Теорема Гильберта о нулях

Сегодня будет доказана использовавшаяся в первой части курса

Теорема 1 (Теорема Гильберта о нулях). *Пусть $X \subset \mathbb{A}^n_{\mathsf{k}}$ – замкнутое алгебраическое подмножество аффинного пространства над алгебраически замкнутым полем k, заданное как множество нулей многочленов $f_1, \ldots, f_m \in \mathsf{k}[x_1, \ldots, x_n]$. Пусть f – многочлен, тождественно равный нулю на X. Тогда f^N лежит в идеале $(f_1, \ldots, f_m)$ при некотором N.*

Другая, более компактная алгебраическая формулировка:

Теорема 2. *Пусть $I \subset \mathsf{k}[x_1, \ldots, x_n]$ – идеал, $\mathsf{k} = \bar{\mathsf{k}}$. Тогда $I(V(I)) = r(I)$.*

Имеется простое, но важное

Следствие 3. *Пусть $I \subset \mathsf{k}[x_1, \ldots, x_n]$ – собственный идеал, $\mathsf{k} = \bar{\mathsf{k}}$. Тогда $V(I)$ непусто.*

Для доказательства нам понадобится следующий сугубо алгебраический факт.

Теорема 4 (алгебраическая версия теоремы Гильберта о нулях). *Пусть A – конечно порождённая алгебра над полем k, сама являющаяся полем. Тогда A – конечное расширение поля k, т.е. конечно порождённый k-модуль.*

Пример 5.

1. Пусть $A = \mathsf{k}[x]$. Тогда A конечно порождена над k как алгебра, но A – не поле. Теорема неприменима, и A – не конечно порождённый модуль над k.
2. Пусть $A = \mathsf{k}(x)$. Тогда A – поле и A конечно порождено над k как поле. Но A не конечно порождена как алгебра. Теорема неприменима, и A – не конечно порождённый модуль над k.

Доказательство теоремы 4. Рассмотрим частный случай: A порождена над k одним элементом x. Тогда если x алгебраический над k, то расширение конечно, т.к. можно выбрать базис над k из степеней x. Если же x трансцендентен над k, то $A \cong \mathsf{k}(x)$, а это не конечно порождённая алгебра над k.

В общем случае идея та же. Пусть $x_1, \ldots, x_n$ порождают A над k. Тогда с точностью до перенумерации можно считать, что $x_1, \ldots, x_m$ алгебраически независимы над k, а $x_{m+1}, \ldots, x_n$ алгебраичны над полем $F = \mathsf{k}(x_1, \ldots, x_m)$. Тогда поле A – конечное расширение F, так как порождено конечным числом алгебраических элементов. Пусть $e_1, \ldots, e_d$ – базис A как векторного пространства над F. Выразим порождающие: $x_i = \sum c_{ij} e_j$, $c_{ij} \in F$. Выразим произведения: $e_i e_j = \sum c_{ijk} e_k$, $c_{ijk} \in F$. Любой элемент в A – многочлен от x_i с коэффициентами в k. Подставим в него вместо x_i их выражения через e_j, потом последовательно будем заменять произведения $e_i e_j$ на их выражение через e_k. Получим, что любой элемент a в A записывается единственным образом как линейная комбинация e_i, где коэффициенты – многочлены от c_{ij} и c_{ijk}:

$$a = \sum e_p \lambda_p, \quad \lambda_p \in \mathsf{k}[c_{ij}, c_{ijk}].$$

Элементы c_{ij} и c_{ijk} – рациональные функции от $x_1, \ldots, x_m$. В знаменателях в них участвует конечное число неприводимых многочленов. Следовательно, в выражении всех элементов $a = \sum e_p \lambda_p$ в знаменателях λ_p встречается лишь конечное число неприводимых многочленов. Пусть $f \in \mathsf{k}[x_1, \ldots, x_m]$ – неприводимый многочлен, которого там нет. Рассмотрим элемент e_1/f и получим противоречие, если только $m > 0$. Следовательно, $m = 0$, $F = \mathsf{k}$ и A – конечный k-модуль. $\square$

Предложение 6. *Предположим, что поле* k *алгебраически замкнуто. Тогда все максимальные идеалы в кольце* $A = \mathsf{k}[x_1, \ldots, x_n]$ *имеют вид* $I(P) = (x_1 - a_1, \ldots, x_n - a_n)$ *для некоторой точки* $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$.

