ОСА. Лекция

12 ноября 2024 г.

$$H \le Aut^F/_K$$
$$L^H = \{a \in F \mid \phi(a) = a\ \forall \phi \in H\} \text{ - подполе в F}$$
$$\phi(a^{-1}) = a^{-1} \quad a \in L^H$$
$$1 = \phi(1) = \phi(a \cdot a^{-1}) = \phi(a)\phi(a^{-1}) = a\phi(a^{-1})$$

Конечные поля

Note $|K| = p^n = q \implies x^q - x = 0\ \forall x \in K$
$x = 0\ +$
$U(K) = K \setminus \{0\} \implies |U(K)| = q - 1 \implies \forall x_0 \in U(K):\ x_0^{q-1} = 1 \implies x_0^q = x_0$

Th1 Пусть p - простое. $\implies \forall n \in \mathbb{N}\ \exists!$ с точность до изоморфизма поле K из p^n элементов
Proof Рассмотрим $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ и $\mathbb{Z}_p \subset L = \mathbb{Z}_p(x_1, \dots x_{p^n})$ - поле разложения f(x)
$x_1, \dots x_{p^n}$ - различны $(f'(x) = -1)$
$(x_i + x_j)^{p^n} = x_i^{p^n} + x_j^{p^n} = x_i + x_j \implies x_i + x_j$ - корень f(x), $i \neq j$
$\left(\frac{x_i}{x_j}\right)^{p^n} = \frac{x_i^{p^n}}{x_j^{p^n}} = \frac{x_i}{x_j}$ - корень f(x) $\implies \{x_1, \dots, x_{p^n}\}$ - поле из p^n элементов и все эл-ты этого поля - корни f(x) $\implies$ оно $= L$ - единственное с точностью до изоморфизма

Th.2 Let L - поле, $|L| = p^n . K \subset L$, где $|K| = p^m$ - подполе $\iff m \mid n$
Proof $\implies: K \subset L \implies$ L - в.п. над K с базисом $\{\alpha_1, \dots, \alpha_s\}$

$$\implies \forall \alpha \in L:\ \alpha = k_1\alpha_1 + \dots + k_s\alpha_s \implies p^n = (p^m)^s \implies m \mid n$$

$\impliedby: m \mid n$
$$p^n - 1 = (p^m)^s - 1 = (p^m - 1) \cdot t$$
$$x^{p^n} - x = x(x^{p^n-1} - 1) = x((x^{(p^m-1)})^t - 1) = x(x^{p^m-1} - 1)h(x)(x^{p^m} - x)h(x) \implies (x^{p^m} - x) \mid (x^{p^n} - x)$$
$$\implies \text{ корни } x^{p^m} - x \text{ являются корями в } x^{p^n} - x$$

Th.3 Пусть K - поле, G - конечняа подгруппа в U(K). Тогда G - циклическая
Proof
$$G = G_{p_1} \times \dots \times G_{p_s},\ \text{где } G_{p_i} = \{g \in G \mid O(g) = p_i^{k_i}\}$$
Выберем элемент $g^\star = (g_1^\star, \dots, g_s^\star)$, где $O(g_i^\star)$ - max in $G_{p_i},\ i = \overline{1, s}$ т.е $O(g_i^\star) = p_i^{t_i},\ t_i - \max \implies O(g^\star) = p_1^{t_1} \dots p_s^{t_s} = q$ Рассмотрим
$$x^q - 1 = e \tag{1}$$

1) $\forall g \in G$ - корень ур-я (1): если $O(g) = p_1^{l_1} \dots p_s^{l_s}$, то $l_i \le t_i \implies g^q = 1$
Корней не более q штук, все степени $g^\star$ - корни (1), их q штук $\implies \forall g \in G$ - степень $g^\star \implies G =< g >$
Следствие Если $|K| = n < \infty$, то $U(K)$ - циклическая

Алгебры над полями

Def K - поле, множество A наз-ся алгебрлой (ассоциативной), если
1) A - кольцо
2) A - векторное пр-во над K
3) $\lambda(ab) = (\lambda a)b = a(\lambda b),\ \forall a, b \in A;\ \lambda \in K$

Examples 1) $K \subset L$
2) $M_n(K)$
3) $F(X, K),\ X$ - мн-во, K - поле $= \{f : X \to K\}$ - функции
4) $K[x]$
Подалгебра - подкольцо + подпр-во
Идеал - идеал кольца + подпр-во
факторалгебра

Def Ассоциативное колько с 1, в котором любой ненулевой элемент обратим называется телом. Алгебра, являющаяся телом, называется алгеброй с делением

$$Z(A) = \{a \in A \mid ab = ba\ \forall b \in A\} \text{ - центр}$$

Если A алгебра с делением, то $Z(A)$ - поле $\implies$ A - алгебра над центром
A - алгебра с делением над K

$$\forall \lambda \in K \mapsto \lambda \cdot 1 \in A$$

$$\{\lambda \cdot 1 \mid \lambda \in K\} \cong K$$

Утв A - конечномерная алгебра без делителей нуля $\implies$ A - алгебра с делением
Proof

$$\forall 0 \neq \alpha \in A;\ \text{A кон/мер} \implies 1, \alpha, \alpha^2, \dots, \alpha^n \text{ - лз} \implies \exists \text{ не все } 0,\ \lambda_0, \lambda_1, \dots \lambda_k \in K$$

$$\implies \lambda_0 + \lambda_n \alpha^n = 0 \implies \alpha \text{ - корень } \lambda_0 + \lambda_n \alpha^n \in K[x] \implies \alpha \text{ - алг над K} \implies$$

$$\text{let } \mu_\alpha(x) = a_0 + a_1 x + \dots + x^s \in K[x],\ \text{т.е. } a_0 + a_1\alpha + \dots + \alpha^s = 0$$

Если $a_0 = 0 \implies \alpha(a_1 + a_2\alpha + \dots + \alpha^{s-1}) = 0 \implies a_1 + a_2\alpha + \dots \alpha^{s-1} = 0$

$$\implies a_0 \neq 0 \implies a_1\lambda + \dots + \lambda^s = -a_0 \implies \alpha(a_1 + \dots + \alpha^s) = -a_0$$

$$\implies \alpha[(a_1 + \dots + \alpha^{s-1})(-a_0)^{-1}] = 1 \implies [(a_1 + \dots + \alpha^{s-1})(-a_0)^{-1}] = \alpha^{-1}$$