые делятся знаменатели «структурных констант» c_{ij}^r, являющихся рациональными дробями от x_n. Выберем неприводимый многочлен $q \in k[x_n]$, отличный от всех p_j. Так как B порождено $x_1, \dots, x_{n-1}, x_n$ как k-алгебра, получаем, что $q^{-1} = \sum_{i=1}^N h_i\omega_i$, где $h_i \in k(x_n)$ — рациональные дроби, знаменатели которых не делятся на неприводимые многочлены, отличные от p_i. Рассмотрим теперь коэффициент при ω_1 в разложении $q^{-1}\omega_1$ по базису $\omega_1, \dots, \omega_N$. Этот коэффициент равен $\sum_i c_{i1}^1 h_i \in k(x_n)$ и тем самым знаменатель этого коэффициента не делится на неприводимые многочлены, отличные от p_j. С другой стороны, в силу линейной независимости ω_i над $k(x_n)$ этот коэффициент равен просто q^{-1}. Противоречие с выбором q доказывает теорему. $\square$

Вернемся к доказательству нашего предложения. Пусть многочлены f_α порождают идеал $I \subset k[X_1, \dots, X_n]$. Предположим, что I не совпадает со всем кольцом многочленов; нам надо доказать, что многочлены из I имеют общий нуль в $\mathbb{A}^n$. Так как I неединичен, он содержится в некотором максимальном идеале $\mathfrak{m}$. Пусть $k[X_1, \dots, X_n]/\mathfrak{m} = B$; обозначим через x_i образы X_i в B. Так как идеал $\mathfrak{m}$ максимален, кольцо B удовлетворяет условиям теоремы 1.4; стало быть, B — конечное расширение поля k, а так как k алгебраически замкнуто, то вложение $k \hookrightarrow B$ является изоморфизмом. Пусть элементы $\xi_1, \dots, \xi_n \in k$ переходят при этом изоморфизме в $x_1, \dots, x_n$ соответственно. Тогда для всякого $f \in \mathfrak{m}$ имеем $f(x_1, \dots, x_n) = 0$ в B и, стало быть, $f(\xi_1, \dots, \xi_n) = 0$ в k. Тем самым точка $(\xi_1, \dots, \xi_n) \in \mathbb{A}^n$ является общим нулем для всех $f \in \mathfrak{m}$ (и тем более для всех $f \in I$). $\square$

Итак, каждому идеалу $I \subset k[X_0, \dots, X_n]$ можно поставить в соответствие множество $V(I) \subset \mathbb{A}^n$, состоящее из общих нулей всех многочленов, лежащих в f (теорема Гильберта о нулях показывает, что $V(I) \neq \varnothing$ если I не совпадает со всем кольцом); напротив, каждому подмножеству $M \subset \mathbb{A}^n$ можно поставить в соответствие идеал $I(M) \subset k[X_0, \dots, X_n]$, состоящий из многочленов, обращающихся в нуль на M. Операции V и I, действующие в противоположные стороны, почти обратны друг другу. Почти, но не совсем:

Предложение 1.5. *Если $M \subset \mathbb{A}^n$, то $V(I(M)) = \overline{M}$, где черточка означает замыкание в топологии Зарисского.*

Доказательство. Это тавтология: замыкание M есть по определению пересечение множеств нулей полиномов, зануляющихся на M, то есть пересечение множеств нулей полиномов из $I(M)$, то есть $V(I(M))$. $\square$

Теперь посмотрим, как связаны I и $I(V(I))$. Второй из этих идеалов может быть строго больше первого. Например, если $n = 1$, $I = (X^2)$, то $V(I) = \{0\}$ и $I(V(I)) = (X)$. Чтобы сформулировать точный результат, нам нужно следующее

Определение 1.6. Пусть A — коммутативное кольцо (с единицей), $I \subset A$ — идеал. *Радикалом* I называется множество таких $f \in A$, что $f^m \in A$ для некоторого $m > 0$.

Радикал идеала I обозначается $r(I)$. Если I — идеал в кольце многочленов, то, очевидно, $I(V(I)) \supseteq r(I)$ (если f — такой многочлен, что f^m обращается в нуль на $V(I)$, то и сам f обращается в нуль на $V(I)$). Замечательно, что это включение на самом деле является равенством:

Теорема 1.7 (Теорема Гильберта о нулях, II). *Если I — идеал в кольце многочленов $k[X_1, \ldots, X_n]$ (поле k алгебраически замкнуто), то $I(V(I)) = r(I)$. Подробнее: если многочлен f обращается в нуль на множестве общих нулей многочленов $h_1, \ldots, h_l$, то $f^m = g_1 h_1 + \cdots + g_l h_l$ для некоторого $m > 0$ и некоторых многочленов $g_1, \ldots, g_l$.*

