# Теорема Гильберта

## Часть 1. Нетеровость

**Определение 1.1.** Модуль $M$ над кольцом $A$ называется нетеровым, если всякая возрастающая цепочка подмодулей $M_1 \subset M_2 \subset M_3 \subset \ldots$ в $M$ стабилизируется, то есть $M_{i+1} = M_i$ для $i \gg 0$.

**Пример 1.2.** Векторное пространство $V$ над полем нетерово $\Longleftrightarrow \dim V < \infty$.

**Определение 1.3.** Модуль $M$ конечно порожден над кольцом $A$, если найдется конечное число элементов $m_1, \ldots, m_n \in M$, такие что всякий элемент из $M$ представляется в виде конечной линейной комбинации элементов $m_i$ с коэффициентами в $A$. Иначе говоря, $M$ изоморфен фактормодулю свободного $A$-модуля конечного ранга.

**Лемма 1.4.** *Модуль $M$ нетеров $\Longleftrightarrow$ любой подмодуль в $M$ конечно порожден.*

Доказательство: ($\Longrightarrow$) Пусть $M$ нетеров и $M' \subset M$. Рассмотрим цепочку подмодулей $0 = M_0 \subset M_2 \subset \ldots$ в $M'$, в которой если $M_i \neq M'$, то $M_{i+1} = M_i + Am_{i+1}$, где $m_{i+1} \in M' \setminus M_i$. Так как цепочка стабилизируется, то $M_i = M'$ при некотором $i$, но тогда $m_1, \ldots, m_i$ порождают $M'$.

($\Longleftarrow$) Пусть $M_1 \subset M_2 \subset \ldots$ — возрастающая цепочка в $M$. Рассмотрим $M' = \bigcup M_i \subset M$. Ясно, что $M'$ — подмодуль. Пусть $m_1, \ldots, m_n$ — его образующие. Тогда для каждого $i$ имеем $m_i \in M_j$ при $j \gg 0$, откуда $M' = M_j$ при $j \gg 0$ и цепочка стабилизируется. □

**Лемма 1.5.** *Если $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ — точная тройка, то $M$ нетеров $\Longleftrightarrow$ $M'$ и $M''$ нетеровы.*

Доказательство: ($\Longrightarrow$) если $M'_1 \subset M'_2 \subset \ldots$ и $M''_1 \subset M''_2 \subset \ldots$ — возрастающие цепочки в $M'$ и $M''$, то $f(M'_1) \subset f(M'_2) \subset \ldots$ и $g^{-1}(M''_1) \subset g^{-1}(M''_2) \subset \ldots$ — возрастающие цепочки в $M$. Следовательно $f(M'_{i+1}) = f(M'_i)$ и $g^{-1}(M''_{i+1}) = g^{-1}(M''_i)$ при $i \gg 0$. Но тогда $M'_{i+1} = M'_i$ и $M''_{i+1} = M''_i$, так как $f$ — моно, а $g$ — эпиморфизм.

($\Longleftarrow$) если $M_1 \subset M_2 \subset \ldots$ — возрастающая цепочка в $M$, то $g(M_1) \subset g(M_2) \subset \ldots$ и $f^{-1}(M_1) \subset f^{-1}(M_2) \subset \ldots$ — возрастающие цепочки в $M''$ и $M'$, поэтому $g(M_{i+1}) = g(M_i)$ и $f^{-1}(M_{i+1}) = f^{-1}(M_i)$ при $i \gg 0$. Но тогда $M_{i+1} = M_i$. Действительно, если $x \in M_{i+1}$, то $g(x) \in g(M_{i+1}) = g(M_i)$, значит найдется $y \in M_i$, так что $g(x) = g(y)$. Тогда $g(x-y) = 0$, значит $x - y \in \operatorname{Ker} g = \operatorname{Im} f$, то есть $x - y \in f(f^{-1}(M_{i+1})) = f(f^{-1}(M_i))$, следовательно найдется $z \in f^{-1}(M_i)$, такой что $x = y + f(z)$. Но $f(z) \in M_i$, значит $x \in M_i$. □

