

## Абсолютната група на Galois на крайно поле.

Абсолютната група на Galois на поле  $K$  е групата на Galois  $Gal(K^{sep}/K)$  на сепарабелната обвивка  $K^{sep}$  на  $K$ . Най-общо казано, алгебричната обвивка  $\overline{K}$  на  $K$  е единственото с точност до изоморфизъм алгебрично затворено разширение на  $K$ , което е алгебрично над  $K$ . Обединението на крайните сепарабелни разширения на  $K$ , съдържащи се в  $\overline{K}$  е подполе на  $\overline{K}$ , което се нарича сепарабелна обвивка на  $K$  в  $\overline{K}$  и се бележи с  $K^{sep}$ . Полетата, чиято сепарабелна обвивка  $K^{sep} = \overline{K}$  съпада с цялата алгебрична обвивка  $\overline{K}$  се наричат съвършени. Крайните полета  $\mathbb{F}_q$  са примери за съвършени полета  $\overline{\mathbb{F}_q} = \mathbb{F}_q^{sep}$  с абсолютна група на Galois, която е изоморфна на про-крайната обвивка  $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}_n$  на безкрайната циклична група  $(\mathbb{Z}, +)$ . А сега да преминем към последователно обяснение на гореспоменатите факти.

### 1. Сепарабелни разширения. Теорема за примитивния елемент

**ОПРЕДЕЛЕНИЕ 2.1.** *Полиномът  $f(x) \in K[x] \setminus K$  се нарича сепарабелен, ако няма кратни корени.*

*Ако  $F \supset K$  е разширение на полета, то елементът  $a \in F$  е сепарабелен над  $K$ , ако минималният му полином над  $K$  е сепарабелен.*

*Алгебрично разширение  $F \supset K$  е сепарабелно над  $K$ , ако всеки елемент на  $F$  е сепарабелен над  $K$ .*

Алгебричен над  $K$  елемент  $\alpha \in F$  е несепарабелен над  $K$  точно когато минималният полином  $f(x) \in K[x] \setminus K$  на  $\alpha$  над  $K$  има твържествено нулева формална производна. По-точно,  $f(x)$  има кратен корен тогава и само тогава, когато има общ корен с формалната си производна  $f'(x) \in K[x]$  или най-големият общ делител  $d(x) = (f(x), f'(x)) \neq k \in K^*$ . Съгласно неразложимостта на  $f(x)$  над  $K$ , имаме  $d(x) = k_o f(x)$  за някое  $k_o \in K^*$  и  $f(x)$  дели  $f'(x)$ . Понеже  $\deg(f'(x)) < \deg(f(x))$ , оттук следва  $f'(x) \equiv 0$  или

$$f(x) = \sum_s a_{ps} x^{ps} = \left( \sum_s \sqrt[p]{a_{ps}} x^s \right)^p \in K(\sqrt[p]{a_{ps}} | s)[x]$$

за краен брой естествени  $s$  и простото число  $p = char(K)$ . В частност, ако  $K$  е поле с характеристика  $char(K) = 0$ , то всеки алгебричен над  $K$  елемент  $\alpha \in F$  е сепарабелен над  $K$ .

Съществуват несепарабелни алгебрични разширения. Например, нека  $F = \mathbb{F}_p(x)$  е полето на рационалните функции на трансцендентна над  $\mathbb{F}_p$  променлива  $x$ . Множеството

$$F^p = \left\{ \frac{f^p(x)}{g^p(x)} \mid f(x), g(x) \in \mathbb{F}_p[x], g(x) \neq 0 \right\},$$

