8. Лекция 8

Рассмотрим n-мерное аффинное пространство $\mathbb{A}^n = \mathbb{A}^n_K$ над полем K, которое мы определим как множество наборов $(x_1, \ldots, x_n)$, где $x_i \in K$. Мы будем изучать *аффинные алгебраические множества* — подмножества в $\mathbb{A}^n$, получаемые как множества решений систем полиномиальных уравнений $f_\alpha(x_1, x_2, \ldots, x_n) = 0$.

Пример 8.1. Окружность на плоскости является аффинным алгебраическим множеством (это множество решений уравнения $x^2 + y^2 - 1 = 0$), а график синусоиды таковым не является (почему, будет ясно чуть позже).

Вообще говоря, системам уравнений разрешается быть бесконечными. Однако оказывается, что всякая бесконечная система полиномиальных уравнений эквивалентна некоторой конечной системе. Это следует из *теоремы Гильберта о базисе.*

8.1. **Нётеровы кольца, теорема Гильберта о базисе.**

Напомним определение нётерова кольца:

Определение 8.2. Коммутативное кольцо A с 1 называется *нётеровым*, если выполнено любое из двух эквивалентных условий:

(1) всякий идеал в A порождается конечным числом элементов;
(2) В A не бывает бесконечно возрастающей цепочки вложенных идеалов $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \ldots$. Иначе говоря, всякая возрастающая цепочка идеалов стабилизируется[1].

Упражнение 8.3. Докажите эквивалентность этих условий.

Пример 8.4. Всякое кольцо главных идеалов нётерово (в нём любой идеал порождён *одним* элементом).

Теорема 8.5 (Теорема Гильберта о базисе, Basissatz)**.** *Пусть A — нетерово кольцо. Тогда кольцо многочленов $A[x]$ тоже нетерово.*

Доказательство. Будем пользоваться первым определением нетеровости. Пусть $I \subset A[x]$ — идеал в кольце многочленов. Докажем, что он конечно порождён.

Рассмотрим множество всевозможных многочленов из I. Их старшие коэффициенты образуют идеал в A (почему?), который мы обозначим через L. Идеал L конечно порождён; выберем в нем какую-нибудь систему образующих $L = (a_1, \ldots, a_r)$. Для каждой из этих образующих возьмём многочлен $f_i = a_i x^{d_i} + \cdots \in I$ со старшим членом a_i. Пусть d_i — степень этого многочлена.

Выберем максимум этих степеней: $N = \max(d_i)$. Для каждого числа $d < N$ рассмотрим множество I_d всех многочленов из I степени не выше d. Их старшие коэффициенты снова образуют идеал

[1] По-английски это условие называется accending chain condition, сокращенно ACC.

в A, который мы обозначим через L_d. Обозначим его образующие через $b_{1,d}, \dots, b_{r_d,d}$ и для каждой из этих образующих выберем в I_d многочлен с соответствующим старшим коэффициентом: $g_{i,d} = b_{i,d}x^d + \dots$. Мы получим конечное множество многочленов $g_{i,d}$, где $d < N$.

По построению, все многочлены f_i и $g_{i,d}$ лежат в идеале I. Породим ими идеал $I' \subset I$. Докажем, что это включение на самом деле является равенством. Преположим противное и возьмём многочлен $h \in I \setminus I'$ минимальной степени. Пусть $h = ax^m + \dots$.

Возможны два случая, в зависимости от степени h. Первый случай: пусть $\deg h \geq N$. Старший коэффициент a многочлена h лежит в L по построению, и при этом $\deg h$ не меньше степеней всех образующих f_i. Тогда найдётся такой многочлен $f \in I'$ такой же степени и с таким же старшим коэффициентом, как h. Поэтому их разность $h - f$ будет лежать в I, но не в I', и будет иметь меньшую степень. Противоречие.

