Теорема Гильберта о нулях

В прошлый раз мы выяснили, что замкнутые подмногообразия аффинного многообразия взаимно-однозначно соответствуют радикальным идеалам в кольце регулярных функций на X. Сегодня мы продолжим переводить разные геометрические понятия на алгебраический язык. Как и прежде, **поле предполагается алгебраически замкнутым**, а под **многообразием** мы имеем в виду **аффинное алгебраическое многообразие**.

Предложение 1. *Аффинное многообразие X неприводимо $\iff$ в кольце $\mathsf{k}[X]$ нет делителей нуля.*

Доказательство. Если есть делители нуля: $f_1 f_2 = 0$, то получаем разложение: $X = \{f_1 = 0\} \cup \{f_2 = 0\}$. Обратно, если разложение $X = X_1 \cup X_2$ нетривиально, то найдутся функции f_i такие, что $f_i|_{X_i} = 0$ и $f_i \neq 0$. Тогда $f_1 f_2 = 0$, значит есть делители нуля. □

Следствие 2. *Пусть $Y \subset X$ — аффинное подмногообразие. Идеал $I(Y) \subset \mathsf{k}[X]$ прост $\iff$ Y неприводимо.*

Доказательство. Многообразие Y неприводимо $\Leftrightarrow$ $\mathsf{k}[Y] = \mathsf{k}[X]/I(Y)$ не имеет делителей нуля $\Leftrightarrow$ $I(Y)$ прост. □

Предложение 3. *Пусть X — аффинное многообразие, а $J \subset \mathsf{k}[X]$ — радикальный идеал. Тогда $J = \cap_{i=1}^m \mathfrak{p}_i$ есть пересечение некоторых простых идеалов $\mathfrak{p}_i$.*

Доказательство. Многообразие $Y = V(J)$ раскладывается в объединение неприводимых компонент $Y = \cup_{i=1}^m Y_i$. Переходя к идеалам при помощи предложения 15 прошлой лекции, получаем

$$J = r(J) = I(V(J)) = I(\cup Y_i) = \cap I(Y_i),$$

где идеалы $\mathfrak{p}_i = I(Y_i)$ простые по следствию 2. □

Замечание 4. Композиция регулярных отображений регулярна.

Пусть $\phi\colon X \to Y$ — регулярное отображение. Оно определяет гомоморфизм

$$\phi^*\colon \mathsf{k}[Y] \to \mathsf{k}[X]$$

на алгебрах функций: если $f \in \mathsf{k}[Y]$, то положим $\phi^* f = f \circ \phi$.

Замечание 5. Для отображений $X \xrightarrow{\phi} Y \xrightarrow{\psi} Z$ имеем $(\psi\phi)^* = \phi^*\psi^*$.

Предложение 6. *Пусть $s\colon \mathsf{k}[Y] \to \mathsf{k}[X]$ — гомоморфизм алгебр над k. Тогда он имеет вид ϕ^* для единственного регулярного отображения $\phi\colon X \to Y$.*

Доказательство. Пусть $Y \subset \mathbb{A}^m$, y_i — координатные функции на $\mathbb{A}^m$, а $\bar{y}_i \in \mathsf{k}[Y]$ — их ограничения на Y. Положим

$$\phi(x) = (s(\bar{y}_1)(x), \dots, s(\bar{y}_m)(x)).$$

Так как $s(\bar{y}_i)$ — регулярные на X функции, то ϕ регулярно по определению. Проверим, что $\operatorname{im}\phi \subset Y$. Пусть $f \in I(Y)$ — многочлен, покажем, что f обнуляется на образе ϕ. Действительно,

$$f(s(\bar{y}_1)(x), \dots, s(\bar{y}_m)(x)) = s(f(\bar{y}_1, \dots, \bar{y}_m))(x) = s(0)(x) = 0.$$

Ясно, что $\phi^* = s$ на всех $\bar{y}_i$ и значит, на всей алгебре $\mathsf{k}[Y]$. Ясно также, что ϕ единственно. □

Следствие 7. *Пусть $\phi\colon X \to Y$ — регулярное отображение между аффинными многообразиями и ϕ^* — изоморфизм. Тогда ϕ — изоморфизм.*

Пусть $\mathsf{k}[X]$ и $\mathsf{k}[Y]$ изоморфны. Тогда X и Y изоморфны.

Предложение 8. *Подмногообразия аффинных многообразий соответствуют сюръективным гомоморфизмам алгебр функций.*

Доказательство. Пусть $X \subset Y$ — аффинное подмногообразие. Любая регулярная функция на X — ограничение многочлена с аффинного пространства, а значит, и ограничение регулярной функции с Y. Поэтому имеем сюръекцию $\mathsf{k}[Y] \to \mathsf{k}[X]$ — ограничение.