**Следствие 1.6.** *Прямая сумма конечного числа нетеровых модулей нетерова.*

Доказательство: индукция, использующая точные тройки $0 \to M_n \to \oplus_{i=1}^n M_i \to \oplus_{i=1}^{n-1} M_i \to 0$. □

**Определение 1.7.** Кольцо $A$ называется нетеровым, если свободный $A$-модуль $A$ нетеров. Иначе говоря, если всякая возрастающая цепочка идеалов в $A$ стабилизируется.

**Примеры 1.8.**
1. Поле нетерово.
2. Конечное кольцо нетерово.
3. Кольцо главных идеалов нетерово (все идеалы главные $\Longrightarrow$ значит все идеалы конечно порождены).

**Лемма 1.9.** *Факторкольцо нетерова кольца нетерово.*

Доказательство: $A/\mathfrak{a}$ является нетеровым $A$-модулем, а значит и нетеровым $A/\mathfrak{a}$-модулем. □

**Теорема 1.10.** *Модуль $M$ над нетеровым кольцом $A$ нетеров $\Longleftrightarrow$ $M$ конечно порожден.*

Доказательство: ($\Longrightarrow$) Следует из леммы 1.4. ($\Longleftarrow$) Выберем в $M$ образующие, рассмотрим сюръекцию $A^{\oplus n} \to M$ и заметим, что по следствию 1.6 модуль $A^{\oplus n}$ нетеров, а по лемме 1.5 модуль $M$ нетеров. □

**Следствие 1.11.** *Подмодуль и фактормодуль конечно порожденного модуля над нетеровым кольцом конечно порождены.*

## Часть 2. Теорема Гильберта о базисе

Когда-то, нетеровость всякого кольца приходилось проверять по отдельности. Теорема Гильберта позволила избавиться от этого.

**Теорема 2.1.** *Если кольцо $A$ — нетерово, то кольцо $A[x]$ — тоже нетерово.*

Доказательство: пусть $I \subset A[x]$ — идеал. Рассмотрим множество $I_0 \subset A$, состоящее из старших коэффициентов многочленов, входящих в $A$. Ясно, что $I_0$ — идеал в $A$, так как $f(x) = ax^n + \dots \in I$, $g(x) = bx^m + \dots \in I \Longrightarrow f(x)x^m + g(x)x^n = (a+b)x^{n+m} + \dots \in I$, $cf(x) = cax^n + \dots \in I \Longrightarrow a + b \in I_0$, $ca \in I_0$ для всех $c \in A$. Идеал $I_0$ конечно порожден над $A$. Выберем конечный набор образующих $a_1, \dots, a_n$ идеала $I_0$ над $A$ и пусть $f_1, \dots, f_n \in A[x]$ — многочлены из $I$, старшие коэффициенты которых равны $a_1, \dots, a_n$. Пусть $N = \max \deg f_i$ Пусть далее $M = I \cap A\langle 1, x, \dots, x^{N-1}\rangle \subset A[x]$. Тогда $M$ является $A$-подмодулем в свободном $A$-модуле конечного ранга, значит $M$ конечно порожден над $A$. Выберем конечный набор образующих $g_1, \dots, g_m$ модуля $M$ над $A$ и докажем, что многочлены $f_1, \dots, f_n, g_1, \dots, g_m$ порождают идеал $I$ над $A[x]$. Для этого надо любой многочлен $h(x) \in I$ представить в виде линейной комбинации многочленов $f_i$, $g_j$. Действительно, если $\deg h < N$, то $h \in M$ и представляется в виде линейной комбинации многочленов $g_j$. Пусть теперь $\deg h > N$, $h = ax^k + \dots$. Тогда $a \in I_0$, значит $a = \sum c_i a_i$, $c_i \in A$, следовательно если $h'(x) = h(x) - \sum c_i x^{k - \deg f_i} f_i$, то $h'(x) \in I$, причем $\deg h' < \deg h$. Повторяя это рассуждение заключаем, что $h$ представляется в виде линейной комбинации многочленов $f_i$ и многочлена, лежащего в $I$, степень которого меньше чем $N$. $\square$