Если же $\deg h < N$, то $h \in I_d$ для некоторого d, а значит, найдётся такой многочлен g, являющийся линейной комбинацией $g_{i,d}$ (т.е. лежащий в I'), который имеет ту же степень и тот же старший член, что h. Снова получаем противоречие с минимальностью степени многочлена h. □

Следствие 8.6. *Кольцо многочленов от конечного числа переменных нетерово.*

Следствие 8.7. *Всякая бесконечная система алгебраических уравнений эквивалентна некоторой конечной системе.*

Доказательство. Породим уравнениями первой системы идеал и выберем в нём конечный базис. □

Замечание 8.8. Теорема Гильберта о базисе утверждает, что базис идеала существует, но не даёт никакого способа его найти. Явное алгоритмическое нахождение такого базиса является предметом теории базисов Грёбнера.

8.2. **Топология Зарисского.** Введём в пространстве $\mathbb{A}^n$ топологию, определив замкнутые подмножества.

Определение 8.9. Множество общих нулей $X \subset \mathbb{A}^n$ системы полиномиальных уравнений $f_i(x_1, \dots, x_n) = 0$ называется *замкнутым в топологии Зарисского.*

По определению, открытые множества — это дополнения до замкнутых.

Пример 8.10. Замкнутые по Зарисскому подмножества прямой $\mathbb{A}^1$ — это пустое множество, вся прямая и всевозможные *конечные* наборы точек.

Убедимся, что это действительно определяет топологию. В самом деле, справедливо следующее

Предложение 8.11. *Объединение конечного числа замкнутых множеств замкнуто; пересечение любого числа замкнутых множеств замкнуто.*

Доказательство. Пересечение замкнутых множеств соответствует объединению систем уравнений, определяющих эти множества. С объединением дело обстоит немногим сложнее: если X задаётся системой уравнений $\{f_\alpha = 0\}$, а Y — системой $\{g_\beta = 0\}$, то их объединение есть множество нулей системы $\{f_\alpha g_\beta = 0\}$. □

8.3. **Теорема Гильберта о нулях, слабая форма.** Пусть у нас имеется некоторая система уравнений $\{f_\alpha = 0\}$. Когда она вообще имеет решение? И, наоборот, когда решений нет? Сразу можно указать ответ на второй вопрос: когда идеал (f_α) содержит единицу, т.е. если при помощи алгебраических комбинаций уравнений системы можно получить уравнение $1 = 0$, то система, очевидно, неразрешима. Теорема Гильберта о нулях (вернее, её слабая форма) утверждает, что если основное поле алгебраически замкнуто, то это необходимое условие является также и достаточным.

Теорема 8.12 (Теорема Гильберта о нулях, слабая форма)**.** *Пусть поле K алгебраически замкнуто. Система полиномиальных уравнений $\{f_\alpha(x_1, \dots, x_n) = 0\}$ не имеет общих решений тогда и только тогда, когда идеал $(f_alpha) \subset K[x_1, \dots, x_n]$ совпадает со всем кольцом, или, что то же самое, найдутся такие $f_1, \dots, f_m$ из системы уравнений и такие многочлены $g_1, \dots, g_m \in K[x_1, \dots, x_n]$, что*

$$f_1 g_1 + \dots + f_m g_m = 1.$$

Доказательство этой теоремы будет приведено в следующей лекции.

Замечание 8.13. Над алгебраически незамкнутым полем теорема, очевидно, неверна: так, идеал $(x^2 + 1) \subset \mathbb{R}[x]$ не совпадает со всем кольцом, но соответствующее уравнение не имеет корней.

Пусть $\xi = (\xi_1, \dots, \xi_n) \in \mathbb{A}^n$ — произвольная точка. Рассмотрим идеал функций, обращающихся в ней в нуль. Тогда $\mathfrak{m}_\xi = (x_1 - \xi_1, \dots, x_n - \xi_n)$ Очевидно, этот идеал максимален: $K[x_1, \dots, x_n]/\mathfrak{m}_\xi \cong K$, причём изоморфизм задаётся вычислением полинома в данной точке (его ядро — это те полиномы, которые в ней равны нулю). Оказывается, других максимальных идеалов нет.

