Лекция 7 Теорема Гильберта о нулях

7.1

Напомним, что для аффинного многообразия $V \subset k^n$ множество
$$\mathbb{I}(V) := \{ f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in V \}$$
всех многочленов, зануляющихся на V, является идеалом в $k[x_1, \dots, x_n]$. Таким образом, имеется отображение
$$\begin{array}{rccc} & \{\text{аффинные многообразия}\} & \longrightarrow & \{\text{идеалы в } k[x_1, \dots, x_n]\}, \\ (7.1) & V & \longmapsto & \mathbb{I}(V). \end{array}$$
Для идеала $I \subset k[x_1, \dots, x_n]$ мы можем определить подмножество
$$\mathbb{V}(I) := \{ (a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \quad \forall f \in I \}$$
в k^n, которое по теореме Гильберта о базисе является аффинным многообразием. Тем самым, имеется и отображение
$$\begin{array}{rccc} & \{\text{идеалы в } k[x_1, \dots, x_n]\} & \longrightarrow & \{\text{аффинные многообразия}\}, \\ (7.2) & I & \longmapsto & \mathbb{V}(I). \end{array}$$

Отметим, что отображение $\mathbb{V}(\cdot)$ не является инъективным. Например, идеалам $\langle x \rangle$ и $\langle x^2 \rangle$ кольца $k[x]$ соответствует аффинное многообразие $V = \{0\} \subset k$. В случае алгебраически незамкнутого поля возникает ещё больше проблем: если $I_1 = \langle 1 \rangle$, $I_2 = \langle 1 + x^2 \rangle$, $I_3 = \langle 1 + x^2 + x^4 \rangle$ — идеалы в $\mathbb{R}[x]$, то
$$\mathbb{V}(I_1) = \mathbb{V}(I_2) = \mathbb{V}(I_3) = \varnothing.$$

Пусть k — алгебраически замкнутое поле, а $I \subset k[x]$ — идеал, т.ч. $\mathbb{V}(I) = \varnothing$. Поскольку $k[x]$ — кольцо главных идеалов, идеал $I = \langle f \rangle$, где $f \in k[x]$. Так как k — алгебраически замкнутое поле, то любой многочлен положительной степени имеет корень в k. Значит из $\mathbb{V}(I) = \varnothing$ следует, что $f \in k - \{0\}$ и идеал $I = \langle 1 \rangle = k[x]$. То есть в кольце $k[x]$, где k — алгебраически замкнутое поле, $\mathbb{V}(I) = \varnothing$ в том и только том случае, когда $I = k[x]$.

Оказывается, что этот факт остаётся верным и для $k[x_1, \dots, x_n]$.

Теорема 7.1: (слабая теорема Гильберта о нулях)

Пусть k - алгебраически замкнутое поле, $I \subset k[x_1, \dots, x_n]$ — идеал. Тогда аффинное многообразие $\mathbb{V}(I) = \varnothing$, если и только если $I = k[x_1, \dots, x_n]$.

Доказательство: Если $I = k[x_1, \dots, x_n]$, то $1 \in I$ и $\mathbb{V}(I) = \varnothing$.

Для доказательства обратного утверждения покажем, что $1 \in I$. Будем делать это по индукции. База индукции $(n=1)$ уже доказана.

Пусть утверждение справедливо в кольце многочленов от $(n-1)$ переменной, которое запишем в виде $k[x_2,\dots,x_n]$. Рассмотрим идеал $I=\langle f_1,\dots,f_s\rangle$ в кольце $k[x_1,\dots,x_n]$ такой, что $\mathbb{V}(I)=\varnothing$. Можно считать, что многочлен f_1 не является постоянным. Итак, его общая степень $N\geq 1$. Сделаем в f_1 линейную замену переменных

$$x_1=\tilde{x}_1,$$
$$x_2=\tilde{x}_2+a_2\tilde{x}_1,$$
$$\vdots$$
$$x_n=\tilde{x}_n+a_n\tilde{x}_1,$$

