Лекция №6 «Группа автоморфизмов. Норма и след». Курс A-I

Иванова Ксения Юрьевна 619/1

14 октября 2025

В прошлый раз
$\mathrm{F}_q = F_p[x]/(f) \quad q = p^n \quad n = degf \quad f -$ непрерыв

Теорема 1. $\forall n \quad \exists F_q \quad q = p^n$

Теорема 2. $F_q^* -$ *циклическая группа с* $\quad \varphi(q-1)$

Расширение полей L/K
Конечное расширение, если $\dim_k L < \infty \quad [L:K] = dim_k L$
$\alpha \in L -$ алгебр. $\Leftrightarrow \exists f \in K(x) \quad f(\alpha) = 0$
L/K - алгебр. $\Leftrightarrow \forall \alpha \in L -$ алгебр.

Теорема 3. *L/K - конечное расширение, то* $\Rightarrow$ *алгебр.*

L/K называется простым, если $\exists \theta \in L \quad L = K(\theta)$
$F_q = F_p[x]/(f) -$ простое построение
$F_q[x] \to F_p[x]/(f)$
$x \to \theta : \quad f(\theta) = 0$
$F_q = F_p(\theta)$

Лемма 1. *1)* $\quad a \in Z_{>0} \quad a^L - 1 | a^m - 1 \Leftrightarrow L|m$
2) $\quad x^L - 1 | x^m - 1 \quad$ *в* $\quad F_q[x] \Leftrightarrow L|m$
$\square \quad$ *Упражнение* $\blacksquare$

Теорема 4. $F_{p^d} -$ *подполе* $\quad F_{p^n} \Leftrightarrow d|n$
$\square$
$\Rightarrow F -$ *подполе* $\quad F_{p^n} \quad F_{p^n}/F/F_p, \quad d = [F:F_p]$
$|F| = p^d \quad |F^*| = p^d - 1$
$\forall x \in F^* \quad x^{p^d-1} - 1 = 0$
$\forall x \in F_{p^n}^* \quad x^{p^n-1} - 1 = 0$
$F^* \subset F_{p^n}^* \Rightarrow x^{p^d-1} - 1 | x^{p^n-1} - 1 \Rightarrow$ (*лемма*) $\quad d|n$
$\Leftarrow$ *Пусть* $\quad d|n$
$F = \{\alpha \in F_{p^n} : \alpha^{p^d} = \alpha\}$
$\forall \alpha, \beta \quad (\alpha+\beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$
$F -$ *поле*
$d|n \Leftrightarrow$ *лемма* $\quad x^{p^d} - x | x^{p^n} - x \quad (x^{p^d} - x \quad$ *имеет* $\quad p \quad$ *различных корней*$) \Rightarrow |F| = p^d \quad$ *элементов*
$F = F_{p^d} -$ *подполе* $\quad F_{p^n} \quad \blacksquare$

Следствие. $F_{q^d} - подполе \quad F_{q^n} \Leftrightarrow d|n$
$\square \quad q = p^t \quad F_{p^{nt}}/F_{p^{dt}} \Leftrightarrow dt|nt \Leftrightarrow d|n \qquad \blacksquare$

Определение 1. $\sigma : K \to K - автоморфизм,\ если\ сохраняется\ структура\ поля.$
$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$
$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$

Определение 2. $L/K \quad Рассмотрим\ автоморфизмы \quad \sigma : L \to L$
$\sigma(a) = a \quad \forall a \in K$
$Gal(L/K) = \{\sigma : L \to L \quad \sigma(a) = a, \quad a \in K\}$
$F_q/F_p, \quad F_q = F_p(\theta)$

Определение 3. $Сопост \quad \sigma : \theta \to \theta^p \quad индуцир\ отобр \quad \sigma : F_q \to F_q$
$\alpha = a_1\theta^{n-1} + \cdots + a_0 \quad \to \quad a_1((\theta)^p)^{n-1} + \ldots \quad a \in F_p \quad \sigma(a) = a^p = a$
$\Rightarrow \sigma \in Gal(F_q/F_p) \quad называется\ автормофизм\ Фробениуса$

Теорема 5. $Gal(F_q/F_p) =< \sigma > - циклическая\ с\ порождающим\ элементом \quad \sigma$
$|Gal(F_q/F_p)| = n = [F_q : F_p]$
$\square \quad Рассмотрим \quad \sigma^i \quad \sigma(\alpha) = \alpha^p$
$\sigma^i(\alpha) = \alpha^{p^i} \quad 0 \le i \le n-1$
$\sigma^i \in Gal(F_q/F_p) = G$
$\sigma^i \ne \sigma^k$
$F_q = F_p[x]/(f) = F_p[\theta]$
$f(\theta) = 0, \quad f = x^n + a_1x^{n-1} + \ldots$
$f(\theta^p) = (\theta^p)^n + a_1(\theta^p)^{n-1} + \cdots = (\theta^n + a_1\theta^{n-1} + \ldots)^p = f(\theta)^p = 0 \quad \theta^p - корень \quad f$
$\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}} - корень \quad f$
$F_q^* =< \eta > \quad \eta - порождающий \quad q-1$
$\eta = b_1\theta^{n-1} + \ldots$
$если \quad 0 \le j \le k \le n-1 \quad \theta^{p^j} = \theta^{p^k}$
$\eta^{p^j} = \eta^{p^k} \Rightarrow \eta^{p^k - p^j} = 1$
$p^k - p^j < q-1 \quad (получаем\ противоречие\ с \quad q)$
$Значит \quad f(x) = \prod_{j=0}^{n-1}(x - \theta^{p^j})$
$\varphi \in Gal(F_q/F_p)$
$0 = \varphi(f(\theta)) = f(\varphi(\theta)) \Rightarrow \varphi(\theta) - корень \quad f$
$\varphi(\theta) = \theta^{p^j} \qquad \blacksquare$