Доказательство. Введем дополнительную неизвестную T и в аффинном пространстве $\mathbb{A}^{n+1}$ с координатами $(x_1, \ldots, x_n, t)$ рассмотрим систему из $l+1$ уравнения $h_1(x_1, \ldots, x_n) = 0$, $\ldots$, $h_l(x_1, \ldots, x_n) = 0$, $t \cdot f(x_1, \ldots, x_n) - 1 = 0$. Из условия вытекает, что эта система несовместна; стало быть, в силу первой части теоремы Гильберта о нулях, существуют такие многочлены $\tilde{g}_1, \ldots, \tilde{g}_{l+1}$ от $X_1, \ldots, X_n$ и T, что выполнено тождество

$$\tilde{g}_1(X_1, \ldots, X_n, T) h_1(X_1, \ldots, X_n) + \cdots + \tilde{g}_l(X_1, \ldots, X_n, T) h_l(X_1, \ldots, X_n) + \\ + \tilde{g}_{l+1}(X_1, \ldots, X_n, T)(T f(X_1, \ldots, X_n) - 1) = 1.$$

Подставив в это тождество $1/f(X_1, \ldots, X_n)$ вместо T и избавившись от знаменателя, получим требуемое соотношение. $\square$

Подведем итог тому, что мы узнали про операции V и I:

Следствие 1.8. *Соответствия $V \mapsto I(V)$ и $I \mapsto V(I)$ задают обращающее включения взаимно однозначное соответствие между множеством замкнутых по Зарисскому подмножеств $\mathbb{A}^n$ и множеством идеалов $k[X_1, \ldots, X_n]$, совпадающих со своим радикалом.*

Топология Зарисского не только мало похожа на «классические» топологии, но и — сама по себе — несет достаточно мало информации (например, все алгебраические кривые в этой топологии гомеоморфны). Тем не менее есть по крайней мере одно важное понятие, которое естественно определить в чисто «топологических по Зарисскому» терминах:

Определение 1.9. Топологическое пространство X называется *неприводимым,* если оно удовлетворяет одному из следующих эквивалентных условий:

а) X нельзя представить в виде объединения двух замкнутых подмножеств, отличных от X;

б) Всякое открытое подмножество $U \subset X$ всюду плотно в X.

Предоставляем слушателям убедиться в том, что эти условия действительно эквивалентны, а также показать, что хаусдорфово пространство является неприводимым тогда и только тогда, когда оно состоит из одной точки. Стало быть, для отделимых пространств определение неприводимости бессодержательно; а вот для топологии Зарисского оно работает. Вот

Пример 1.10. Пусть f — многочлен; положим $Z = V(f)$ (такие подмножества называются *гиперповерхностями*). Если $f = f_1^{r_1} \ldots f_m^{r_m}$ — разложение f на неприводимые множители, то $Z = V(f_1) \cup \cdots \cup V(f_m)$, причем следствие 1.8 показывает, что ни одно из $V(f_i)$ не совпадает с Z (если $m > 1$, разумеется). Стало быть, если f приводим, то гиперповерхность $V(f)$ также приводима; с другой стороны, нетрудно показать, что все $V(f_i)$ уже неприводимы (и вообще, $V(f)$ неприводима если f неприводим — вскоре мы докажем более общее утверждение).

Ситуация из этого примера является типичной:

Предложение 1.11. *Пусть $X \subset \mathbb{A}^n$ — замкнутое по Зарисскому множество. Тогда $X = \bigcup_{i=1}^m X_i$, где все X_i замкнуты, неприводимы, и ни одно из множеств X_i не содержится в другом. Такое разложение единственно.*

Доказательство. Начнем с существования. Если X неприводимо, то доказывать нечего. Пусть X приводимо, $X = X_1 \cup Y_1$. Если X_1 и Y_1 неприводимы, то разложение уже есть; если, скажем, X_1 приводимо, $X_1 = X_2 \cup Y_2$, то $X = X_2 \cup Y_1 \cup Y_2$; если среди этих трех множеств есть приводимые, продолжим этот процесс, и т. д. Через конечное число шагов этот процесс оборвется: в противном случае у нас получилась бы бесконечная цепочка замкнутых множеств $X \supset X_1 \supset X_2 \ldots$, в которой каждое последующее множество строго меньше предыдущего, и тем самым (в силу следствия 1.8) бесконечная строго возрастающая цепочка идеалов $I(X) \subset I(X_1) \subset I(X_2) \ldots$, чего в нётеровом кольце быть не может (см. §1 главы VI книги Ленга). Осталось только из полученного разложения $X = \bigcup X_j$ выкинуть множества, содержащиеся в объединении остальных (если $X_j \subset \bigcup_{i \neq j} X_i$, то в силу неприводимости $X_j \subset X_i$ для некоторого i).