где $a_j\in k$ подобраны должным образом. А именно, в многочлене

$$f_1(x_1,\dots,x_n)=f_1(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\dots,\tilde{x}_n+a_n\tilde{x}_1)=c(a_2,\dots,a_n)\tilde{x}_1^N+\text{слагаемые, где степень } \tilde{x}_1<N$$

коэффициент $c(a_2,\dots,a_n)\neq 0$. Записав многочлен f в виде суммы

$$f=h_N+h_{N-1}+\dots+h_0$$

однородных компонент h_j степени j, где $0\leq j\leq N$, заметим, что

$$h_N(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\dots,\tilde{x}_n+a_n\tilde{x}_1)=\sum\alpha_{i_1\dots i_n}x_1^{i_1}x_2^{i_2}\cdot\ldots\cdot x_n^{i_n}=$$

$$=\sum\alpha_{i_1\dots i_n}\tilde{x}_1^{i_1}(\tilde{x}_2+a_2\tilde{x}_1)^{i_2}\dots(\tilde{x}_n+a_n\tilde{x}_1)^{i_n}=\Big(\sum\alpha_{i_1\dots i_n}a_2^{i_2}\cdot\ldots\cdot a_n^{i_n}\Big)\tilde{x}_1^N+\text{слагаемые, где степень } \tilde{x}_1<N=$$

$$=h_N(1,a_2,\dots,a_n)\tilde{x}_1^N+\text{слагаемые, где степень } \tilde{x}_1<N,$$

то есть $c(a_2,\dots,a_n)=h_N(1,a_2,\dots,a_n)$. Поскольку $h_N\in k[x_1,\dots,x_n]$ — ненулевой однородный многочлен, многочлен $h_N(1,a_2,\dots,a_n)\in k[a_2,\dots,a_n]$ тоже является ненулевым. Таким образом, действительно существуют $a_2,\dots,a_n\in k$ такие, что $c(a_2,\dots,a_n)\neq 0$.

Указанное линейное преобразование индуцирует гомоморфизм колец

$$k[x_1,\dots,x_n]\to k[\tilde{x}_1,\dots,\tilde{x}_n]$$
$$f\mapsto \tilde{f}:=f(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\dots,\tilde{x}_n+a_n\tilde{x}_1).$$

Образ $\tilde{I}=\{\tilde{f}: f\in I\}$ идеала I сам является идеалом в $k[\tilde{x}_1,\dots,\tilde{x}_n]$. Из $\mathbb{V}(I)=\varnothing$ вытекает, что аффинное многообразие $\mathbb{V}(\tilde{I})=\varnothing$. Так как гомоморфизм оставляет на месте константы из поля k, из $1\in\tilde{I}$ следует, что $1\in I$.

Рассмотрим идеал исключения $\tilde{I}_1:=\tilde{I}\cap k[\tilde{x}_2,\dots,\tilde{x}_n]$. Одна из образующих идеала $\tilde{I}$ имеет вид

$$\tilde{f}_1=c(a_2,\dots,a_n)\tilde{x}_1^N+\text{слагаемые, где степень } \tilde{x}_1<N,$$

где $c(a_2,\dots,a_n)\in k-\{0\}$. Тогда по следствию из теорема 5.2 о продолжении, которая остаётся справедливой и для произвольного алгебраически замкнутого поля k, $\mathbb{V}(\tilde{I}_1)=\pi_1(\mathbb{V}(\tilde{I}))$, где π_1 — проекция из k^n на аффинное подпространство k^{n-1} с координатами $\tilde{x}_2,\dots,\tilde{x}_n$. Следовательно, $\mathbb{V}(\tilde{I}_1)=\pi_1(\mathbb{V}(\tilde{I}))=\pi_1(\varnothing)=\varnothing$, откуда, т.к. $\tilde{I}_1\in k[\tilde{x}_2,\dots,\tilde{x}_n]$, по предположению индукции $1\in\tilde{I}_1$, а значит и $1\in\tilde{I}$. Тем самым, теорема доказана. ◀

Слабая теорема Гильберта о нулях даёт практический способ разрешения вопроса о совместности системы полиномиальных уравнений с коэффициентами в алгебраически замкнутом поле

$$f_1=0,\ \dots,\ f_s=0,$$

— нужно проверить, что $1\in\langle f_1,\dots,f_s\rangle$ (либо найти остаток от деления 1 на базис Грёбнера этого идеала, либо найти редуцированный базис Грёбнера этого идеала).

