Алгебра 12

Igor Engel

1

Определение 1.1. R - кольцо, $I \subset R$, I называется идеалом R, если

1. $u, v \in I \implies u + v \in I$
2. $u \in I$, $r \in R$, $ru \in I$
3. $0 \in I$

Лемма 1.1.1. Если I - идеал в R, то I - подгруппа аддитивной группы R.

Доказательство. Замкнутость и наличие нетрального гарантируется свойствами.
Заметим, что $-1 \in R$, тогда $\forall u \in I \quad -1 \cdot u = -u \in I$. □

Определение 1.2. Идеал, порождённый элементами $a_1, \ldots, a_n$:

$$I = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \mid \forall i \quad x_i \in R\}.$$

Определение 1.3. Главный идеал - идеал, порождённый одним элементом.

$$dR = \{dx \mid x \in R\}.$$

Теорема 1.1. K - поле, тогда $\forall I \leq K[x] \quad \exists d \in K[x] \quad I = dK[x]$.

Доказательство. Если $I = \{0\}$, то $I = 0K[x]$.
Пусть $I \neq \{0\}$: Рассмотрим ненулевой многочлен $d \in I$, $\deg d$ - минимальна.
Покажем, что $I = dK[x]$.
Рассмотрим $a \in I$, тогда $a = dq + r$, $\deg r < \deg d$.
$dq \in I$, $a - dq = r$, $r \in I$, $\deg r < \deg d \implies r = 0$, $a \in dK[x]$, $I \subset dK[x]$.
По второму свойству, $dK[x] \subset I$, значит $I = dK[x]$ □

Лемма 1.1.1. K - поле, $f, g \in K[x]$. Тогда $\exists (f, g) \quad$, и $(f, g)K[x] = \langle f, g \rangle$.

Доказательство. Пусть $\langle f, g \rangle = dK[x]$.
Заметим, что $f, g \in dK[x]$, значит $f \vdots d$ и $g \vdots d$.
Возьмём произвольный общий делитель f, g назовём d'.

$$d = fu + gv.$$

$fu \vdots d'$, $gv \vdots d'$, знаит $d \vdots d'$. □

Лемма 1.3.1. Пусть $p \in K[x]$.
p прост только тогда, когда неприводим.

Доказательство. Рассмотрим (a, p).
Есть два случая: $(a, p) \in K[x]^*$, $(a, p) \equiv p$.
Разберём второй случай:

$$(a, p) \vdots p.$$

Но $a \vdots (a, p)$, значит $a \vdots p$.
Рассмотрим первый случай: НОД определённ с точностью до ассоциированности, значит можно считать что $(a, p) = 1$.
Тогда $1 = ax + py$ □

Теорема 1.2.

$$\forall f \in K[x] \quad \exists p_1, \ldots, p_n \quad \in K[x] \exists \varepsilon \in K^* \quad \varepsilon \prod_{i=1}^{n} p_i.$$

Это разложение единственно, с точностью до порядка и ассоцированности.

Доказательство. Если f неприводим, то, $n = 1$ $p_1 = f$.
Если f обратим, то $n = 0$, $\varepsilon = f$.
Иначе существует разложение $f = gh$, степени g, h меньше степени f, раскладываем по индукции.
Докажем единственность:

$$\varepsilon_1 \prod_{i=1}^{n} p_i = \varepsilon_2 \prod_{i=1}^{n} q_i.$$

Левая часть делится на p_1, значит, правая часть делится на p_1, значит какое-то q_i ассоциированно с p_1, делим, переходим по индукции. □

Лемма 1.2.1. R - кольцо, $f \in R[x]$, $f \vdots (x - a) \iff f(a) = 0$.

Доказательство. □

Определение 1.4. R - область целостности. Тогда $a \in R$ является корнем $f \in R[x]$ кратнсоти $k \geq 1$, если $f \vdots (x - a)^k$ и $f \not\vdots (x - a)^{k+1}$.

Теорема 1.3. K - поле, $f \in K[x]$, тогда кол-во корней f с учётом кратности не больше степени f.

Доказательство. Перечислим все корни $\lambda_1, \ldots, \lambda_s$ и их кратность $r_1, \ldots, r_s$.
Тогда кол-во корней - $\sum_{i=1}^{s} r_i$.
Заметим, что многочлен $x - \lambda_i$ неприводим.

Заметим, что $(x-\lambda_i) \not\sim (x-\lambda_j)$.
Разложим f на множители:

$$f = \varepsilon(x-\lambda_1)^{r_1} \dots (x-\lambda_s)^{r_s} g.$$

$$\deg f = r_1 + \dots + r_s + \deg g.$$

$$\deg g \geq 0. \qquad \square$$

Лемма 1.3.1. $f, g \in K[x]$, $\deg f, \deg g \leq n$, и есть попарно различные $\lambda_0, \dots, \lambda_n$, такие, что $\forall i \quad f(\lambda_i) = g(\lambda_i)$, тогда $f = g$.

Доказательство. Рассмотрим $h = f - g$.
Тогда λ_i - корни. Но тогда у h есть $n+1$ корень, значит $h(x) = 0$. $\square$

Теорема 1.4 (Теорема о формальном и функциональном равенстве многочленов)**.** $f, g \in K[x]$, K - бесконечное, если $\forall \lambda \in K \quad f(\lambda) = g(\lambda)$, то $f = g$.

Доказательство. Пусть $n = \max(\deg f, \deg g)$.
Выберем $n+1$ точку из K. По предыдущей лемме, многочлены равны. $\square$

Теорема 1.5 (Теорема Вильсона)**.** $p \in \mathbb{Z}$ - простое, тогда и только тогда, когда $(p-1)! \equiv -1 \mod p$.

Доказательство. $\square$