**Следствие 2.2.** *Кольцо многочленов $\mathsf{k}[x_1, \dots, x_n]$ нетерово.*

**Следствие 2.3.** *Любая конечно порожденная коммутативная $\mathsf{k}$-алгебра нетерова.*

**Следствие 2.4.** *Если $A$ нетерово, то любая конечно порожденная коммутативная $A$-алгебра нетерова.*

**Следствие 2.5.** *Любой идеал в конечно порожденной коммутативной $\mathsf{k}$-алгебре конечно порожден.*

## Часть 3. Теорема Гильберта о нулях

**Теорема 3.1.** *Если $X \subset \mathbb{A}^n$ — аффинное алгебраическое многообразие над алгебраически замкнутым полем $\mathsf{k}$, $\mathfrak{a} \subset A_X$ — идеал в его координатной алгебре, то $I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a})$.*

Покажем, что условие алгебраической замкнутости поля $\mathsf{k}$ в формулировке теоремы существенно. Рассмотрим идеал $\mathfrak{a} := (x^2+1)\mathbb{R}[x] \subset \mathbb{R}[x]$. Тогда $V(\mathfrak{a}) \subset \mathbb{R}$ задается уравнением $x^2 + 1 = 0$, которое не имеет вещественных решений. Поэтому $V(\mathfrak{a}) = \emptyset$ и $I_{V(\mathfrak{a})} = \mathbb{R}[x] \ne \mathfrak{r}(\mathfrak{a})$. Причина в том, что $V(\mathfrak{a})$ не имеет вещественных точек, но имеет две комплексные точки $i$ и $-i$, поэтому при переходе к полю $\mathbb{C}$ получаем $V(\mathfrak{a}) = \{\, i, -i \,\}$ и $I_{V(\mathfrak{a})} = \{\, f(x) \in \mathbb{C}[x] \mid (x-i) | f(x), (x+i) | f(x) \,\} = \{\, f(x) \in \mathbb{C}[x] \mid (x^2+1) | f(x) \,\} = \mathfrak{a}$. Разобранный факт является иллюстрацией следующего принципа:

> *алгебраическое многообразие над незамкнутым полем $\mathsf{k}$ следует рассматривать как множество точек соответствующего многообразия над $\bar{\mathsf{k}}$, имеющих координаты в $\mathsf{k}$.*

Тот же пример показывает, что в формулировке “слабой формы” теоремы Гильберта о нулях, утверждающей что всякий максимальный идеал в алгебре $A_X$ функций на многообразии $X$ имеет вид $I_x$, где $x \in X$, существенно условие алгебраической замкнутости поля. А именно, идеал $\mathfrak{a}$ рассмотренный выше максимален ($\mathbb{R}[x]/\mathfrak{a} \cong \mathbb{C}$), однако, чтобы его представить в виде $I_x$, надо в качестве точки $x$ взять точку с комплексными координатами.

Прежде чем приступить к доказательству теоремы Гильберта, нам потребуются приготовления.

