Оглавление

Глава 1

Кольца и поля

1.1. Присоединение корней многочлена

Этот параграф более-менее по ван дер Вардену.

Теорема 1 (существование простого расширения). K — поле, $P(x) \in K[x]$ — неприводимый. Тогда существует расширение поля K такое, что $P(x)$ имеет в L корень α и $L = K(\alpha)$.

Доказательство. Рассмотрим множество формальных сумм вида

$$a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n, \quad a_i \in K$$

Введём отношение эквивалентности:
Если

$$s = a_0 + a_1 X + \dots, \qquad t = b_0 + b_1 X + \dots$$
$$S(x) \coloneqq a_0 + a_1 x + \dots, \qquad T(x) \coloneqq b_0 + b_1 x + \dots$$

и $S(x) - T(x) \,\vdots\, P(x)$, то $s \sim t$.
Определим на множестве классов элквивалентности сложение и умножение:
Если

$$s = a_0 + a_1 X + \dots, \qquad t = b_0 + b_1 X + \dots, \qquad u = c_0 + c_1 X + \dots$$
$$S(x) = a_0 + a_1 x + \dots, \qquad T(x) = b_0 + b_1 x + \dots, \qquad U(x) = c_0 + c_1 x + \dots$$

и $S(x)T(x) - U(x) \,\vdots\, P(x)$, то положим $u \coloneqq st$.
Сложение — аналогично.
Получается поле, изоморфное $K[x] / \langle P(x) \rangle$
Изоморфизм: $\overline{a_0 + a_1 X + \dots} \mapsto \overline{a_0 + a_1 x + \dots}$
$\overline{X}$ подойдёт в качестве α (т. к. $P(x) \mapsto \overline{P(x)} = 0$). □

Пример. $K = \mathbb{Z}_3$
$p(x) = x^3 + 2x + 1$ — неприводимый над $\mathbb{Z}_3$
α — корень. Существует поле $K(\alpha)$.
Теперь знаем, что $K(\alpha)$ алгебраическое над K, $\quad |K(\alpha) : K| = 3$
Элементы имеют вид $a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Z}_3$
Знаем, что $\alpha^3 + 2\alpha + 1 = 0$
Пример умножения.

$$a = 1 + 2\alpha + \alpha^2, \qquad b = 2 + \alpha + \alpha^2$$

$$ab = (1 + 2\alpha + \alpha^2)(2 + \alpha + \alpha^2) = 2 + (1+1)\alpha + (2+2+1)\alpha^2 + (2+1)\alpha^3 + \alpha^4 \underset{3}{\equiv} 2 + 2\alpha + \alpha^2 + \alpha^4$$

Поделим $x^4 + x^2 + 2x + 2$ на $x^3 + 2x + 1$:

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$ab = (\underbrace{\alpha^3 + \alpha + 2}_{0}) \cdot \alpha + 2 = 2$$

Пример деления.

$$\frac{1}{\alpha^2+1}$$

x^2+1 и $P(x)$ взаимно просты. Значит есть линейное представление НОД:

$$(x+2)P(x)+(2x^2+x+2)(x^2+1)=1$$

Подставим $x=\alpha$:

$$(\alpha+2)\cdot 0+(2\alpha+\alpha+2)(\alpha^2+1)=1 \qquad \Longrightarrow \qquad \frac{1}{\alpha^2+1}=2\alpha^2+\alpha+2$$

Определение 1. Расширения L_1, L_2 поля K называются эквивалентными (относительно K), если $L_1 \simeq L_2$ и существует изоморфизм $f: L_1 \to L_2$ такой, что $f\Big|_K = \mathrm{id}$.

Теорема 2 (эквивалентные простые расширения). α, β — алгебраические над K, их минимальные многочлены совпадают.
Тогда $K(\alpha)$ и $K(\beta)$ эквивалентны K, причём существует изоморфизм $f: K(\alpha) \to K(\beta)$ такой, что

$$f\Big|_K = \mathrm{id}, \quad (\alpha) = f(\beta)$$

Доказательство. Пусть $P(x)$ — минимальный многочлен для α и β, $\quad n := \deg P$.
Элементы $K(\alpha)$ — это $u_0+u_1\alpha+\dots+u_{n-1}\alpha^{n-1}$.
Положим

$$f(u_0+u_1\alpha+\dots+u_{n-1}\alpha^{n-1}) := u_0+u_1\beta+\dots+u_{n-1}\beta^{n-1}$$

Пусть

$$s=u_0+u_1\alpha+\dots, \qquad t=v_0+v_1\alpha+\dots$$

$$S(x)=u_0+u_1x+\dots, \qquad T(x)=v_0+v_1x+\dots$$

Пусть $R(x)=w_0+w_1x+\dots+w_{n-1}x^{n-1}$ — такой, что $S(x)T(x)-R(x) \vdots P(x)$

$$r=w_0+w_1\alpha+\dots+w_{n-1}\alpha^{n-1}$$

Тогда $s=S(\alpha), \quad t=T(\alpha), \quad r=R(\alpha)$

$$f(s)=S(\beta), \qquad f(t)=T(\beta), \qquad f(r)=R(\beta)$$

$$st=S(\alpha)T(\alpha) \underset{ST-R \vdots P}{=\!=\!=\!=} R(\alpha)=r^2$$

$$f(ST)=f(r)=R(\beta)$$

$$f(s)f(t)=S(\beta)T(\beta)=R(\beta)$$

Сложение — аналогично.
Биективность:

- Инъективность:

$$u_0+u_1\alpha+\dots \to 0$$

$$u_0+u_1\beta+\dots=0$$

$$\Longrightarrow u_i=0$$

- Сюръективность:
  Любой элемент $K(\beta)$ — это $u_0+u_1\beta+\dots$

$\square$

Примеры.

1. $\mathbb{Q}, \quad P(x)=x^3-2$

Корни $P(x)$:

$$\alpha = \sqrt[3]{2}, \qquad \left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}, \qquad \gamma = \left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}$$

$$L_1 = K(\alpha), \qquad L_2 = K(\beta)$$

$$a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \quad \mapsto \quad a + b\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\sqrt[3]{2} + c\left(\dots\right)^2, \qquad a,b,c \in \mathbb{Q}$$

Это — изоморфизм $L_1 \to L_2$
Аналогично, $K(\beta) \to K(\gamma)$ — сужение комплексного сопряжения.

2. $\mathbb{Q}$, $\quad P(x) = x^2 - 2$

$$\alpha = \sqrt{2}, \qquad \beta = -\sqrt{2}$$

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$$

По теореме, существует изоморфизм $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ такой, что $f\Big|_Q = \mathrm{id}, \quad f(\sqrt{2}) = -\sqrt{2}$