Предложение 8.14. *Всякий максимальный идеал в кольце многочленов над алгебраически замкнутым полем имеет вид $\mathfrak{m}_\xi$ для некоторой точки ξ.*

Доказательство. Рассмотрим произвольный максимальный идеал $\mathfrak{m} \subset K[x_1, \ldots, x_n]$. Он отличен от всего кольца, т.е. не содержит единицу. Поэтому, согласно теореме Гильберта о нулях, существуют такие точки, где все многочлены из этого идеала обращаются в нуль. Поскольку идеал максимален, то такая точка только одна (иначе бы $\mathfrak{m}$ содержался бы собственным образом в идеале $\mathfrak{m}_\xi$ для каждой из этих точек, что противоречит максимальности). □

8.4. **Соответствие между идеалами и их множествами нулей.** Пусть $X \subset \mathbb{A}^n$ — замкнутое по Зарисскому множество. Ему можно сопоставить идеал функций $I(X) \subset K[x_1, \ldots, x_n]$, обращающихся в нуль на X.

Обратно, если у нас имеется идеал $I \subset K[x_1, \ldots, x_n]$, ему соответствует замкнутое по Зарисскому множество точек $V(I) \subset \mathbb{A}^n$, где все функции из этого идеала обращаются в нуль. По слабой теореме Гильберта о нулях, для собственного идеала это множество будет непустым.

Таким образом, имеются два отображения: из идеалов в замкнутые множества и обратно. У этих отображений существует две композиции (в разном порядке). Рассмотрим их подробнее.

Что получится, если начать с множества X, сопоставить ему идеал $I(X)$, а потом по нему построить множество $V(I(X))$? Оказывается, получится само X. Это тавтология: идеал $I(X)$ состоит из функций, равных нулю на X, а множество точек, где все эти функции равны нулю, есть $V(I(X))$.

Теперь рассмотрим отображение из идеалов в идеалы, задаваемое композицией этих двух отображений в другом порядке: т.е. идеалу I сопоставляется идеал $I(V(I))$. С одной стороны, ясно, что $I \subset I(V(I))$. Однако несложно построить пример, когда это включение строгое.

Пример 8.15. Пусть $I = (x^n) \subset K[x]$. Тогда $V(I) = \{0\}$, и $I(V(I)) = (x)$.

То есть соответствия $I \mapsto V(I)$ и $X \to I(X)$ не биективны. (Вернее, первое из них не инъективно, а второе не сюръективно). Оказывается, их можно сделать биекциями, сузив множество рассматриваемых идеалов.

Определение 8.16. *Радикал* идеала $I \subset A$ в кольце A — это идеал $r(I) = \{f \in A \mid f^n \in I\}$, состоящий из всех элементов, некоторая степень которых содержится в I. Идеал называется *радикальным*, если $r(I) = I$.

Упражнение 8.17. Проверьте, что $r(I)$ действительно является идеалом, а при каноническом эпиморфизме $A \to A/I$ идеал $r(I)$ переходит в нильрадикал кольца A/I (т.е. в идеал всех нильпотентных элементов этого кольца). Соответственно, идеал I радикален тогда и только тогда, когда A/I не содержит нильпотентов.

Упражнение 8.18. Проверьте, что $r(r(I)) = r(I)$.

Сильная форма теоремы Гильберта о нулях утверждает, что соответствие между замкнутыми по Зарисскому подмножествами в $\mathbb{A}^n$ и *радикальными* идеалами в кольце $K[x_1, \dots, x_n]$ является биекцией.

Теорема 8.19 (Теорема Гильберта о нулях, сильная форма)**.** *Если $I \subset K[x_1, \dots, x_n]$ — идеал, то $I(V(I)) = r(I)$. Более подробно, если многочлен f обращается в нуль на множестве общих нулей системы $h_1 = \dots = h_m = 0$, то найдётся такое натуральное число k и многочлены $g_1, \dots, g_m$, что*

$$g_1 h_1 + \dots + g_m h_m = f^k.$$

Эту теорему мы также докажем (вернее, выведем из слабой теоремы Гильберта о нулях) в следующей лекции.