Доказательство. Напомним удобный критерий: идеал $I \subset R$ максимален титтк фактор-кольцо R/I – поле.

Проверим сперва, что идеалы указанного вида максимальны. Пусть $P = (a_1, \ldots, a_n)$ – точка, рассмотрим гомоморфизм $\mathsf{k}[x_1, \ldots, x_n] \to \mathsf{k}$, переводящий f в $f(P)$. Он сюръективен, и его ядро – идеал $I(P)$, значит $A/I(P) \cong \mathsf{k}$ и $I(P)$ максимален.

Обратно, пусть $\mathfrak{m} \subset A$ – максимальный идеал, тогда поле $F = A/\mathfrak{m}$ содержит поле k и конечно порождено над ним как алгебра (т.к. алгебра A конечно порождена). Значит, по теореме 4 поле F – конечное расширение k. Но k алгебраически замкнуто, поэтому $F = \mathsf{k}$. Пусть элементы $\bar{x}_i \in F$ (образы $x_i \in A$) соответствуют числам $a_i \in \mathsf{k}$. Тогда образы $x_i - a_i$ в F равны нулю и $x_i - a_i \in \mathfrak{m}$. Следовательно, $I(P) = (x_1 - a_1, \ldots, x_n - a_n) \subset \mathfrak{m}$. Из максимальности $I(P)$ получаем, что $I(P) = \mathfrak{m}$. □

Доказательство следствия 3. Это доказательство не зависит от теоремы 1 и будет использовано для её получения.

Пусть $I \subset \mathsf{k}[x_1, \ldots, x_n]$ – собственный идеал. Его можно вложить в максимальный идеал $\mathfrak{m}$. Он имеет вид $\mathfrak{m} = I(P)$ для некоторой точки $P \in \mathbb{A}^n$. Тогда $P \in V(I)$: если $f \in I$, то $f \in I(P)$ и $f(P) = 0$. □

Доказательство теоремы 1. Пусть $X \subset \mathbb{A}^n$ задано уравнениями $f_1 = \ldots = f_m = 0$, и $f|_X = 0$. Рассмотрим $\bar{X} \subset \mathbb{A}^{n+1}$, заданное уравнениями

$$f_i(x_1, \ldots, x_n) = 0 \quad \text{и} \quad x_{n+1} f(x_1, \ldots, x_n) - 1 = 0.$$

Очевидно, $\bar{X}$ пусто: если $f_i(x_1, \ldots, x_n) = 0$, то $x_{n+1} f(x_1, \ldots, x_n) - 1 = -1 \neq 0$. Значит, по следствию 3 многочлены $f_i(x_1, \ldots, x_n)$ и $x_{n+1} f(x_1, \ldots, x_n) - 1$ порождают всё кольцо $\mathsf{k}[x_1, \ldots, x_{n+1}]$. Запишем

$$1 = b(x_1, \ldots, x_{n+1})(x_{n+1} f(x_1, \ldots, x_n) - 1) + \sum a_i(x_1, \ldots, x_{n+1}) f_i(x_1, \ldots, x_n).$$

Пусть N – максимальная степень, с которой x_{n+1} входит в многочлены a_i, домножим на f^N.

$$f(x)^N = f(x)^n b(x)(x_{n+1} f(x) - 1) + \sum f(x)^N a_i(x_1, \ldots, x_{n+1}) f_i(x_1, \ldots, x_n).$$

Для всех встреч x_{n+1}^d в a_i заменим $x_{n+1}^d f^d$ на $1 + (x_{n+1}^d f^d - 1) = 1 + (x_{n+1} f - 1)(\ldots)$. Перенесём $(x_{n+1} f - 1)(\ldots)$ в слагаемое, где $b(x)(x_{n+1} f(x) - 1)$. Получим:

$$f(x_1, \ldots, x_n)^N = \widetilde{b}(x)(x_{n+1} f(x_1, \ldots, x_n) - 1) + \sum \widetilde{a}_i(x_1, \ldots, x_n) f_i(x_1, \ldots, x_n).$$

