

1

$$\frac{9 - 40\sqrt[3]{6} - 6\sqrt[3]{36}}{1 - 3\sqrt[3]{6} - \sqrt[3]{36}} \in \mathbb{Q}(x) \simeq \mathbb{Q}[x]/(x^3 - 6)$$

$$\frac{9 - 40\sqrt[3]{6} - 6\sqrt[3]{36}}{1 - 3\sqrt[3]{6} - \sqrt[3]{36}} = a_0 + a_1x + a_2x^2 \rightarrow 9 - 40\sqrt[3]{6} - 6\sqrt[3]{36} = (1 - 3\sqrt[3]{6} - \sqrt[3]{36}) \cdot (a_0 + a_1x + a_2x^2)$$

Понижение степени $x^3 = 6, x^4 = 3x$

$$\begin{cases} 9 = a_0 - 6a_2 - 18a_1 \\ -40 = a_1 - a_0 - 18a_2 \\ -6 = a_2 - a_2 - 3a_2 \end{cases} \rightarrow \begin{cases} a_0 = 3, \\ a_1 = -1, \\ a_2 = 2 \end{cases}$$

$$\frac{9 - 40\sqrt[3]{6} - 6\sqrt[3]{36}}{1 - 3\sqrt[3]{6} - \sqrt[3]{36}} = 3 - x + x^2$$

2

$$a = \sqrt{7} - \sqrt{3} - 1 \rightarrow (a - 1)^2 = 10 - 2\sqrt{21} \rightarrow (a^2 + 2a - 9)^2 = 84 \rightarrow x^4 + 4x^3 - 14x^2 - 36x - 3 - \text{минимальный многочлен для } a$$

Теперь покажем, что $[\mathbb{Q}(\sqrt{7})(\sqrt{3}) : \mathbb{Q}] = 4$

$$[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2, \min_{\text{многочлен}} = x^2 - 7$$

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\sqrt{7})] = 2$$

$$\text{Пусть } \sqrt{3} \in \mathbb{Q}(\sqrt{7}) \rightarrow \sqrt{3} = a + b\sqrt{7} \rightarrow 7 = a^2 + 7b^2 + 2\sqrt{7}ab \rightarrow \begin{cases} 7 = a^2 + 7b^2 \\ 0 = 2\sqrt{7}ab \end{cases} \rightarrow$$

$a = 0$ или $b = 0$ - Противоречие.

$$[\mathbb{Q}(\sqrt{7})(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4, \text{ базис } \mathbb{Q}(\sqrt{7})(\sqrt{3}) = \{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$$

3

$x^3 + x + 1$ - неприводимый многочлен степени 3 над полем \mathbb{Z}_2 . $|\mathbb{Z}_2/(x^3 + x + 1)| = 2^3 = 8$

$$\mathbb{Z}_2/(x^3 + x + 1) = F_8 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^2+x\} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \},$$

где α - корень многочлена $x^3 + x + 1$

$$\alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1, \alpha^7 = 1$$

Сложение идет по модулю 2.

| \times | 0 | 1 | α | α^2 | α^3 | α^4 | α^5 | α^6 |
|------------|---|------------|------------|------------|------------|------------|------------|------------|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | α | α^2 | α^3 | α^4 | α^5 | α^6 |
| α | 0 | α | α^2 | α^3 | α^4 | α^5 | α^6 | 1 |
| α^2 | 0 | α^2 | α^3 | α^4 | α^5 | α^6 | 1 | α |
| α^3 | 0 | α^3 | α^4 | α^5 | α^6 | 1 | α | α^2 |
| α^4 | 0 | α^4 | α^5 | α^6 | 1 | α | α^2 | α^3 |
| α^5 | 0 | α^5 | α^6 | 1 | α | α^2 | α^3 | α^4 |
| α^6 | 0 | α^6 | 1 | α | α^2 | α^3 | α^4 | α^5 |

Таблица 1: Таблица умножения в поле F_8

4

Поле $K[\alpha] \subseteq K(\alpha)$ по определению.

Надо доказать включение в обратную сторону.

$K[\alpha]$ — конечно, значит можно рассматривать его как векторное пространство над K

Теперь рассмотрим минимальный многочлен $p(x)$ для α .

Он неприводим над K , его степень равна степени расширения $[K[\alpha] : K]$.

Теперь рассмотрим элемент из $K(\alpha)$. Любой его элемент может быть представлен в виде $\frac{g(\alpha)}{h(\alpha)}$. Но в тоже время $\frac{g(\alpha)}{h(\alpha)} \in K[\alpha] \rightarrow \frac{g(\alpha)}{h(\alpha)} = \gamma_0 + \gamma_1 \cdot \alpha + \dots + \gamma_n \cdot \alpha^n$ (т.к для всех степеней, начиная с n будет формула понижения степени). $\rightarrow K(\alpha) \subseteq K[\alpha] \rightarrow K(\alpha) = K[\alpha]$