Алгебраические подмножества аффинного пространства

Пусть k – некоторое поле, например, поле действительных или комплексных чисел.

Определение 1. *Аффинным n-мерным пространством* $\mathbb{A}^n_{\mathsf{k}}$ над k называется множество наборов $(x_1, \ldots, x_n), x_i \in \mathsf{k}$ элементов k длины n.

Алгебраическим подмножеством аффинного пространства $\mathbb{A}^n$ называется множество решений некоторой (возможно, бесконечной) системы уравнений $f_\alpha(x_1, \ldots, x_n) = 0$, где $f_\alpha \in \mathsf{k}[x_1, \ldots, x_n]$ – многочлены. Обозначается такое множество $V(f_\alpha)$.

Как мы вскоре увидим, на самом деле всегда достаточно конечного числа уравнений – остальные будут из них следовать.

Пример 2.

1. окружность – задаётся уравнением $x^2 + y^2 - 1 = 0$ в вещественной плоскости $\mathbb{A}^2_{\mathbb{R}}$;
2. параметризованная кривая $\{(t^2, t^3, t^4) \mid t \in \mathbb{C}\} \subset \mathbb{A}^3_{\mathbb{C}}$ задаётся уравнениями $x^3 - y^2 = z - x^2 = 0$;
3. точка $(a_1, \ldots, a_n)$ задаётся уравнениями $x_i - a_i = 0$.
4. график функции $y = \sin x$ – не алгебраическое подмножество.

Одно и то же подмножество можно задавать разными системами уравнений. Рассмотрим максимальную из них.

Определение 3. *Идеалом* алгебраического подмножества $X \subset \mathbb{A}^n_{\mathsf{k}}$ называется

$$I(X) = \{f \in \mathsf{k}[x_i] \mid f|_X = 0\}$$

– множество всех многочленов, обращающихся в ноль тождественно на X.

Напомним, что

Определение 4. *Идеалом* в коммутативном кольце A называется множество $I \subset A$, для которого верно:

- $x, y \in I \Rightarrow x + y \in I$;
- $x \in I \Rightarrow -x \in I$;
- $x \in I, a \in A \Rightarrow ax \in I$.

Очевидно, идеал алгебраического подмножества — это идеал в кольце $\mathsf{k}[x_1, \ldots, x_n]$. Ясно также, что для алгебраического подмножества X верно $V(I(X)) = X$, поэтому любое алгебраическое подмножество есть множество нулей многочленов некоторого идеала.

С другой стороны, любое алгебраическое подмножество можно задать конечным числом уравнений. Впрочем, это совсем не очевидно.

Определение 5. Идеалом в кольце A, *порождённым* набором элементов $a_1, \ldots, a_m \in A$, называется минимальный идеал в A, содержащий все a_i. Этот идеал можно описать явно как множество элементов вида $\sum_{i=1}^m a_i b_i$, где $b_i \in A$ — произвольные элементы. Такой идеал обозначается $(a_1, \ldots, a_m)$ и называется *конечно порождённым*.

Имеет место важная теорема, которую мы прямо сейчас доказывать не будем.

Теорема 6 (теорема Гильберта о базисе). *Любой идеал в кольце* $\mathsf{k}[x_1, \dots, x_n]$ *конечно порождён.*

Следствие 7. *Любое алгебраическое подмножество* $X \subset \mathbb{A}^n$ *задаётся конечным числом уравнений.*

Доказательство. Идеал $I(X) \subset \mathsf{k}[x_1, \dots, x_n]$ конечно порождён, пусть $I(X) = (f_1, \dots, f_m)$. Тогда $X = V(I(X)) = V(f_1, \dots, f_m)$: действительно, пусть для некоторой точки $x \in \mathbb{A}^n$ все $f_i(x) = 0$. Тогда $f(x) = 0$ при всех f вида $\sum_i f_i g_i$, которые и образуют $I(X)$. Значит, X есть множество общих нулей многочленов $f_1, \dots, f_m$, ч.т.д. □

Лемма 8. *Объединение и пересечение алгебраических подмножеств – алгебраическое подмножество.*

Доказательство. Пусть алгебраические подмножества V и W заданы системами уравнений $f_i = 0$ и $g_j = 0$. Тогда $V \cap W$ задаётся системой $f_i = g_j = 0$, а $V \cup W$ – системой $f_i g_j = 0$ (все попарные произведения). □

Изучим для начала простейший пример аффинных подмножеств – кривые на плоскости. Будем считать, что основное поле — алгебраически замкнутое.

Определение 9. *Плоской алгебраической кривой* $V(f) \subset \mathbb{A}^2_{\mathsf{k}}$ назовём множество решений уравнения $f(x, y) = 0$, где $f \in \mathsf{k}[x, y]$ – многочлен (отличный от константы).

Если $f = f_1 f_2$, то кривая распадается в объединение двух кривых: $V(f) = V(f_1) \cup V(f_2)$. Естественно поэтому изучить кривые, заданные многочленом f, который не раскладывается на множители.

Определение 10. Многочлен $f \in \mathsf{k}[x_1, \dots, x_n]$ называется *неприводимым*, если из $f = g \cdot h$, где $g, h \in \mathsf{k}[x_1, \dots, x_n]$ следует $\deg g = 0$ или $\deg h = 0$.

Что будет, если пересечь две плоские кривые? Чтобы это понять, докажем две леммы.

Лемма 11. *Если многочлен* $g \in \mathsf{k}[x, y]$ *обращается в ноль тождественно на* $V(f)$, *то* $g^N \vdots f$ *для некоторой степени* N.