на  $p$ -тите степени на елементите на  $F$  е подполе на  $F$ . По-точно, за произволни

$$\frac{f_1(x)^p}{g_1(x)^p}, \frac{f_2(x)^p}{g_2(x)^p} \in F^p$$

с негъждествено нулеви  $g_1(x), f_2(x), g_2(x) \in \mathbb{F}_p[x]$  е изпълнено

$$\frac{f_1(x)^p}{g_1(x)^p} - \frac{f_2(x)^p}{g_2(x)^p} = \left( \frac{f_1(x)}{g_1(x)} - \frac{f_2(x)}{g_2(x)} \right)^p \in F^p,$$

$$\left( \frac{f_1(x)^p}{g_1(x)^p} \right) : \left( \frac{f_2(x)^p}{g_2(x)^p} \right) = \left( \frac{f_1(x)g_2(x)}{g_1(x)f_2(x)} \right)^p \in F^p.$$

Твърдим, че алгебричното разширение  $F \supset F^p$  не е сепарабелно. Например,  $x \in F$  не е сепарабелен над  $F^p$ . Нека  $f(y) \in F^p[y]$  е минималният полином на  $x \in F$  над  $F^p$ . Полиномът  $g(y) = y^p - x^p = (y - x)^p \in F^p[y]$  се дели на  $f(y)$ , защото  $g(x) = 0$ . Следователно  $f(y) = (y - x)^r$  за някое естествено  $1 \leq r \leq p$ . При  $r \geq 2$  полиномът  $f(y)$  не е сепарабелен над  $F^p$ , а оттам и елементът  $x \in F$  не е сепарабелен над  $F^p$ . В случая  $r = 1$  имаме  $x = \frac{h_1(x)^p}{h_2(x)^p} \in F^p$ , откъдето  $xh_2^p(x) = h_1^p(x)$  в пръстена  $\mathbb{F}_p[x]$  на полиномите на трансцендентна над  $\mathbb{F}_p$  променлива  $x$ . Сравняването на степените на двете страни дава  $1 + p \deg(h_2) = p \deg(h_1)$  с  $\deg(h_j) \in \mathbb{Z}$ ,  $\deg(h_j) \geq 0$  и изисква  $p$  да дели 1. Противоречието доказва, че  $f(y) = (y - x)^r$  с  $2 \leq r \leq p$  и  $x \in F$  не е сепарабелен над  $F^p$ .

**ТЕОРЕМА-ОПРЕДЕЛЕНИЕ 1.** (Теорема за примитивния елемент) (i) *Да предположим, че  $F \supset K$  е разширение на полета,  $\alpha \in F$  е алгебричен над  $K$  и  $\beta \in F$  е сепарабелен над  $K$ . Тогава съществува елемент  $\theta \in K(\alpha, \beta)$ , който поражда  $K(\alpha, \beta) = K(\theta)$  над  $K$ . Ако*

$$f_\alpha(x) = \prod_{i=1}^n (x - \alpha_i) \in K[x] \setminus K$$

*е минималният полином на  $\alpha = \alpha_1$  над  $K$ , а*

$$f_\beta(x) = \prod_{j=1}^m (x - \beta_j) \in K[x] \setminus K$$

*е минималният полином на  $\beta = \beta_1$  над  $K$ , то съществува  $\theta = \alpha + c\beta$  с  $c \in K$ , така че минималният полином  $f_\theta(x) \in K[x] \setminus K$  на  $\theta$  над  $K$  дели полинома*

$$g(x) := \prod_{j=1}^m f_\alpha(x - c\beta_j) \in K[x]$$

*и равенството  $f_\theta(x) \equiv g(x)$  е в сила тогава и само тогава, когато*

$$[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K].$$

(ii) *Нека  $F \supset K$  е разширение на полета,  $\alpha \in F$  и  $\beta \in F$  са сепарабелни над  $K$ . Тогава съществува сепарабелен над  $K$  елемент  $\theta \in K(\alpha, \beta)$ , който поражда  $K(\alpha, \beta) = K(\theta)$  над  $K$ .*

*Оттук, ако  $F \supset K$  е разширение на полета и  $a_1, \dots, a_m \in F$  са сепарабелни над  $K$ , то съществува сепарабелен над  $K$  елемент  $\theta \in K(a_1, \dots, a_m)$ , който поражда  $K(a_1, \dots, a_m) = K(\theta)$  над  $K$ .*