7.2 Теорема Гильберта о нулях

Как показывают примеры идеалов $\langle x \rangle$ и $\langle x^2 \rangle$, переход к алгебраически замкнутому полю не делает отображение (7.2) инъективным. Следующая теорема говорит, в случае алгебраически замкнутого поля, единственная причина, по которой разные идеалы задают одно многообразие — это то, что зануление многочлена f во всех точках $\mathbb{V}(I)$ влечёт принадлежность некоторой степени этого многочлена идеалу I.

Теорема 7.2: (Гильберта о нулях) Пусть k — алгебраически замкнутое поле. Если $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$, т.ч. $f \in \mathbb{I}(\mathbb{V}(f_1, \dots, f_s))$, то существует целое $m \geq 1$, для которого

$$f^m \in \langle f_1, \dots, f_s \rangle$$

(обратное утверждение очевидно тоже является верным)

Доказательство: (трюк Рабиновича) Рассмотрим идеал

$$\tilde{I} := \langle f_1, \dots, f_s, 1 - yf \rangle$$

в кольце $k[x_1, \dots, x_n, y]$. Покажем, что ни одна точка $a = (a_1, \dots, a_n, a_{n+1}) \in k^{n+1}$ не может лежать в $\mathbb{V}(\tilde{I})$. Если $(a_1, \dots, a_n) \in \mathbb{V}(f_1, \dots, f_s)$, то $f(a_1, \dots, a_n) = 0$ по условию теоремы. Тогда многочлен $(1 - yf)(a) = 1 - a_{n+1} f(a_1, \dots, a_n) = 1 \neq 0$, т.е. такая точка $a \notin \mathbb{V}(\tilde{I})$. Если же теперь точка $(a_1, \dots, a_n) \notin \mathbb{V}(f_1, \dots, f_s)$, то найдётся f_i, т.ч. $f_i(a_1, \dots, a_n) \neq 0$, где $i \in \{1, \dots, s\}$. Поскольку $f_i \in \tilde{I} \cap k[x_1, \dots, x_n]$, то как элемент кольца $k[x_1, \dots, x_n, y]$ многочлен $f_i(a_1, \dots, a_n, a_{n+1}) \neq 0$. Значит, и такая точка $(a_1, \dots, a_n, a_{n+1})$ не лежит в $\mathbb{V}(\tilde{I})$. Следовательно, $\mathbb{V}(\tilde{I}) = \emptyset$.

Тогда по слабой теореме Гильберта о нулях $1 \in \tilde{I}$, т.е. найдутся $p_1, \dots, p_s, q \in k[x_1, \dots, x_n, y]$, т.ч.

$$1 = \sum_{i=1}^{s} p_i(x_1, \dots, x_n, y) f_i + q(x_1, \dots, x_n, y)(1 - yf).$$

Правую часть указанного равенства можно трактовать как многочлен из кольца $(k(x_1, \dots, x_n))[y]$. Вычислив его значение в т. $1/f(x_1, \dots, x_n) \in k(x_1, \dots, x_n)$, мы получим равенство

$$1 = \sum_{i=1}^{s} p_i(x_1, \dots, x_n, \tfrac{1}{f}) f_i$$

в $k(x_1, \dots, x_n)$. Очевидно, что домножив его на достаточно большую степень f^m, мы придём к тому, что в кольце $k[x_1, \dots, x_n]$

$$f^m = \sum_{i=1}^{s} \tilde{p}_i \cdot f_i,$$

где $\tilde{p}_i \in k[x_1, \dots, x_n]$. Следовательно, $f^m \in \langle f_1, \dots, f_s \rangle$. ◀

7.3 Радикальные идеалы

Определение 7.1: Идеал I называется радикальным, если $f^m \in I$ влечёт $f \in I$.

