Оглавление

Глава 1

Кольца и поля

1.1. Алшебраические расширения

Определение 1. L — расширение K, $\quad \alpha \in L$
α называется алгебраическим над K, сели $\exists\, P(x) \in K[x]$ такой, что $P(\alpha) = 0$, $\quad P(x)$ — не нулевой.
Если такого $P(x)$ не существует, то α называется трансцендентным.

Определение 2. α — алгебраическое над K, $\quad P(x) \in K[x]$, $\quad P(\alpha) = 0$.
Тогда

- $P(x)$ — алгебраический над α
- $P(x)$ аннулирует α

Минимальным многочленом α над K называется ненулевой аннулирующий многочлен наименьшей степени со старшим коэффициентом, равным 1

Определение 3. Алгебраическим числом называется комплексное число, алгебраическое над $\mathbb{Q}$

Примеры. $K = \mathbb{Q}$, $\quad L = \mathbb{C}$

1. $\alpha = i$ — алгебраическое
   Минимальный многочлен $P(x) = x^2 + 1$
2. $\alpha = \sqrt[3]{5}$
   $P(x) = x^3 - 5$ — аннулирующий, минимальный
3. $\alpha = 1 + \sqrt[3]{5}$ — алгебраическое
   Найдём аннулирующий многочлен:
$$(\alpha - i)^3 = 5$$
$$\alpha^3 - 3\alpha^2 i + 3\alpha i^2 - i^3 = 5$$
$$(\alpha^3 - 3\alpha - 5) + (-3\alpha + 1)i = 0$$
$$\alpha^3 - 3\alpha - 5 = (-3\alpha + 1)i$$
$$(\alpha^2 - 3\alpha - 5)^2 = -(-3\alpha + 1)^2$$
$$(\alpha^3 - 3\alpha + 5)^2 + (3\alpha + 1)^2 = 0$$
$$P(x) = (x^3 - 3x + 5)^2 + (3x + 1)^2$$
4. $\alpha = \sqrt[3]{2 + 4\sqrt[4]{5}}$ — алгераич.
$$\alpha^3 = 2 + 4\sqrt[4]{5}$$
$$\alpha^3 - 2 = 4\sqrt[4]{5}$$
$$(\alpha^3 - 2)^4 = 4^4 \cdot 5$$

$$(\alpha^3-2)^4 - 4^4\cdot 5 = 0$$
$$P(x) = (x^3-2)^4 - 4^4\cdot 5$$

5. e, π — трансцендентные

Свойства (минимального многочлена). K — поле, L — расширение K, $\alpha \in L$, α алг. над K

1. Пусть $P(x)$ — минимальный для α.
   Тогда
   $$F(\alpha) = 0 \iff F(x) \vdots P(x)$$

   Доказательство.
   $$F(x) = P(x)Q(x) + R(x), \qquad \deg R < \deg P$$

   - $\Longleftarrow$
     $$F(x) \vdots P(x) \implies R(x) = 0$$
     $$F(x) = P(x)Q(x)$$
     Подставим α:
     $$F(\alpha) = \underbrace{P(\alpha)}_{0} Q(x) = 0$$
   - $\implies$
     $$\underbrace{P(\alpha)}_{0} Q(\alpha) + R(\alpha) = 0$$
     $$R(\alpha) = 0 \implies R \text{ — нулевой}$$

   □

2. Минимальный многочлен для α единственен

   Доказательство. Пусть $P_1 P_2$ — минимальные
   $$\xRightarrow[\text{св-во 1}]{} \begin{cases} P_1(x) \vdots P_2(x) \\ P_2(x) \vdots P_1(x) \end{cases} \implies P_1(x) = P_2(x)$$
   □

3. Минимальный многочлен неприводим над K

   Доказательство. Пусть $P(x) = S(x)T(x)$, $0 < \deg S, \deg T < \deg P$
   $$0 = P(\alpha) = \underbrace{\underbrace{S(\alpha)}_{\in L}\underbrace{T(\alpha)}_{\in L}\ L \text{ — поле}} \left[\begin{array}{l} S(\alpha) = 0 \\ T(\alpha) = 0 \end{array}\right. \quad \lightning \quad \deg S, \deg T < \deg P$$
   □

4. Если $P(x)$ неприводим над K, $P(x) \neq 0$, $P(\alpha) = 0$
   $$\implies P(x) \text{ — минимальный для } \alpha$$