**Лемма 3.2.** *Если $A \subset B \subset C$ и $B$ — конечно порожденная $A$-алгебра, а $C$ — конечно порожденная $B$-алгебра, то $C$ — конечно порожденная $A$-алгебра.*

Доказательство: если $b_1, \dots, b_n$ порождают $B$ над $A$, а $c_1, \dots, c_m$ порождают $C$ над $B$, то $b_1, \dots, b_n, c_1, \dots, c_m$ порождают $C$ над $A$. $\square$

**Лемма 3.3.** *Поле $K = \mathsf{k}(x_1, \ldots, x_m)$ является конечно порожденной $\mathsf{k}$-алгеброй только при $m = 0$.*

Доказательство: предположим, что $\phi_1, \ldots, \phi_n$ порождают $K$ над $\mathsf{k}$, $\phi_i = f_i/g_i$. Выберем неприводимый многочлен $p \in \mathsf{k}[x_1, \ldots, x_m]$, не являющийся делителем ни одного из многочленов $g_i$ (неприводимых делителей у многочленов $g_i$ лишь конечное число в силу факториальности кольца $\mathsf{k}[x_1, \ldots, x_m]$, а различных неприводимых — бесконечное (для любого множества $p_1, \ldots, p_N$ неприводимых многочленов всякий неприводимый делитель многочлена $p_1 \cdots p_N + 1$ взаимно прост с каждым из $p_i$)). Тогда $1/p$ не лежит в подкольце поля $K$, порожденном над $\mathsf{k}$ элементами $\phi_i$. $\square$

**Определение 3.4.** Набор элементов $a_1, \ldots, a_n$ в коммутативной $\mathsf{k}$-алгебре $A$ называется **алгебраически независимым** над $\mathsf{k}$, если для любого многочлена $0 \neq f(x_1, \ldots, x_n) \in \mathsf{k}[x_1, \ldots, x_n]$ имеем $f(a_1, \ldots, a_n) \neq 0$.

**Лемма 3.5.** *Если конечно порожденная коммутативная $\mathsf{k}$-алгебра $A$ является полем, то $A/\mathsf{k}$ — конечное расширение полей.*

Доказательство: выберем конечный набор образующих $a_1, \ldots, a_n$ алгебры $A$ над $\mathsf{k}$. Можно считать, что образующие перенумерованы таким образом, что $a_1, \ldots, a_m$ алгебраически независимы над $\mathsf{k}$, а $a_1, \ldots, a_m, a_i$ при $m < i \leqslant n$ уже алгебраически зависимы. Далее, гомоморфизм $\mathsf{k}[x_1, \ldots, x_m] \to A$, $x_i \mapsto a_i$ является вложением, значит индуцирует изоморфизм поля $\mathsf{k}(x_1, \ldots, x_m)$ и подполя $K \subset A$, порожденного элементами $a_1, \ldots, a_m$. При этом все $a_i$ при $m < i \leqslant n$ алгебраичны над $K$, следовательно $A$ алгебраично над $K$, следовательно $\dim_K A < \infty$. Пусть $e_1, \ldots, e_l$ — базис $A$ над $K$. Тогда для всех $1 \leqslant i, j \leqslant n$ имеем

$$a_i = \sum_{k=1}^{l} \lambda_{ik} e_k, \qquad e_i e_j = \sum_{k=1}^{l} \mu_{ijk} e_k, \qquad \lambda_{ik}, \mu_{ijk} \in K.$$

Пусть $B \subset A$ — алгебра, порожденная над $\mathsf{k}$ элементами $\lambda_{ik}, \mu_{ijk}$. Тогда $B$ — нетерова. Из предыдущих равенств следует, что элементы $e_1, \ldots, e_l$ порождают $A$ как $B$-модуль, то есть $A$ конечно порожденный $B$-модуль, следовательно $K$ — тоже конечно порожденный $B$-модуль, так как $K \subset A$, следовательно $K$ — конечно порожденная $B$-алгебра, следовательно $K$ — конечно порожденная $\mathsf{k}$-алгебра. Но $K \cong \mathsf{k}(x_1, \ldots, x_m)$, следовательно $m = 0$, $K = \mathsf{k}$ и $\dim_{\mathsf{k}} A < \infty$. $\square$

**Следствие 3.6.** *Если $\mathfrak{m}$ — максимальный идеал в конечно порожденной коммутативной $\mathsf{k}$-алгебре $A$, то поле $A/\mathfrak{m}$ является конечным расширением поля $\mathsf{k}$.*