Обратно, если гомоморфизм $\phi^*\colon \mathsf{k}[Y] \to \mathsf{k}[X]$ сюръективен, пусть I — его ядро. Пусть подмногообразие $X' \subset Y$ — множество нулей всех функций из I. Тогда образ ϕ лежит в X', и если $f \in I(X')$, то $\phi(f) = 0$, поэтому $f \in I$. Значит $I = I(X')$ и для отображения $\psi\colon X \to X'$ имеем $\psi^*\colon \mathsf{k}[X'] = \mathsf{k}[Y]/I \to \mathsf{k}[X]$ — изоморфизм. По следствию 7 получаем, что ψ — изоморфизм, т.е. X — подмногообразие. □

Пример 9. Пусть $X = \mathbb{A}^1$, $Y = \mathbb{A}^2$, $\phi(t) = (t^2, t^3)$. Тогда $\phi^*(x) = t^2$, $\phi^*(y) = t^3$. Образ ϕ^* — подкольцо $\mathsf{k}[t^2, t^3] \subset \mathsf{k}[t]$, т.е. ϕ^* не сюръективно. Хотя отображение ϕ и инъективно на множестве точек, оно не является вложением подмногообразия — его образ не изоморфен $\mathbb{A}^1$.

Напомним

Определение 10. Подмножество M топологического пространства X называется *плотным*, если его замыкание $\overline{M}$ совпадает с X.

Предложение 11. *Отображение $\phi\colon X \to Y$ имеет плотный (в топологии Зарисского) образ $\iff$ гомоморфизм ϕ^* инъективен.*

Доказательство. Если ϕ^* имеет нетривиальное ядро, возьмём $f \in \mathsf{k}[Y]$, $\phi^* f = 0$. Тогда образ ϕ (а значит, и его замыкание) лежит в замкнутом подмножестве $\{y \mid f(y) = 0\} \subset Y$, и потому не плотен. Обратно, если $\overline{\operatorname{im}\phi} \neq Y$, то найдётся ненулевая $f \in \mathsf{k}[Y]$ такая, что $f = 0$ на $\phi(Y)$. Значит, ядро ϕ^* нетривиально. □

Пример 12. Пусть $X = Y = \mathbb{A}^2$, $\phi(u, v) = (u, uv)$. Тогда $\phi^*(x) = u, \phi^*(y) = uv$, и ϕ^* инъективен. При этом образ ϕ состоит из точек (x, y), где $x \neq 0$, и точки $(0, 0)$. Он не замкнут и не открыт, но плотен. Если же взять $\psi(u, v) = (u - v, (u - v)^2)$, то $\psi^*(x^2 - y) = 0$, то есть, ψ^* не инъективно. При этом образ ψ — парабола на плоскости, это не плотное множество.

Предложение 13. *Вложения многообразия X в аффинное пространство соответствуют системам образующих в алгебре $\mathsf{k}[X]$.*

Доказательство. Если $X \subset \mathbb{A}^n$, то ограничения координатных функций $\bar{x}_i \in \mathsf{k}[X]$ порождают алгебру $\mathsf{k}[X]$. Обратно, системе порождающих $e_1, \ldots, e_n \in \mathsf{k}[X]$ соответствует сюръективный гомоморфизм $\mathsf{k}[x_1, \ldots, x_n] \to \mathsf{k}[X]$, а значит, по предложению 8, вложение $X \subset \mathbb{A}^n$. □

Теперь вернёмся к теореме Гильберта о нулях. Напомним

Теорема 14. *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 15. *Пусть $J \subset \mathsf{k}[X]$ – идеал в кольце функций аффинного алгебраического многообразия X, $\mathsf{k} = \bar{\mathsf{k}}$. Тогда $I(V(J)) = r(J)$.*

Имеется простое, но важное

Следствие 16. *Пусть $J \subset \mathsf{k}[x_1, \ldots, x_n]$ – собственный идеал, $\mathsf{k} = \bar{\mathsf{k}}$. Тогда $V(J)$ непусто.*

Для доказательства нам понадобится следующий сугубо алгебраический факт.

Теорема 17 (алгебраическая версия теоремы Гильберта о нулях)**.** *Пусть A – конечно порождённое кольцо над полем k, само являющееся полем. Тогда A – конечное расширение поля k, т.е. конечномерно над k.*

Пример 18.

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.

Следствие 19. *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 $\iff$ 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 17 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 16. Это доказательство не зависит от теоремы Гильберта 17 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 17. 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 20. *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 19 имеем $p^{-1}\mathfrak{m} = I(P)$. При этом $I(X) = \ker p \subset p^{-1}\mathfrak{m} = I(P)$, следовательно $P \in X$. □

Итак, максимальные идеалы кольца регулярных функций – это точки многообразия. В абстрактной алгебраической геометрии это принимается за определение точки многообразия.