Заметим, что для аффинного многообразия V, если $f^m \in \mathbb{I}(V)$, то и $f \in \mathbb{I}(V)$. Таким образом, $\mathbb{I}(V)$ — радикальный идеал.

Определение 7.2: Пусть $I \subset k[x_1, \dots, x_n]$ — идеал. Его радикалом называется
$$\sqrt{I} := \{f \in k[x_1, \dots, x_n] : f^m \in I \text{ для некоторого целого } m \geq 1\}.$$
Идеал I содержится в своём радикале $\sqrt{I}$. Очевидно, что I радикальный $\Leftrightarrow I = \sqrt{I}$.

Утверждение 7.1: Пусть $I \subset k[x_1, \dots, x_n]$ — идеал. Тогда его радикал $\sqrt{I}$ является радикальным идеалом в $k[x_1, \dots, x_n]$.

Доказательство: Сперва докажем, что $\sqrt{I}$ — идеал. Пусть $f, g \in \sqrt{I}$, тогда существуют целые $m \geq 1$ и $\ell \geq 1$, т.ч. $f^m, g^\ell \in I$. Согласно формуле бинома Ньютона
$$(f+g)^{m+\ell-1} = \sum_{i+j=m+\ell-1} C^i_{i+j} f^i g^j,$$
где $f^i \in I$ при $i \geq m$, $g^j \in I$ при $j \geq \ell$, т.е. каждое слагаемое лежит в I, а значит $(f+g)^{m+\ell-1} \in I$. Таким образом, $f+g \in \sqrt{I}$. Наконец, если $f \in \sqrt{I}$, то $f^m \in I$. Для любого $h \in k[x_1, \dots, x_n]$ произведение $h^m \cdot f^m = (hf)^m \in I$, т.е. $hf \in \sqrt{I}$. Следовательно, $\sqrt{I}$ действительно идеал.

Докажем радикальность $\sqrt{I}$. Рассмотрим многочлен $f \in k[x_1, \dots, x_n]$, т.ч. $f^m \in \sqrt{I}$ для некоторого целого $m \geq 1$. По определению радикала найдётся такое целое $\ell \geq 1$, что степень $(f^m)^\ell = f^{m\ell} \in I$. Отсюда получаем, что $f \in \sqrt{I}$. ◀

Теперь переформулируем в новых терминах теорему Гильберта о нулях.

Теорема 7.3: (Гильберта о нулях) Пусть k — алгебраически замкнутое поле. Если $I \subset k[x_1, \dots, x_n]$ — идеал, то
$$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}.$$
Доказательство: Докажем, что $\sqrt{I} \subset \mathbb{I}(\mathbb{V}(I))$. Если многочлен $f \in \sqrt{I}$, то его некоторая степень $f^m \in I$. Тогда f^m зануляется на $\mathbb{V}(I)$, а значит и f зануляется на $\mathbb{V}(I)$, то есть $f \in \mathbb{I}(\mathbb{V}(I))$.

Покажем обратное включение $\mathbb{I}(\mathbb{V}(I)) \subset \sqrt{I}$. Пусть $f \in \mathbb{I}(\mathbb{V}(I))$, тогда по теореме Гильберта о нулях $f^m \in I$ для некоторого целого $m \geq 1$, поэтому $f \in \sqrt{I}$. ◀

Теорема 7.4: (о соответствии между идеалами и многообразиями)
Пусть k — произвольное поле. Тогда
(i) Отображения $\{\text{афф. мн-зия}\} \xrightarrow{\mathbb{I}} \{\text{идеалы}\}$ и $\{\text{идеалы}\} \xrightarrow{\mathbb{V}} \{\text{афф. мн-зия}\}$ обращают включения, т.е., если идеал $I_1 \subset I_2$, то $\mathbb{V}(I_1) \supset \mathbb{V}(I_2)$, а также, если аффинные многообразия $V_1 \subset V_2$, то $\mathbb{I}(V_1) \supset \mathbb{I}(V_2)$. Более того, для всякого аффинного многообразия V справедливо $\mathbb{V}(\mathbb{I}(V)) = V$, т.е. $\mathbb{I}$ является 1:1 отображением.
(ii) Если k алгебраически замкнуто, то отображения $\{\text{афф. мн-зия}\} \xrightarrow{\mathbb{I}} \{\text{радикальные идеалы}\}$ и $\{\text{радикальные идеалы}\} \xrightarrow{\mathbb{V}} \{\text{афф. мн-зия}\}$ являются взаимно-обратными, обращающими включения биекциями.