   Доказательство.
   $$\left.\begin{array}{l} P(x) \vdots \text{ миним.} \\ P(x) \text{ — непривод.} \end{array}\right\} \implies P(x) \text{ — миним.}$$
   □

Пример. $x^3 - 5$ — минимальный для $\sqrt[3]{5}$ над $\mathbb{Q}$, т. к. он неприводим над $\mathbb{Q}$

Определение 4. Расширение L над K называется алгебраическим, если любой элемент L является

алгебраическим над K
Иначе — тренсцендентным

Теорема 1. Конечное расширение полей является алгебраическим

Доказательство. Пусть L — конечное расширение K, $\quad n := |L : K|, \quad \alpha \in L$.
Докажем, что α — алгебраическое:
Элементы $\underbrace{1, \alpha, \dots, \alpha^{n-1}, \alpha^n}_{n+1} \in L$ ЛЗ над K, т. е.

$$\exists\, k_0, k_1, \dots, k_{n-1} k_n \in K \notin \bigodot : \quad k_0 \cdot 1 + k_1\alpha + \dots + k_{n-1}\alpha^{n-1} + k_n\alpha^n = 0$$

Пусть $P(x) = k_0 + k_1 x + \dots + k_{n-1}x^{n-1} + k_n x^n$.
Тогда $P(x) \in K[x], \quad P(x)$ — ненулевой, $\quad P(\alpha) = 0 \quad \implies \alpha$ — алгебраичсекое. $\square$

Определение 5. L — поле, $\qquad K$ — подполе L, $\qquad \alpha_1, \dots \alpha_n \in L$
Через $K(\alpha_1, \dots, \alpha_n)$ будем обозначать наимеьшее подполе L, содержащее K и $\alpha_1, \dots, \alpha_n$.
Если $M = K(\alpha_1, \dots \alpha_n)$, то говорят, что M получено из K присоединением $\alpha_1, \dots, \alpha_n$.
Поле, полученное из K присоединением оного элемента, называется простым расширением K.

Пример. $\mathbb{Q}(\sqrt{2})$ — простое расширение $\mathbb{Q}$

Теорема 2 (строение простого алгебраического расширения). L — поле, $\qquad K$ — подполе L, $\qquad \alpha \in L$, $\qquad \alpha$ алг. над K, $\qquad P(x)$ — минимальный многочлен для α над K
Тогда

1. $K(\alpha) \simeq {}^{K[x]}\!/\!_{\langle P(x)\rangle}$
   $\overline{F(x)} \mapsto F(\alpha)$ является изоморфизмом.
2. $K(\alpha)$ конечно над K, $\quad |K(\alpha) : K| = \deg P$
   $1, \alpha, \dots, \alpha^{n-1}$ образуют базис $K(\alpha)$ над K.

Доказательство. Определим $f : K[x] \to K(\alpha)$ как $f(F) := F(\alpha)$ $(x \mapsto \alpha)$, т. к.

$$f(c_0 + c_1 x + \dots c_k x^k) = c_0 + c_1\alpha + \dots c_k\alpha^k, \qquad c_i \in K$$

- Проверим, что f — гомоморфизм:

$$f(F + G) = (F + G)(\alpha) = F(\alpha) + G(\alpha) = f(F) + f(G)$$

$$f(FG) = (FG)(\alpha) = F(\alpha)G(\alpha) = f(F)f(G)$$

- Найдём $\ker f$:

$$F(x) \in \ker f \iff f(F) = 0 \iff F(\alpha) = 0 \iff F(x) \,\vdots\, P(x)$$

$$\implies \ker f = \langle P(x)\rangle$$

- Применим теорему о гомомрфизме:

$$\operatorname{Im} f \simeq {}^{K[x]}\!/\!_{\ker f}$$

  Изоморфизм $\varphi(\overline{F}) = f(F) = F(\alpha)$
  Получили изоморфизм ${}^{K[x]}\!/\!_{\langle P(x)\rangle} \to \operatorname{Im} f$

- Проверим, что $\operatorname{Im} f \stackrel{?}{=} K(\alpha)$:

$$\left.\begin{aligned} &\alpha \in \operatorname{Im} f, \text{ т. к.} \alpha = f(x) \\ &K \subset \operatorname{Im} f, \text{ т. к.} \underset{\in K}{k} = f(k) \end{aligned}\right\} \xRightarrow[\operatorname{Im} f\text{ — поле}]{} \operatorname{Im} f \supset K(\alpha)$$