Здесь f^N и все слагаемые суммы не содержат x_{n+1}, а $\widetilde{b}(x)(x_{n+1} f - 1)$ содержит её, если только $\widetilde{b}(x) \neq 0$. Значит, $\widetilde{b}(x) = 0$

$$f(x_1, \ldots, x_n)^N = \sum \widetilde{a}_i(x_1, \ldots, x_n) f_i(x_1, \ldots, x_n),$$

что и требовалось. □

Итак, максимальные идеалы в кольце многочленов над замкнутым полем соответствуют точкам аффинного пространства. Верно аналогичное и для любых аффинных многообразий.

Предложение 7. *Пусть $X \subset \mathbb{A}^n$ – аффинное многообразие над полем $\mathsf{k} = \bar{\mathsf{k}}$. Тогда любой максимальный идеал в $\mathsf{k}[X]$ имеет вид $I(P)$ для $P \in X$.*

Доказательство. Пусть $A = \mathsf{k}[x_1, \ldots, x_n]$, а $p\colon A \to \mathsf{k}[X]$ – естественная сюръекция, $\mathfrak{m} \subset \mathsf{k}[X]$ – максимальный идеал. Тогда $p^{-1}\mathfrak{m} \subset A$ – максимальный идеал, т.к. отображение $A/p^{-1}\mathfrak{m} \to \mathsf{k}[X]/\mathfrak{m}$ биективно. По предложению 6 имеем $p^{-1}\mathfrak{m} = I(P)$ и $\mathfrak{m}$ – идеал точки P. При этом $P \in X$: если функция $f \in A$ обращается в ноль всюду на X, то $f \in \ker p \subset p^{-1}\mathfrak{m} = I(P)$, т.е. $f(P) = 0$. □

Итак, максимальные идеалы кольца регулярных функций – это точки многообразия. В абстрактной алгебраической геометрии это принимается за определение точки многообразия. Что происходит с точками при регулярном отображении?

Пусть $f\colon X \to Y$ – регулярное отображение аффинных многообразий, $f^*\colon \mathsf{k}[Y] \to \mathsf{k}[X]$ – двойственное отображение на функциях, $x \in X$ – точка, $I(x) \subset \mathsf{k}[X]$ – соответствующий максимальный идеал. Тогда $(f^*)^{-1}I(x) \subset \mathsf{k}[Y]$ – идеал, состоящий из функций $g \in \mathsf{k}[Y]$ таких, что $f^*(g) = gf \in I(x)$, т.е. $gf(x) = 0$, т.е. $g(f(x)) = 0$. Значит, это идеал $I(f(x))$. Итак, образу точек при регулярном отображении соответствует прообраз максимального идеала.

Пример 8. Прообраз максимального идеала при гомоморфизме колец не всегда максимален: рассмотрим вложение $\mathbb{Z} \to \mathbb{Q}$. Прообраз максимального идеала $(0) \subset \mathbb{Q}$ – идеал $(0) \subset \mathbb{Z}$, он не максимален.

Однако для конечно порождённых алгебр над полем алгебр всё хорошо.

Лемма 9. *Пусть $p\colon A \to B$ – гомоморфизм конечно порождённых над полем k алгебр, а $\mathfrak{m} \subset B$ – максимальный идеал. Тогда идеал $p^{-1}\mathfrak{m}$ максимален.*

Доказательство. Поле $B/\mathfrak{m}$ конечно порождено над k, значит по теореме Гильберта $B/\mathfrak{m}$ конечно над k. Индуцированный гомоморфизм $A/p^{-1}\mathfrak{m} \to B/\mathfrak{m}$ – вложение, притом $\mathsf{k} \subset A/p^{-1}\mathfrak{m}$. Поэтому алгебра $A/p^{-1}\mathfrak{m}$ порождена над k конечным числом алгебраических элементов и потому является полем. Т.е. $p^{-1}\mathfrak{m} \subset A$ – максимальный идеал. □

Часто помимо максимальных идеалов (точек аффинного многообразия) бывает удобно рассматривать одновременно все простые идеалы (неприводимые подмногообразия в заданном). Для них прообраз всегда прост:

Лемма 10. *Пусть $p\colon A \to B$ – гомоморфизм колец, а $\mathfrak{p} \subset B$ – простой идеал. Тогда идеал $p^{-1}\mathfrak{p}$ прост.*

Доказательство. Напомним удобный критерий: идеал $I \subset R$ прост титтк кольцо I/R не имеет делителей нуля.

