Модуль III Теория Галуа (Galois) лекция 11

1. $F_4 \not\cong \mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$
2. $F_4 \not\subset F_8$

(N1)

Чему равно $F_2 \otimes F_3$ или $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z}$ - ?

$\alpha \quad a \otimes b$

$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$

$(\lambda a) \otimes b = a \otimes (\lambda b) = \lambda (a \otimes b)$

$\mathbb{Z}$ в $\mathbb{Z}_1 \otimes \mathbb{Z}_3$

$5a \otimes b \quad a \otimes 5b$

$\| \quad \|$

$a \otimes b \quad a \otimes 2b$

$\|$

$a \otimes (-b) = -a \otimes b$

$2(a \otimes b) = 0$

$3(a \otimes b) = 0$

$\Downarrow$

$a \otimes b = 0$

$\Downarrow$

Ответ: $\{0\}$

(N2)

$\mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = ?$

$3(a \otimes b) = 0$

$\Downarrow$

Ответ: $\mathbb{Z}/3\mathbb{Z}$ $(1 \otimes 1 = 2 \otimes 2; \quad 1 \otimes 2 = 2 \otimes 1; \quad 0)$

(N3)

$\mathbb{Z}/6\mathbb{Z} \otimes \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$

$\|$

$(\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z}) \otimes \mathbb{Z}/6\mathbb{Z}$

Ответ: $\mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/НОД(n,m)\mathbb{Z}$

Теория Галуа - Теория решения алгебраических уравнений ⇒ Теория расширения полей

$x^4 - 4x^3 + 3x^2 - 5x + 6 = 0$

$\sqrt[3]{121}$, $\sqrt[4]{\sqrt[3]{121} + i\sqrt{15}}$, $x^3 = 121$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{121}) \subset \mathbb{Q}(\sqrt[4]{\sqrt[3]{121}})$

$\cup$

$\mathbb{Q}(x_0)$

Корпус - K-поле $\subset L$-поле

Field F $K((t))$

$\cup$

$\mathbb{R} \subset \mathbb{R}((t))$ $\{t^N\}$, $N \in \mathbb{Z}$ $1 + t + t^2 + \dots$

$\mathbb{Q}$

Конечное расширение L над K - конечномерное векторное пространство

ψ_x

$1 \in K$, $x, x^2, x^3, \dots$ $x_i \in K$

$\underbrace{a_0 \cdot 1 + a_1 \cdot x + a_2 \cdot t^2 + \dots + a_N x^N = 0}$

уравнение на x

$\forall x \in L$ удовлетворяет алгебраическому уравнению над K

Как строить конечные расширения

$K \rightsquigarrow K[t]$ p - неприводимый многочлен над K

$K[t]/(p)$ - фактор кольцо

$Q \sim Q'$ если $Q - Q' : P$

Если P-неприводим, то $K[t]/(P)$ - поле Нужно проверить что к каждому элементу есть обратный

$\bar{Q} \neq 0$, т.е $Q \not\vdots P$

$\exists \bar{R} : \bar{Q}\bar{R} = 1$

Хотим найти R т.что $QR = 1 \pmod P$

$QR \sqcap PS = 1$ для некоторого $S \in K[t]$

Взаимно просты ⇒ Алгоритм Евклида

Вопрос $\dim_K K[t]/(P)$ ∞

$\deg P = N$

$\bar{1}, \bar{t}, \bar{t^2}, \bar{t^3}, \dots, \bar{t}^{N-1}$ - базис в $K[t]/(P)$

$\mathbb{R}[t]/(t^2+1) \xrightarrow{\sim} \mathbb{C}$ $\bar{t} \to i$

Теорема о примитивном элементе

При естественных ограничениях всякое конечное $L|_K$ имеет вид $K[t]/(p)$

<u>Поле разложения</u> Пусть $p(t)$ - любой многочлен над K

$K[t]/p(t)$ Разложим на неприводимые многочлены $p = p_1^{\alpha_1} \dots p_n^{\alpha_n}$

$$K \rightsquigarrow K[t]/(p_1) = L_1$$

$$p \in K[t] \subset L_1[t]$$

У многочлена $p \in L_1[t]$ есть корень $\bar{t} \in L_1$

$(K = \mathbb{R},\ p = t^2+1$

$L = \mathbb{R}[t]/(t^2+1) \simeq \mathbb{C},\ \bar{t} \to i)$.

$K = \mathbb{Q},\ p = t^3-2$

$L = \mathbb{Q}[t]/(t^3-2)$

Над L:

$p = (t - \sqrt[3]{2})\, p' \quad \deg p' = 2$.

<u>Так можно строить конечное расширение</u> Над полем L ${}^{(1)}p = {}^{(1)}p_1^{a_1}, \dots, {}^{(1)}p_m^{a_m}$ сделаем с ним то же

в конце концов получим поле L_r, над которым p раскладывается на линейные многочлены

<u>Задача</u> 183 станции, 14 станций на линии, $\forall 2$ станции соедин. линией, $\forall 2$ линии пересекаются. Возможно?

Решение: $\mathbb{F}_{13} = \mathbb{Z}/13\mathbb{Z}$

$$\mathbb{P}^2(\mathbb{F}_{13}) = \underset{169}{A^2} \sqcup \underset{13}{A^1} \sqcup \underset{1}{A^0} \quad \text{линии-прямые } \mathbb{P}^1$$

$|\mathbb{P}^1| = 13 + 1 = 14,\ A^1 \sqcup \infty$

Теорема: мультипликативная группа $F \setminus 0$ конечного поля циклическая

$\mathbb{F}_{17} = \mathbb{Z}/17\mathbb{Z}$ есть вычет a т.е.

$a, a^2, a^3, \dots, a^{16} = 1$ – все вычеты $\neq 0$

Д-во: $F \setminus 0$ – абелева конечная группа

$\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus$

Порядок ее равен $1 = q_1^{\alpha_1} \dots q_n^{\alpha_n}$

$\frac{p-1}{q_1}, \frac{p-1}{q_2}, \dots, \frac{p-1}{q_n}$

$r_1 \quad r_2 \quad r_n$

$x^{p-1} = 1$ – уравнение над F, которое разложится на все линейные множители, у него равно $(p-1)$ корней $\{F \setminus 0\}$

$t^{r_1} = 1$ у него $= r_1$ корней

$\Rightarrow$ есть x_1, т.что $x_1^{r_1} \neq 1$

$r_1 = q_1^{a_1 - 1} q_2^{a_2} \dots q_n^{a_n}$

Возведя x_1 в подходящую степень, получим элемент порядка $(x_1 q_2^{a_2} \dots q_n^{a_n}) = y_1$

$y_1^{q_1^{a_1}} = 1$, $r_1 = y_1^{q_1^{a_1 - 1}} \neq 1$

$\operatorname{ord} y_1 \equiv q_1^{a_1}$, $\operatorname{ord} y_n = q_n^{a_n}$