*Ако  $E = K(\theta)$ , то казваме, че  $\theta$  е примитивен елемент на  $E$  над  $K$ .*

**Доказателство:** (i) Ако  $K = \mathbb{F}_q$  е крайно поле, то крайно породеното разширение  $K(\alpha, \beta) \supset K$  на  $K$  чрез алгебрични над  $K$  елементи  $\alpha$  и  $\beta$  е крайно. За  $[K(\alpha, \beta) : K] = n \in \mathbb{N}$  полето  $K(\alpha, \beta)$  съдържа  $|K(\alpha, \beta)| = q^n$  елемента и е изоморфно на  $\mathbb{F}_{q^n}$ . Нека  $\mathbb{F}_p$  е простото подполе на  $\mathbb{F}_q$ , а  $\theta$  е пораждач на мултипликативната група  $\mathbb{F}_{q^n}^* = \langle \theta \rangle$  на  $\mathbb{F}_{q^n}$ . Тогава  $\mathbb{F}_{q^n} = \mathbb{F}_p(\theta) \subseteq \mathbb{F}_q(\theta)$ . От друга страна,  $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_{q^n}$ , защото  $\mathbb{F}_q$  е подполе на  $\mathbb{F}_{q^n}$  и  $\theta \in \mathbb{F}_{q^n}$ . Следователно  $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$ . Елементът  $\theta \in \mathbb{F}_{q^n}$  е корен на полинома  $g(x) = x^{q^n} - x \in \mathbb{F}_p[x] \subset \mathbb{F}_q[x]$ , който е сепарабелен съгласно  $g'(x) = -1 \neq 0$ . Минималният полином  $f_\theta(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$  на  $\theta$  над  $\mathbb{F}_q$  дели полинома  $g(x)$ . Оттук  $f_\theta(x)$  и  $\theta$  са сепарабелни.

Отсега нататък ще считаме, че  $K$  е безкрайно поле. Съгласно сепарабелността на  $\beta_1$ , минималният полином  $f_\beta(x) \in K[x] \setminus K$  на  $\beta$  над  $K$  има различни корени  $\beta_1, \dots, \beta_m$ . За произволни  $1 \leq i_1, i_2 \leq n$  и  $1 \leq j_1 \neq j_2 \leq m$  образуваме

$$\gamma_{(j_1, j_2)}^{(i_1, i_2)} := \frac{\alpha_{i_1} - \alpha_{i_2}}{\beta_{j_1} - \beta_{j_2}} \in K(\alpha, \beta)$$

и избираме

$$c \in K \setminus \left\{ \gamma_{(j_1, j_2)}^{(i_1, i_2)} \mid 1 \leq i_1, i_2 \leq n, 1 \leq j_1 \neq j_2 \leq m \right\}.$$

Елементите  $\gamma_{(j_1, j_2)}^{(i_1, i_2)} \in K(\alpha, \beta)$  са краен брой, така че безкрайността на полето  $K$  осигурява съществуването на  $c$ . Твърдим, че

$$\theta := \alpha + c\beta \in K(\alpha, \beta)$$

е примитивен елемент на  $K(\alpha, \beta)$  над  $K$ . Включването  $K(\theta) \subseteq K(\alpha, \beta)$  е ясно. За обратното включване да разгледаме най-големия общ делител

