Лекция 1

1.1 Многочлены и аффинное пространство

Пусть k – поле (важнейшими примерами для нас будут $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$).

Определение 1.1: **Многочленом** f от $x_1,\dots,x_n$ с коэффициентами в k будем называть конечную линейную комбинацию

(1.1) $$f = \sum_{\alpha} a_\alpha x^\alpha$$

мономов $x^\alpha := x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}$, где наборы $\alpha := (\alpha_1,\dots,\alpha_n)$ пробегают некоторое конечное подмножество в $(\mathbb{Z}_{\geq 0})^n$, а коэффициенты $a_\alpha \in k$. Множество всех таких многочленов будем обозначать $k[x_1,\dots,x_n]$.

Определение 1.2: Число $|\alpha| := \alpha_1+\ldots+\alpha_n$ условимся называть **полной** или **суммарной степенью** монома x^α. Для многочлена (1.1) его **полной** или **суммарной степенью** будем называть число

$$\deg f := \max\{|\alpha| : a_\alpha \neq 0\}.$$

Напомним, что **кольцом** R называется абелева группа с операцией $(a,b)\mapsto ab$ („умножением“), т.ч. для всех $a,b,c\in R$ выполняются условия:

(ассоц-ть) $a(bc) = (ab)c$

(дистр-ть) $a(b+c) = ab+ac$

$(b+c)a = ba+ca$

(единица) $\exists 1\in R$, т.ч. $1a = a1 = a$.

Кольцо R **коммутативно**, если выполняется св-во

(ком-ть) $ab = ba$ для всех $a,b\in R$.

Нетрудно проверить, что множество $k[x_1,\dots,x_n]$ является коммутативным кольцом относительно операций сложения и умножения, введённых естественным образом. Поэтому мы будем называть $k[x_1,\dots,x_n]$ **кольцом многочленов** от n переменных.

Определение 1.3: Мы будем называть **n-мерным аффинным пространством над полем k** множество
$$k^n := \{(a_1,\dots,a_n) : a_1,\dots,a_n \in k\}.$$

Многочлен $f \in k[x_1,\dots,x_n]$ определяет k-значную функцию $f: k^n \to k$ на аффинном пространстве: $f(a_1,\dots,a_n) := \sum_\alpha a_\alpha \cdot a_1^{\alpha_1} \cdot \ldots \cdot a_n^{\alpha_n} \in k$. Однако различные многочлены могут определять одну и ту же функцию (например, ненулевому многочлену $x^2 - x \in \mathbb{F}_2[x]$ также как и нулевому многочлену из $\mathbb{F}_2[x]$ соответствует тождественно равная нулю на $(\mathbb{F}_2)^2$ функция). К счастью, для бесконечных полей этой неоднозначности не возникает.

Предложение 1.1: Пусть k — бесконечное поле, $f \in k[x_1,\dots,x_n]$. Тогда
$f = 0$ в $k[x_1,\dots,x_n]$ (все коэффициенты f равны нулю) $\Leftrightarrow$
$f: k^n \to k$ — функция тождественно равная нулю на k^n
($f(a_1,\dots,a_n) = 0$ для всех наборов $(a_1,\dots,a_n) \in k^n$).

Доказательство: Необходимость очевидна.
Достаточность будем доказывать индукцией по n. Пусть $n=1$.
Хорошо известно, что многочлен $f \in k[x]$ степени m имеет не более m корней. Поэтому, если $f \in k[x]$ такой, что $f(a) = 0$ для всех $a \in k$, то в силу бесконечности поля k многочлен f имеет бесконечно много корней. Следовательно, f — нулевой многочлен.

Предположим, что утверждение верно для многочленов над бесконечным полем k от $n-1$ переменной. Пусть $f \in k[x_1,\dots,x_n]$, т.ч. $f(a) = 0$ для всех $a \in k^n$. Мы можем переписать f в виде $f = \sum_{i=0}^{N} g_i(x_1,\dots,x_{n-1})\, x_n^i$, где коэффициенты $g_i(x_1,\dots,x_{n-1}) \in k[x_1,\dots,x_{n-1}]$. Зафиксировав точку $(a_1,\dots,a_{n-1}) \in k^{n-1}$, мы получим многочлен $f(a_1,\dots,a_{n-1},x_n)$ из $k[x_n]$. По предположению он зануляется во всех точках $a_n \in k$, поэтому является нулевым многочленом в $k[x_n]$, т.е. все коэффициенты $g_i(a_1,\dots,a_{n-1}) = 0$.
В силу произвольности выбора $(a_1,\dots,a_{n-1}) \in k^{n-1}$, каждый $g_i \in k[x_1,\dots,x_{n-1}]$ задаёт нулевую функцию на k^{n-1}. Тогда по предположению индукции каждый g_i является нулевым многочленом в кольце $k[x_1,\dots,x_{n-1}]$. Поэтому f тоже является нулевым многочленом в кольце $k[x_1,\dots,x_n]$. ◀