Индуцированный гомоморфизм $A/p^{-1}\mathfrak{p} \to B/\mathfrak{p}$ – вложение. Кольцо $B/\mathfrak{p}$ не имеет делителей нуля, значит их нет и в $A/p^{-1}\mathfrak{p}$. Т.е. $p^{-1}\mathfrak{p} \subset A$ – простой идеал. □

Геометрически прообраз простого идеала соответствует образу подмногообразия. А именно, пусть $f\colon X \to Y$ – регулярное отображение аффинных многообразий, $f^*\colon \mathsf{k}[Y] \to \mathsf{k}[X]$ – двойственное отображение на функциях, $W \subset X$ – неприводимое подмногообразие, $I(W) \subset \mathsf{k}[X]$ – соответствующий простой идеал. Тогда $(f^*)^{-1}I(W) \subset \mathsf{k}[Y]$ – идеал, состоящий из функций $g \in \mathsf{k}[Y]$ таких, что $gf \in I(W)$, т.е. $gf = 0$ на W, т.е. $g = 0$ на $f(W)$. Значит, $(f^*)^{-1}I(W)$ – это идеал замыкания $f(W)$ в топологии Зарисского.

Как на языке идеалов описать прообраз? Пусть во введенных обозначениях $y \in Y$ – точка и $I(y) \subset \mathsf{k}[Y]$ – её идеал. Тогда

$$f(x) = y \Leftrightarrow (f^*)^{-1}I(x) = I(y) \Leftrightarrow f^*(I(y)) \subset I(x).$$

Аналогично для подмногообразия $W \subset X$ имеем $f(W) = y$ титтк $I(W) \supset f^*(I(y))$. Отсюда ясно, что интерес представляют минимальные простые идеалы в $\mathsf{k}[X]$ среди содержащих $f^*(I(Y))$. Это – в точности минимальные ассоциированные с $(f^*(I(Y)))$ простые идеалы из листка 5, они соответствуют неприводимым компонентам в $f^{-1}(y)$.

Отметим, что образ идеала $I \subset A$ при гомоморфизме колец $p\colon A \to B$ – не обязательно идеал. Однако всегда можно рассмотреть идеал $(p(I)) \subset B$, порождённый множеством $p(I)$. Часто его и называют *образом идеала* при гомоморфизме. Он может совпадать со все кольцом, геометрически это соответствует тому, что прообраз подмногообразия пуст. Идеал, порождённый образом простого идеала, не обязательно прост. Геометрически это может означать, что прообраз неприводимого многообразия приводим, либо что через $p(I)$ выражаются не все полиномиальные соотношения на точки прообраза.

Пример 11. Рассмотрим отображение $f\colon \mathbb{A}^2 \to \mathbb{A}^1, f(x,y) = xy$. Двойственное отображения на функциях такое: $f^*\colon \mathsf{k}[t] \to \mathsf{k}[x,y], f^*(t) = xy$. Образ (t) в $\mathsf{k}[x,y]$ – это $\mathsf{k}[xy]$, идеал $(f^*(t)) = (xy)$. Он не прост, раскладывается в пересечение двух ассоциированных простых идеалов: $(x) \cap (y)$. Прообраз точки 0 при f – это пара прямых.

Пример 12. Рассмотрим отображение $f\colon \mathbb{A}^1 \to \mathbb{A}^1, f(x) = x^2$. Двойственное отображения на функциях такое: $f^*\colon \mathsf{k}[x] \to \mathsf{k}[x], f^*(x) = x^2$. Образ (x) в $\mathsf{k}[x]$ – это $\mathsf{k}[x^2]$, идеал $(f^*(x)) = (x^2)$. Он не прост, но его радикал (x) прост, это единственный ассоциированный идеал. Это значит, что прообразом является неприводимое многообразие (точка 0), но «взятое с кратностью 2».