- Проверим, что $1, \alpha, \dots, \alpha^{\deg P - 1}$ — базис:
  Пусть $n := \deg P$
  - ЛНЗ:
    Пусть ЛЗ:
    $$a_0 \cdot 1 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = 0, \quad a_i \in K$$
    Пусть $F(x) := a_0 + a_1x + \dots + a_{n-1}x^{n-1} \implies F(\alpha) = 0$
    $$\implies F(x) \vdots P(x) \xRightarrow[F(x)\text{ — ненулевой}]{} \deg F \geq \deg P = n \quad \lightning$$
  - Попрождающий:
    $$K(\alpha) = \operatorname{Im} f$$
    Пусть $u \in K(\alpha) \implies \exists F \in K[x]: \quad f(F) = u \quad \implies F(\alpha) = u$
    Делим с остатком:
    $$F(x) = Q(x)P(x) + R(x), \qquad \deg R < \deg P$$
    $$\implies \deg R \leq n + 1$$
    $$F(\alpha) = Q(\alpha)\underbrace{P(\alpha)}_{0} + R(\alpha) = R(\alpha)$$
    $$R(x) = a_0 + a_1x + \dots a_{n-1}x^{n-1} \implies F(\alpha) = a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1}$$

□

Примеры.

1. $\mathbb{Q}(\sqrt[3]{2}), \quad \alpha = \sqrt[3]{2}$
   $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ — базис $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.
   Любой элемент можно представить в виде $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, \quad a, b, c \in \mathbb{Q}$.
   Пример сложения:
   $$\left(1 + 2\sqrt[3]{2} + 3(\sqrt[3]{2})^2\right) + (-1 + \sqrt[3]{2}) = 3\sqrt[3]{2} + 3(\sqrt[3]{2})^2$$
   Пример умножения:
   $$(1 + \sqrt[3]{2})(2\sqrt[3]{2} + 3\sqrt[3]{2})^2 = 2\sqrt[3]{2} + 3(\sqrt[3]{2})^2 + 2\sqrt[3]{2}^2 + 3(\sqrt[3]{2})^3 = 2\sqrt[3]{2} + 5(\sqrt[3]{2})^2 + 6$$
2. $P(x) = x^5 - 5x^4 + 5$ — неприводимый над $\mathbb{Q}$ по критерию Эйзенштейна
   $$x^5 - \underset{\vdots 5}{5}x^4 + \underset{\vdots 5}{0}x^3 + \underset{\vdots 5}{0}x^2 + \underset{\vdots 5}{0}x + \underset{\vdots 5}{5}$$
   α — комплексный корень
   $$K = \mathbb{Q}, \quad L = \mathbb{C}$$
   Рассмотрим $\mathbb{Q}(\alpha)$:
   $$|\mathbb{Q}(\alpha) : \mathbb{Q}| = 5$$
   $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ — базис $\mathbb{Q}(L)$ над $\mathbb{Q}$.

Следствие. α — алгебраический над K, $\qquad F, G \in K[x], \qquad G(\alpha) \neq 0, \qquad \beta = \frac{F(\alpha)}{G(\alpha)}$
Тогда β — алгебраический над K

Доказательство. L — расширение K, $\qquad \alpha \in L$
$$\implies \beta \subset L$$
Существует поле $K(\beta)$.
При этом $\beta \in K(\alpha)$.
$$K \subset K(\beta) \subset K(\alpha)$$
Применим одно из следствий из теоремы о мультипликативности расширения:

$K(\alpha)$ над K конечно $\implies K(\beta)$ над K конечно
$\implies$ все элементы $K(\beta)$ алгебраичны над K $\square$

Примеры.

1. α — алг. над K.
   Тогда $\frac{\alpha^2+3}{\alpha+1}$ — алг. над K
2. $\dfrac{\sqrt[3]{2}+1}{(\sqrt[3]{2})^2+5}$ — алг. число

Следствие. $\alpha_1, \ldots, \alpha_n$ алгебраичны над K
Тогда $K(\alpha_1, \ldots, \alpha_n)$ конечно над K

Доказательство.

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \ldots, \alpha_n)$$

Достаточно доказать, что $K(\alpha_1, \ldots, \alpha_i, \alpha_{i+1})$ кончено над $K(\alpha_1, \ldots, \alpha_i)$:
.... TODO: Дописать доказательство $\square$

Следствие. α, β алгебраичны над K
$\implies \alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta, \quad {}^{\alpha}\!/_{\beta}$ алгебраичны над K

Доказательство. TODO: Дописать доказательство $\square$