Если $A = A_X$, $X \subset \mathbb{A}^n$, $x_1, \ldots, x_n$ — координаты в $\mathbb{A}^n$, $A/\mathfrak{m} = F$ и $\pi : A \to F$ — соответствующий эпиморфизм, и $\lambda_i := \pi(x_i) \in F$, то $\mathfrak{m} = \{ f \in \mathsf{k}[x_1, \ldots, x_n] \mid f(\lambda_1, \ldots, \lambda_n) = 0 \} = I_{(\lambda_1, \ldots, \lambda_n)}$. Иначе говоря, максимальный идеал $\mathfrak{m}$ соответствует точке многообразия $X$ с координатами в расширении $F$ поля $\mathsf{k}$.

Теперь можно приступить к доказательству теоремы Гильберта.

Шаг 1. Предположим, что теорема доказана для простых идеалов. Тогда для любого $\mathfrak{a}$, если $\mathfrak{a} \subset \mathfrak{p}$, то $V(\mathfrak{p}) \subset V(\mathfrak{a})$, значит $I_{V(\mathfrak{a})} \subset I_{V(\mathfrak{p})} = \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$, следовательно $I_{V(\mathfrak{a})} \subset \bigcup_{\mathfrak{a} \subset \mathfrak{p}} \mathfrak{p} = \mathfrak{r}(\mathfrak{a})$.

Шаг 2. Предположим, что $f \in I_{V(\mathfrak{p})}$, $f \notin \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$. Рассмотрим подкольцо в поле частных целостного кольца $A/\mathfrak{p}$, порожденное элементом $1/f$: $B = A/\mathfrak{p}[1/f]$. Так как $f \neq 0$ в $A/\mathfrak{p}$, то $B \neq 0$. Выберем максимальный идеал $\mathfrak{m}$ в кольце $B$. Кольцо $B$ конечно порождено над $A$, поэтому $B$ конечно порождено над $\mathsf{k}$, поэтому $B/\mathfrak{m}$ является конечно порожденной $\mathsf{k}$-алгеброй. Следовательно, поле $B/\mathfrak{m}$ является конечным расширением поля $\mathsf{k}$. Но $\mathsf{k}$ алгебраически замкнуто, поэтому $B/\mathfrak{m} \cong \mathsf{k}$. Пусть $\pi : B \to \mathsf{k}$ — соответствующий эпиморфизм, а $\rho$ — композиция $A \to A/\mathfrak{p} \to A/\mathfrak{p}[1/f] = B \to \mathsf{k}$. Ясно, что $\mathfrak{p} \subset \operatorname{Ker} \rho$. Пусть также $\lambda_i = \rho(x_i) \in \mathsf{k}$, где $x_1, \ldots, x_n$ — координаты в аффинном пространстве, в котором лежит $X$. Тогда если $\lambda = (\lambda_1, \ldots, \lambda_n)$, то эпиморфизм $\rho$ совпадает с эпиморфизмом $A \to A/I_\lambda \cong \mathsf{k}$

$$\begin{tikzcd}
A \arrow[r] \arrow[d] \arrow[rrd, "\rho"] & A/\mathfrak{p} \arrow[r] & B \arrow[d, "\pi"] \\
A/I_\lambda \arrow[rr, equal] & & \mathsf{k}
\end{tikzcd}$$

(эпиморфизм однозначно определяется значениями на образующих кольца), поэтому $\mathfrak{p} \subset I_\lambda$, следовательно $\lambda \in V(I_\lambda) \subset V(\mathfrak{p})$. Однако, $\pi(1/f) = 1/f(\lambda_1, \ldots, \lambda_n)$, поэтому $f(\lambda_1, \ldots, \lambda_n) \neq 0$, значит $f \notin I_{V(\mathfrak{p})}$. $\square$