Пусть $\quad G_n = Gal(F_{p^n}/F_p)$
$[F_{p^n} : F_p] = n = |G_n|$
$F_{p^d} -$ подполе $\quad F_{p^n} \Leftrightarrow d|n \Leftrightarrow$ существует цикл подгруппа порядка $\quad d \quad$ b $\quad G_n$
Общий случай : $\quad L/K, \quad G = Gal(L/K)$

$$\left\{\begin{matrix}\text{подполя} \quad F \\ L/F/K\end{matrix}\right\} \Leftrightarrow \left\{\begin{matrix}\text{подгруппы} \\ H < G\end{matrix}\right\}$$

$F \to Gal(F/K)$
$L^H \leftarrow H \quad (\text{для} \quad L : \{\alpha \in L : \quad \forall \sigma \in H \quad \sigma\alpha = \alpha\})$

Определение 4. *Коненчое расширение* $\quad L/K \quad$ *называется расширением Галуа, если* $\quad |Gal(L/K)|=[L:K]$

Лемма 2. $|Gal(L/K)| \leq [L:K]$

Норма и след
L/K - конечное расширение
[L:K]=n
$\forall \alpha \in L \qquad \zeta \to \alpha\zeta$
$\{\omega_1, \ldots, \omega_n\} -$ базис $\quad L/K$
$A_\alpha = (a_{ij}) -$ матрица $\quad \zeta \to \alpha\zeta$
$\alpha w_i = \sum_{i=1}^{n} a_{ij} w_j \quad a_{ij} \in K$
$g_\alpha(x) = det(xE_n - A) \in K[x]$

Лемма 3. *$\alpha \in L, f_\alpha \in K[x] -$ линейный многочлен $\quad \alpha, \quad g_\alpha -$ характеристический многочлен. Тогда $\quad g_\alpha = f_\alpha^s$*
$\square \quad L/K(\alpha)/K$
$n = [L:K] = [L:K(\alpha)][K(\alpha):K] \quad ([L:K(\alpha)] = s, \quad [K(\alpha):K] = m)$
Упражнение ■

Лемма 4. *g_α не зависит от выбора базиса!*
$\square \quad \ldots$ ■

Определение 5. $N_{L/K}(\alpha) = detA_\alpha$

$\mathrm{Tr}_{L/K}(\alpha) = trA_\alpha$

Лемма 5. *1)* $\quad a \in K \quad N_{L/K}(a) = a^n \quad Tr_{L/K}(a) = na$
2) $\quad N(\alpha\beta) = N(\alpha)N(\beta) \quad Tr(\alpha + \beta) = Tr\alpha + Tr\beta$

Лемма 6. *$M/L/K$*
$N_{M/K} = N_{M/L} * N_{L/K}$
$Tr_{M/K} = Tr_{M/L} * Tr_{L/K}$

Определение 6. *L/K - конечное расширение называется сепарабельным* $\Leftrightarrow Tr_{L/K} \not\equiv 0$

Пример. *char $h = p$*
$Tr_{L/K}(1) = n \neq 0, \quad p \not| \quad n$

Определение 7. *$L/K \quad$ называется нормальным, если $\quad \forall \alpha \in L$*
$f_\alpha(x) \quad$ полностью раскладывается на линейные множители $\quad (L)$

Теорема 6. *L/K - нормально, сепарабельно* $\Leftrightarrow |Gal(L/K)| = [L:K]$

Лемма 7. *F_q/F_p*
1) $\quad N(\alpha) = \prod_{j=0}^{n-1} \sigma^j(\alpha) = \prod_{j=0}^{n-1} \alpha^{p^j}$
$Tr(\alpha) = \sum_{j=0}^{n-1} \sigma^j(\alpha) = \sum_{j=0}^{n-1} \alpha^{p^j}$
2) $\quad N: \quad F_q^* \to F_p^*, \quad Tr: \quad F_q \to F_p \quad$ *отображение на*
$\square \quad 2) \quad Tr \quad x + x^p + \cdots + x^{p^n - 1} \leq p^{n-1} \quad$ *корней,* $\quad a \quad |F_q^*| = p^n - 1 \qquad$ ■