$$d(x) := (f_\alpha(\theta - cx), f_\beta(x))$$

на полиномите  $f_\alpha(\theta - cx), f_\beta(x) \in K(\theta)[x]$ . От една страна,  $d(x) \in K(\theta)[x]$  е полином с коефициенти от  $K(\theta)$ , защото може да се получи чрез последователни деления на полиноми от  $K(\theta)[x]$  по алгоритъма на Евклид. От друга страна, корените на  $d(x)$  са общите корени на  $f_\alpha(\theta - cx)$  и  $f_\beta(x)$ . Съгласно  $f_\alpha(\theta - c\beta_1) = f_\alpha(\alpha) = 0$  и  $f_\alpha(\theta - c\beta_j) = f_\alpha(\alpha_1 + c(\beta_1 - \beta_j)) \neq 0$  за  $\forall 2 \leq j \leq m$ ,  $\alpha_1 + c(\beta_1 - \beta_j) \notin \{\alpha, \alpha_2, \dots, \alpha_n\}$  имаме  $d(x) = a_o(x - \beta) \in K(\theta)[x]$  за някое  $a_o \in K(\theta)^*$ . Следователно  $\beta \in K(\theta)$  и  $\alpha = \theta - c\beta \in K(\theta)$ , откъдето  $K(\alpha, \beta) \subseteq K(\theta)$  и  $K(\alpha, \beta) = K(\theta)$ .

За да докажем, че минималният полином  $f_\theta(x) \in K[x] \setminus K$  на  $\theta$  над  $K$  дели полинома

$$g(x) := \prod_{j=1}^m f_\alpha(x - c\beta_j) \in K[x],$$

да забележим преди всичко, че полиномът  $g(x) \in K(\beta_1, \dots, \beta_m)[x]$  е с коефициенти от  $K$ , защото  $g(x)$  е симетричен полином на  $\beta_1, \dots, \beta_m$  и елементарните симетрични полиноми на  $\beta_1, \dots, \beta_m$  се различават евентуално само по знак от коефициентите на  $f_\beta(x) \in K[x]$ . От  $f_\alpha(\theta - c\beta_1) = f_\alpha(\alpha) = 0$  следва  $g(\theta) = 0$ , така че  $g(x) \in I(\theta) = \langle f_\theta(x) \rangle$  съгласно Твърдение 1.13(i). Полиномите  $f_\theta(x), g(x) \in K[x] \setminus K$  със старши коефициенти 1 съвпадат точно когато имат равни степени  $\deg(f_\theta) = mn$ .

(ii) За сепарабелността на примитивния елемент  $\theta$  на  $K(\alpha, \beta)$  над  $K$  е достатъчно да докажем, че ако  $f_\alpha(x)$  и  $f_\beta(x)$  нямат кратни корени, то и  $g(x) \in K[x]$  няма кратни корени. Тогава делителят  $f_\theta(x) \in K[x]$  на  $g(x)$  няма кратни корени и  $\theta$  е сепарабелен над  $K$ . Ако допуснем, че

$$g(x) = \prod_{i=1}^n \prod_{j=1}^m (x - \alpha_i - x\beta_j)$$

има кратен корен, то съществуват различни наредени двойки  $(i_1, j_1) \neq (i_2, j_2)$  с  $\alpha_{i_1} + c\beta_{j_1} = \alpha_{i_2} + c\beta_{j_2}$ . Ако  $j_1 = j_2$ , то  $\alpha_{i_1} = \alpha_{i_2}$ , откъдето  $i_1 = i_2$  и  $(i_1, j_1) = (i_2, j_2)$ , противно на избора на  $(i_1, j_1) \neq (i_2, j_2)$ . Следователно  $j_1 \neq j_2$  и  $c = \gamma_{(j_2, j_1)}^{(i_1, i_2)}$ , противно на избора на  $c$ . Това доказва, че полиномите  $g(x)$  и  $f_\theta(x)$  са сепарабелни и примитивният елемент  $\theta$  на  $K(\alpha, \beta) = K(\theta)$  над  $K$  е сепарабелен над полето  $K$ .

С индукция по  $i$  ще проверим, че ако  $a_1, \dots, a_i$  са сепарабелни над  $K$ , то съществува сепарабелен над  $K$ , примитивен елемент  $\theta_i$  на  $K(a_1, \dots, a_i) = K(\theta_i)$ .