Чтобы доказать единственность, предположим, что

$$X = X_1 \cup \dots \cup X_m = X'_1 \cup \dots \cup X'_l$$

— два разложения X в объединение не содержащихся друг в друге неприводимых множеств. Тогда для всякого $j \in [1; m]$ имеем $X_j = \bigcup_{i=1}^{l} (X_j \cap X'_i)$, откуда, в силу неприводимости, $X_j \subset X'_i$ для некоторого i. Аналогично, всякое X'_i содержится в некотором X_j. Так как различные X_j (а также различные X'_j) друг в друге не содержатся, то вышеупомянутые включения являются равенствами, и два разложения совпадают. □

Разложение, о котором шла речь в этом предложении, называется *разложением на неприводимые компоненты.*

Полезно также выяснить, какие идеалы соответствуют неприводимым множествам:

Предложение 1.12. *Замкнутое множество $X \subset \mathbb{A}^n$ неприводимо тогда и только тогда, когда идеал $I(X)$ прост.*

Доказательство. Пусть X неприводимо и $fg \in I(X)$. Тогда $X = (X \cap V(f)) \cup (X \cap V(g))$, откуда, в силу неприводимости, $X \subset V(f)$ или $X \subset V(g)$, то есть $f \in I(X)$ или $g \in I(X)$. Это означает, что $I(X)$ — простой идеал; часть «только тогда» доказана.

Если $I(X)$ прост и $X = Y_1 \cup Y_2$, то $I(Y_1)I(Y_2) \subset I(X)$, откуда (в силу простоты $I(X)$) либо $I(Y_1)$, либо $I(Y_2)$ содержится в (и тем самым совпадает с) $I(X)$. Значит, X совпадает с Y_1 или Y_2, что и доказывает его неприводимость. □

Замечание 1.13. В свете примера 1.10 разложение замкнутого множества на неприводимые компоненты можно рассматривать как обобщение разложения многочлена на неприводимые множители. Из того же примера видно, что при этом обобщении часть информации теряется: из разложения гиперповерхности $V(f)$ на компоненты невозможно увидеть, с какими кратностями неприводимые множители входят в разложение f. По-настоящему точным обобщением разложения на неприводимые множители является так называемое примарное разложение идеала. В нашем курсе оно не встретится; прочитать про него можно в любом руководстве по коммутативной алгебре.

Теперь мы можем, наконец, дать важное

Определение 1.14. *Аффинным алгебраическим многообразием* называется неприводимое замкнутое по Зарисскому подмножество аффинного пространства $\mathbb{A}^n$. Если $V \subset \mathbb{A}^n$ — аффинное многообразие, то *регулярной функцией* на V называется функция из V в k, являющаяся ограничением на V многочлена от $X_1, \ldots, X_n$.

Всерьез работать с аффинными многообразиями мы начнем на следующей лекции. Пока же — три простых, но важных замечания.

Во-первых, регулярные функции на аффинном многообразии $V \subset \mathbb{A}^n$ образуют кольцо; это кольцо обозначается $k[V]$. По самому́ определению имеем $k[V] \cong k[X_1, \ldots, X_n]/I(V)$.

Во-вторых, теорема Гильберта о нулях и следствие 1.8 остаются верными, если в их формулировках заменить $\mathbb{A}^n$ на произвольное аффинное многообразие V, а кольцо многочленов — на $k[V]$:

Предложение 1.15. *Пусть X — аффинное многообразие. Для всякого подмножества $M \subset X$ положим $I(M) = \{ f \in k[X] \mid f|_M = 0 \}$, а для всякого идеала $I \subset k[X]$ положим $V(I) = \{ x \in X \mid f(x) = 0 \text{ для всех } f \in I \}$. Тогда:*

а) $V(I) \neq \varnothing$ тогда и только тогда, когда $I \neq k[X]$;

б) $I(V(I)) = r(I)$;

в) $V(I(M)) = \overline{M}$;

г) Соответствия $V \mapsto I(V)$ и $I \mapsto V(I)$ задают обращающее включения взаимно однозначное соответствие между множеством замкнутых по Зарисскому подмножеств X и множеством идеалов $k[X]$, совпадающих со своим радикалом.

Все эти утверждения мгновенно сводятся к их аналогам для $\mathbb{A}^n$.

В-третьих, предложение 1.12 показывает, что для аффинного многообразия $V \subset \mathbb{A}^n$ кольцо регулярных функций $k[V] \cong k[X_1, \ldots, X_n]/I(V)$ является конечно порожденной k-алгеброй без делителей нуля. Обратно, если k-алгебра A порождена, скажем, n образующими и не имеет делителей нуля, то $A \cong k[X_1, \ldots, X_n]/\mathfrak{p}$, где $\mathfrak{p}$ — простой идеал. Полагая $V = V(\mathfrak{p}) \subset \mathbb{A}^n$, получаем, что V — аффинное многообразие и $A \cong k[V]$. Следовательно, классы колец регулярных функций на аффинных многообразиях и конечно порожденных k-алгебр без делителей нуля совпадают.