Доказательство. Сделав линейную замену переменных, можно считать, что f содержит член x^N, где $N = \deg f$. Тогда можно делить на f с остатком в кольце многочленов $(\mathsf{k}[y])[x]$ (как многочлены от x). При любом фиксированном значении $y = y_0$ корни f лежат среди корней g. Поскольку возможны кратности, то $g(x, y_0)^N \vdots f(x, y_0)$. Поделим с остатком как многочлены от x: $g^N = f \cdot q + r$, $\deg_x r < \deg f$. При любом y_0 имеем $r(x, y_0) = 0$, а значит $r = 0$. □

Следствие 12. *Если многочлен* $g \in \mathsf{k}[x, y]$ *обращается в ноль на множестве нулей неприводимого многочлена* f, *то* $g \vdots f$. *Другими словами,* $I(V(f)) = (f)$.

Следствие 13. *Если* f *неприводим, то кривая* $V(f)$ *не представляется в виде объединения двух нетривиальных (отличных от* $V(f)$*) алгебраических подмножеств.*

Доказательство. Если $V(f) = C_1 \cup C_2$, то найдутся многочлены f_1 и f_2, для которых f_i обращается в нуль на C_i, но не на $V(f)$. Тогда $f_1 f_2$ равен нулю на $V(f)$, значит $f_1 f_2 \vdots f$. Так как f неприводим, то f_1 или $f_2 \vdots f$ и значит f_1 или f_2 равен нулю на $V(f)$ – противоречие. □

Определение 14. Алгебраическое подмножество называется *неприводимым*, если его нельзя представить в виде объединения двух строго меньших алгебраических подмножеств.

То есть, множество нулей неприводимого многочлена на плоскости – неприводимая кривая. Теперь пересечём неприводимую кривую нетривиальным образом.

Лемма 15. *Пусть многочлен $f \in \mathsf{k}[x, y]$ неприводим и g не делится на f. Тогда пересечение $V(f) \cap V(g)$ – конечное множество.*

Доказательство. Рассмотрим НОД f и g в кольце $\mathsf{k}(y)[x]$. Пусть он равен многочлену $h(x, y) \in \mathsf{k}[x, y]$ с точностью до умножения на обратимые, причём коэффициенты h по степеням x взаимно просты. Тогда $f \vdots h$ в $\mathsf{k}(y)[x]$ влечёт $f \vdots h$ в $\mathsf{k}[y, x]$. Так как f неприводим, $h = 1$ либо $h = f$. Во втором случае $g \vdots f$ в $\mathsf{k}(y)[x]$ и значит в $\mathsf{k}[y, x]$ – противоречие условию. Поэтому $h = 1$. Запишем $1 = \alpha g + \beta f$, где $\alpha, \beta \in \mathsf{k}(y)[x]$. Тогда для всех y_0 (кроме конечного числа нулей знаменателей в α и β) получим, что $f(x, y_0)$ и $g(x, y_0)$ не могут иметь общих корней по x. А для конечного числа y_0 получим конечное число корней, т.е. точек пересечения $V(f)$ и $V(g)$. □

Следствие 16. *Алгебраические подмножества аффинной плоскости (нетривиальные) – это конечные объединения неприводимых кривых (заданных неприводимым многочленом) и точек.*

Доказательство. Рассмотрим последовательно уравнения, задающие подмножество. $V(f_1)$ есть объединение конечного числа неприводимых кривых. Пересекая далее каждую из них с нулями многочленов, получим либо конечное число точек, либо её саму. □

Алгебраические подмножества плоской неприводимой кривой – конечные множества точек. Это можно взять за определение неприводимой кривой. Кривой далее естественно назвать конечное объединение неприводимых кривых. Неприводимой поверхностью назовём алгебраическое подмножество, нетривиальные алгебраические подмножества которого – конечные объединения кривых и точек, поверхностью – конечное объединение неприводимых поверхностей, и т.д. Так можно определить алгебраические множества любой размерности, но есть более компактный (и равносильный) способ сделать это.

Определение 17. *Размерностью* (точнее говоря, *размерностью Крулля*) алгебраического подмножества X называется максимум таких n, что в X существует цепочка строго вложенных неприводимых алгебраических подмножеств

$$X_n \supset X_{n-1} \supset \ldots \supset X_1 \supset X_0.$$

Обозначение: $\dim X$.

Очевидно, что размерность аффинной прямой – 1, и мы показали, что размерность аффинной плоскости – 2. Конечно, верно и то, что размерность $\mathbb{A}^n_{\mathsf{k}}$ равна n, но доказать это совсем не просто.

Приведём без доказательства несколько свойств размерности

Предложение 18.

1. $\dim \mathbb{A}^n = n$. *Предположим далее, что поле* k *алгебраически замкнуто.*
2. *Пусть* $f \in \mathsf{k}[x_1, \dots, x_n], \deg f > 0$. *Тогда* $\dim V(f) = n - 1$.
3. *Более общо, если* $X \subset \mathbb{A}^n$ *— неприводимое подмножество и* $f \in \mathsf{k}[x_1, \dots, x_n]$ *— не равный всюду нулю на* X *многочлен, то* $X \cap V(f)$ *имеет размерность* $\dim X - 1$ *или пусто.*

Определение 19. *Гиперповерхностью* в $\mathbb{A}^n$ называется подмножество вида $V(f)$, где $f \in \mathsf{k}[x_1, \dots, x_n], \deg f > 0$. *Степенью* гиперповерхности $V(f)$ называется число $\deg f$.