Случаят  $i = 2$  е вече разгледан. Ако съществува сепарабелен над  $K$  примитивен елемент  $\theta_{i-1} \in K(a_1, \dots, a_{i-1})$  на  $K(a_1, \dots, a_{i-1}) = K(\theta_{i-1})$  над  $K$ , то  $K(a_1, \dots, a_{i-1}, a_i) = K(a_1, \dots, a_{i-1})(a_i) = K(\theta_{i-1}, a_i)$ . Прилагайки разсъжденията от случая  $i = 2$  получаваме съществуването на сепарабелен над  $K$  елемент  $\theta_i \in K(\theta_{i-1}, a_i)$ , така че  $K(\theta_{i-1}, a_i) = K(\theta_i)$ . Q.E.D.

**СЛЕДСТВИЕ 2.2.** *Ако  $K(\theta) \supset K$  е просто алгебрично разширение на  $K$  чрез сепарабелен над  $K$  елемент  $\theta$ , то всеки елемент  $\rho \in K(\theta)$  е сепарабелен над  $K$ , т.е.  $K(\theta) \supset K$  е сепарабелно разширение.*

**Доказателство:** Да допуснем, че съществува несепарабелен над  $K$  елемент  $\rho \in K(\theta)$ . Тогава минималният полином  $f_\rho(x) \in K[x] \setminus K$  на  $\rho = \rho_1$  над  $K$  е от вида  $f_\rho(x) = \prod_{i=1}^r (x - \rho_i)^{k_i}$  с  $k_i \in \mathbb{N}$  и поне едно  $k_{i_0} \geq 2$ . Степента на този полином  $k = \sum_{i=1}^r k_i = [K(\rho) : K]$  дели

$$n = [K(\theta) : K] = [K(\theta) : K(\rho)][K(\rho) : K] = k[K(\theta) : K(\rho)]$$

и минималният полином

$$g_\theta(\rho, x) \in K(\rho)[x] \setminus K(\rho) = \sum_{i=0}^m c_i x^i = \sum_{i=0}^m \sum_{j=0}^{k-1} c_{ij} \rho^j x^i \in K[\rho, x]$$

на  $\theta$  над  $K(\rho)$  е от степен  $m = \frac{n}{k} = [K(\theta) : K(\rho)]$  с  $c_{ij} \in K$ . Коефициентите на полинома

$$h(x) := \prod_{i=1}^r g_\theta(\rho_i, x)^{k_i}$$

са симетрични полиноми от корените на  $f_\rho(x)$ , броени с техните кратности. Следователно  $h(x) \in K[x]$ . Степента на  $h(x)$  е  $\deg(h) = mk = n = [K(\theta) : K]$ , а старшият коефициент е 1, така че  $h(x) \in K[x] \setminus K$  е минималният полином на  $\theta$  над  $K$ . По построение,  $h(x)$  има кратни корени, което противоречи на сепарабелността на  $\theta$  над  $K$ , Q.E.D.

**ЗАДАЧА 2.3.** *Да се намери примитивен елемент  $\theta$  за разширението*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q},$$

*както и минималният полином  $f_\theta(x) \in \mathbb{Q}[x] \setminus \mathbb{Q}$  на  $\theta$  над  $\mathbb{Q}$ .*

## 2. Група на Galois на разширение. Крайни разширения на Galois.

Преди да пристъпим към пресмятане на  $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$  да разгледаме групите на Galois на крайните разширения на Galois на поле  $K$ .

**ОПРЕДЕЛЕНИЕ 2.4.** *Взаимно-еднозначните хомоморфизми на пръстени  $g : F \rightarrow F$  се наричат автоморфизми на полето  $F$ .*

*Ако  $F \supset K$  е сепарабелно разширение на полето, то групата*

$$Aut(F/K) = \{g \in Aut(F) \mid g(\alpha) = \alpha, \forall \alpha \in K\}$$

*на автоморфизмите  $g : F \rightarrow F$  на полето  $F$ , които оставят на място всеки елемент на  $K$  се нарича група на Galois на  $F$  над  $K$ .*

Ако  $\alpha \in F$  е алгебричен над  $K$  и има минимален полином  $f(x) \in K[x] \setminus K$  над  $K$ , то  $\forall g \in Aut(F/K)$  изобразява  $\alpha$  в корен  $g(\alpha)$  на  $f(x) = 0$ .