Следствие 1: Пусть k - бесконечное поле, многочлены $f, g \in k[x_1, \dots, x_n]$. Тогда $f = g$ в $k[x_1, \dots, x_n]$ $\Leftrightarrow$ функции $f: k^n \to k$ и $g: k^n \to k$ совпадают.

1.2 Аффинные многообразия

Определение 1.4: Пусть k - поле, многочлены $f_1, \dots, f_s \in k[x_1, \dots, x_n]$
Множество вида

(1.2) $$\mathbb{V}(f_1, \dots, f_s) := \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0, \ i = \overline{1, s}\}$$

называется **аффинным многообразием**.

Предложение 1.2: Пусть $V, W \subset k^n$ - аффинные многообразия. Тогда пересечение $V \cap W$ и объединение $V \cup W$ тоже являются аффинными многообразиями в k^n.

Доказательство: Запишем $V = \mathbb{V}(f_1, \dots, f_s)$ и $W = \mathbb{V}(g_1, \dots, g_t)$. Докажем, что

$$V \cap W = \mathbb{V}(f_1, \dots, f_s, g_1, \dots, g_t),$$
$$V \cup W = \mathbb{V}(f_i g_j : 1 \le i \le s, \ 1 \le j \le t).$$

Первое равенство очевидно, поскольку точка $(a_1, \dots, a_n) \in V \cap W$ тогда и только тогда, когда все $f_i(a_1, \dots, a_n) = 0$ и $g_j(a_1, \dots, a_n) = 0$.

Обратимся к доказательству второго равенства. В точке $(a_1, \dots, a_n) \in V$ все f_i-ые равны нулю, поэтому все произведения $f_i g_j$ тоже зануляются в этой точке, и справедливо включение $V \subset \mathbb{V}(f_i g_j)$. Включение $W \subset \mathbb{V}(f_i g_j)$ доказывается аналогично. Итак, мы показали, что $V \cup W \subset \mathbb{V}(f_i g_j)$. Пусть теперь $(a_1, \dots, a_n) \in \mathbb{V}(f_i g_j)$. Либо эта точка лежит в V, либо найдётся i_0, т.ч. $f_{i_0}(a_1, \dots, a_n) \neq 0$.
Во втором случае, поскольку все $f_{i_0} g_j$-ые должны зануляться, многочлены g_j обращаются в нуль для все $j = \overline{1, t}$, т.е. $(a_1, \dots, a_n) \in W$. Таким образом $\mathbb{V}(f_i g_j) \subset V \cup W$. ◀

В нашем курсе мы научимся отвечать для заданного набора многочленов $\{f_1, \dots, f_s\} \subset k[x_1, \dots, x_n]$ на следующие три вопроса:

1) Пусто ли $\mathbb{V}(f_1, \dots, f_s)$? То есть совместна ли система $f_1 = \dots = f_s = 0$?
2) Конечно ли $\mathbb{V}(f_1, \dots, f_s)$? Если да, то как получить все решения системы?
3) Как определить „размерность“ $\mathbb{V}(f_1, \dots, f_s)$?

1.3 Идеалы

Напомним, что **идеал в коммутативном кольце** R — аддитивная подгруппа I такая, что выполняется условие:

(замк-ть) для всех $r \in R$ и всех $q \in I$ произведение $rq \in I$.

Например, множество

(1.3) $$\langle f_1, \dots, f_s \rangle := \{h_1 f_1 + \dots + h_s f_s : h_i \in k[x_1, \dots, x_n], i = \overline{1, s}\},$$

соответствующее набору многочленов $\{f_1, \dots, f_s\} \subset k[x_1, \dots, x_n]$, очевидным образом является идеалом в кольце многочленов $k[x_1, \dots, x_n]$. Этот идеал состоит из всевозможных „полиномиальных следствий“ алгебраической системы $f_1 = \dots = f_s = 0$.