Изучим коротко важное понятие локализации кольца. Одна из геометрических мотивировок такова.

Пусть $X \subset \mathbb{A}^n$ – аффинное многообразие, а $f \in \mathsf{k}[x_1, \dots, x_n]$ – многочлен. Положим $X_f = \{x \in X \mid f(x) \neq 0\}$, это также аффинное многообразие. Как описать на нём регулярные функции? X_f вкладывается в $\mathbb{A}^{n+1}$ следующим образом. Пусть $I(X)$ порождён многочленами f_i. Рассмотрим $\bar{X} \subset \mathbb{A}^{n+1}$, заданное уравнениями $f_i(x_1, \dots, x_n) = 0$ и $x_{n+1}f(x_1, \dots, x_n) - 1 = 0$. Тогда проекция $\bar{X} \to X$: $(x_1, \dots, x_{n+1}) \mapsto (x_1, \dots, x_n)$ даёт изоморфизм между $\bar{X}$ и X_f. Итак,

$$\mathsf{k}[X_f] = \mathsf{k}[x_1, \dots, x_{n+1}]/(f_i, x_{n+1}f - 1) = \mathsf{k}[X][x_{n+1}]/(x_{n+1}f - 1),$$

говоря неформально,

$$\mathsf{k}[X_f] = \mathsf{k}[X][1/f],$$

где роль $1/f$ играет x_{n+1}. Формально обращение функции f в $\mathsf{k}[X]$ – пример локализации кольца.

Определение 13. *Мультипликативной системой* в коммутативном кольце A называется любое подмножество $S \subset A$, замкнутое относительно умножения и не содержащее 0. Для удобства будем считать, что $1 \in S$.

Определение 14. Пусть $S \subset A$ – мультипликативная система. *Локализацией* A по S называется кольцо A_S вместе с гомоморфизмом $l\colon A \to A_S$, для которых выполнены два условия.

1. Элемент $l(s) \in A_S$ обратим при всех $s \in S$.

2. Для любого гомоморфизма $f\colon A \to B$ такого, что $f(s)$ обратимы при всех $s \in S$, существует единственный гомоморфизм $g\colon A_S \to B$, для которого $gl = f$.

Попросту говоря, локализация A по S – это формальное обращение всех элементов из S. Из универсального определения следует, что локализация единственна. Существование проверяется явной конструкцией, обобщающей построение поля частных.

Обозначим через A_S множество классов дробей a/s ($a \in A$, $s \in S$) по следующему отношению эквивалентности: $a/s \sim a'/s'$, если $(as' - a's)s'' = 0$ для подходящего $s'' \in S$. Определим сложение и умножение дробей обычными формулами, приводя к общему знаменателю. Определим гомоморфизм $l\colon A \to A_S$ формулой $l(a) = a/1$. Тогда $l(s)$ обратим: $s/1 \cdot 1/s \sim 1/1$. Можно проверить, что так определённое кольцо будет удовлетворять нужному универсальному свойству.

Пример 15. Пусть A – кольцо без делителей нуля, рассмотрим мультипликативную систему $S = A \setminus 0$. Тогда локализация A_S – поле частных A.

Следующие два примера – основные в геометрии.

Пример 16. Пусть $\mathfrak{p} \subset A$ – простой идеал. Тогда система $S = A \setminus \mathfrak{p}$ мультипликативна. Локализация по ней называется локализацией по простому идеалу. Геометрически, если $Y \subset X$ – неприводимое подмногообразие в аффинном, то локализация $\mathsf{k}[X]$ по $I(Y)$ – это множество рациональных функций на X, хорошо определённых на Y.

Пример 17. Пусть $f \in A$ – не нильпотентный элемент. Тогда $S = \{1, f, f^2, f^3, \ldots\}$ – мультипликативная система. Локализация по ней – это формальное обращение одного элемента кольца. Геометрически, если f – регулярная функция на многообразии X, то локализация $\mathsf{k}[X]$ по f – это множество регулярных функций на X_f.