Доказательство: (i) Пусть $I_1 \subset I_2$, если точка $a \in \mathbb{V}(I_2)$, то она зануляет всякий многочлен из I_2, в частности, она занулит и всякий многочлен из I_1, т.е. $a \in \mathbb{V}(I_1)$. Таким образом, $\mathbb{V}(I_2) \subset \mathbb{V}(I_1)$.

Пусть теперь $V_1 \subset V_2$, если $f \in \mathbb{I}(V_2)$, то он зануляется в каждой точке многообразия V_2, то он зануляется и в каждой точке многообразия V_1. Следовательно, $f \in \mathbb{I}(V_1)$, и $\mathbb{I}(V_2) \subset \mathbb{I}(V_1)$.

Покажем, что $\mathbb{V}(\mathbb{I}(V)) = V$ для аффинного многообразия $V = \mathbb{V}(f_1, \dots, f_s) \subset k^n$. Включение $V \subset \mathbb{V}(\mathbb{I}(V))$ следует сразу из определения $\mathbb{I}(\cdot)$ и $\mathbb{V}(\cdot)$. Теперь заметим, что $f_1, \dots, f_s \in \mathbb{I}(V)$ по определению $\mathbb{I}(\cdot)$, значит $\langle f_1, \dots, f_s \rangle \subset \mathbb{I}(V)$. Так как $\mathbb{V}$ обращает включение, то $\mathbb{V}(\mathbb{I}(V)) \subset \mathbb{V}(\langle f_1, \dots, f_s \rangle) = V$. Таким образом, $\mathbb{V}(\mathbb{I}(V)) = V$, и $\mathbb{I}$ является 1:1 отображением, так как у него есть левое обратное.

(ii) Идеал $\mathbb{I}(V)$ радикальный, поэтому отображение $\mathbb{I}$ переводит аффинное многообразие в радикальный идеал. Поскольку $\mathbb{V}(\mathbb{I}(V)) = V$ уже доказано, то остаётся показать, что $\mathbb{I}(\mathbb{V}(I)) = I$, если I радикальный. Но из теоремы Гильберта о нулях следует, что $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$, а $\sqrt{I} = I$, т.к. I радикальный. Следовательно, отображения $\mathbb{V}$ и $\mathbb{I}$ взаимнообратные и определяют биекцию между множествами радикальных идеалов и аффинных многообразий. ◀

Следующее утверждение позволяет алгоритмически выяснять лежит ли многочлен $f \in k[x_1, \dots, x_n]$ в радикале идеала $I = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$.

Утверждение 7.2: Пусть k – произвольное поле, $I = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$ – идеал. Тогда $f \in \sqrt{I}$ если и только, если $1 \in \tilde{I} := \langle f_1, \dots, f_s, 1 - yf \rangle \subset k[x_1, \dots, x_n, y]$.

Доказательство: Из доказательства теоремы 7.2 следует, что из $1 \in \tilde{I}$ вытекает $f^m \in I$ для некоторого m, а значит и $f \in \sqrt{I}$. Теперь предположим, что $f \in \sqrt{I}$. Некоторая его степень $f^m \in I \subset \tilde{I}$. Поскольку многочлен $1 - yf \in \tilde{I}$, то

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \dots + y^{m-1} f^{m-1})$$

лежит в $\tilde{I}$. ◀

Для того, чтобы выяснить лежит ли f в $\sqrt{\langle f_1, \dots, f_s \rangle}$, нужно найти редуцированный базис Грёбнера идеала $\langle f_1, \dots, f_s, 1 - yf \rangle \subset k[x_1, \dots, x_n, y]$. Если он равен $\{1\}$, то $f \in \sqrt{I}$. В противном случае $f \notin \sqrt{I}$.