Определение 1.5: Идеал I в $k[x_1, \dots, x_n]$ называется **конечно-порождённым**, если существует набор $\{f_1, \dots, f_s\} \subset k[x_1, \dots, x_n]$ такой, что
$$I = \langle f_1, \dots, f_s \rangle.$$
Сам набор $\{f_1, \dots, f_s\}$ называется **базисом идеала** I.

Вскоре мы докажем, что любой идеал в $k[x_1, \dots, x_n]$ является конечно-порождённым (теорема Гильберта о базисе).

Определение 1.6: Пусть $V \subset k^n$ — аффинное многообразие. Тогда множество

(1.4) $$\mathbb{I}(V) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ для всех } (a_1, \dots, a_n) \in V\}$$

называется **идеалом аффинного многообразия** V.

Множество $\mathbb{I}(V)$ действительно является идеалом в $k[x_1, \dots, x_n]$!

Пример 1.1: Идеал $\mathbb{I}(\{(0,0)\}) = \langle x, y\rangle$. С одной стороны, произвольный многочлен $A(x,y)x + B(x,y)y \in \langle x,y\rangle$ зануляется в точке $(0,0)$. С другой, если многочлен $f = \sum_{i,j} a_{ij} x^i y^j$ зануляется в точке $(0,0)$, то свободный коэффициент $a_{00} = 0$, но тогда мы можем записать его в виде

$$f = \left(\sum_{i>0} a_{ij} x^{i-1} y^j\right) x + \left(\sum_{j>0} a_{0j} y^{j-1}\right) y \in \langle x, y\rangle.$$

Рассмотрим цепочку соответствий:

$$\{f_1, \dots, f_s\} \longrightarrow \mathbb{V}(f_1, \dots, f_s) \longrightarrow \mathbb{I}(\mathbb{V}(f_1, \dots, f_s)).$$

Всегда ли $\mathbb{I}(\mathbb{V}(f_1, \dots, f_s)) = \langle f_1, \dots, f_s\rangle$? Ответ: нет, например,

$$\mathbb{I}(\mathbb{V}(x^2, y^2)) = \langle x, y\rangle \neq \langle x^2, y^2\rangle.$$

Предложение 1.3: Если $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, то $\langle f_1, \dots, f_s\rangle \subset \mathbb{I}(\mathbb{V}(f_1, \dots, f_s))$.

Доказательство: Пусть $f \in \langle f_1, \dots, f_s\rangle$. Существуют многочлены $h_1, \dots, h_s \in k[x_1, \dots, x_n]$ такие, что $f = h_1 f_1 + \dots + h_s f_s$. Поскольку все f_i-ые зануляются в точках $\mathbb{V}(f_1, \dots, f_s)$, то f тоже зануляется в таких точках, а это означает, что $f \in \mathbb{I}(\mathbb{V}(f_1, \dots, f_s))$.

Предложение 1.4: Пусть $V, W \subset k^n$ – аффинные многообразия. Тогда

1) $V \subset W \Leftrightarrow \mathbb{I}(V) \supset \mathbb{I}(W)$.
2) $V = W \Leftrightarrow \mathbb{I}(V) = \mathbb{I}(W)$.

Доказательство: Утверждение 2) сразу следует из 1).
Докажем 1). Пусть $V \subset W$. В этом случае любой многочлен, обращающийся в ноль на W, должен обращаться в ноль на V, т.е. $\mathbb{I}(W) \subset \mathbb{I}(V)$.
Пусть $\mathbb{I}(W) \subset \mathbb{I}(V)$. Запишем $W = \mathbb{V}(g_1, \dots, g_t)$, где $g_j \in k[x_1, \dots, x_n]$.
Тогда $g_1, \dots, g_t \in \mathbb{I}(W) \subset \mathbb{I}(V)$, т.е. g_j-ые зануляются в точках V, поэтому $W \supset V$.

В завершение поставим вопросы об идеалах в $k[x_1, \dots, x_n]$, которые мы вскоре разрешим:

1) Всякий ли идеал I в $k[x_1, \dots, x_n]$ может быть представлен в виде $\langle f_1, \dots, f_s\rangle$ для некоторых $f_1, \dots, f_s \in k[x_1, \dots, x_n]$?
2) Существует ли алгоритм, определяющий лежит ли многочлен $f \in k[x_1, \dots, x_n]$ в идеале $\langle f_1, \dots, f_s\rangle$? (проблема принадлежности идеалу)
3) Каково точное соотношение между идеалами $\langle f_1, \dots, f_s\rangle$ и $\mathbb{I}(\mathbb{V}(f_1, \dots, f_s))$?