Ако  $P$  е простото подполе на  $F$ , то  $Aut(F) = Gal(F/P)$ , защото единственият автоморфизъм на  $P$  е тъждественото изображение. По-точно, ако характеристиката на  $F$  е 0 и  $P \simeq \mathbb{Q}$ , то произволен автоморфизъм  $\varphi : P \rightarrow P$

изпълнява равенствата  $\varphi(0_P) = 0_P$  и  $\varphi(1_P) = 1_P$  за нулата  $0_P \in P$  и единицата  $1_P \in P$  на  $P$ . С индукция по  $n \in \mathbb{N}$ , от  $\varphi((n-1)1_P) = (n-1)1_P$  следва  $\varphi(n1_P) = \varphi((n-1)1_P + 1_P) = \varphi((n-1)1_P) + \varphi(1_P) = (n-1)1_P + 1_P = n1_P$ . Сега от  $\varphi((-n)1_P) = -\varphi(n1_P) = -(n1_P) = (-n)1_P$  за  $\forall n \in \mathbb{N}$  получаваме, че  $\varphi$  действа тъждествено върху подмножеството  $\mathbb{Z}1_P \subset P$ . Понеже  $P = \{(a1_P)(b1_P)^{-1} \mid a, b \in \mathbb{Z}, b \neq 0\}$  и  $[(a1_P)(b1_P)^{-1}](b1_P) = a1_P$ , оттук следва, че  $\varphi((a1_P)(b1_P)^{-1})b1_P = \varphi((a1_P)(b1_P)^{-1})\varphi(b1_P) = \varphi(a1_P) = a1_P$ , откъдето  $\varphi((a1_P)(b1_P)^{-1}) = (a1_P)(b1_P)^{-1}$ ,  $\varphi = \text{Id}_P$  и  $\text{Aut}(P) = \{\text{Id}_P\}$  за просто поле  $P \simeq \mathbb{Q}$  с характеристика 0. Ако характеристиката на  $P$  е просто число  $p$ , то  $P \simeq \mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$  и с индукция по  $1 \leq i \leq p-1$  проверяваме, че  $\varphi(\bar{i}) = \bar{i}$  за всеки автоморфизъм  $\varphi \in \text{Aut}(P)$ .

**ОПРЕДЕЛЕНИЕ 2.5.** Алгебричното разширение  $F \supset K$  е нормално, ако за  $\forall a \in F$  минималният полином  $f_a(x) \in K[x] \setminus K$  на  $a$  над  $K$  се разлага в линейни множители над  $F$ .

**ОПРЕДЕЛЕНИЕ 2.6.** Нормалните сепарабелни алгебрични разширения на полета  $F \supset K$  се наричат разширения на Galois.

**ОПРЕДЕЛЕНИЕ 2.7.** Нека  $F \supset K$  е разширение на полета. Елементите  $a, b \in F$  са спрегнати над  $K$ , ако имат един и същи минимален полином над  $K$ .

Лесно се вижда, че  $a$  и  $b$  са спрегнати над  $K$  тогава и само тогава, когато  $b$  е корен на минималния полином  $f_a(x) \in K[x] \setminus K$  на  $a$  над  $K$ . По-точно, ако  $f_a(b) = 0$ , то минималният полином  $f_b(x) \in K[x] \setminus K$  на  $b$  над  $K$  дели  $f_a(x)$  и  $f_a(x) = f_b(x)$  поради неразложимостта на  $f_a(x)$  над  $K$  и това, че  $f_a(x)$  и  $f_b(x)$  имат старши коефициент 1.

**ЛЕМА 2.8.** Нека  $K(\theta) \supset K$  е крайно просто разширение на Galois,  $\alpha = g(\theta) \in K(\theta) = K[\theta] = K + K\theta + \dots + K\theta^{n-1}$  за  $n = [K(\theta) : K]$ . Тогава следните условия са еквивалентни:

- (i)  $\alpha$  е спрегнат на  $\beta \in K(\theta)$  над  $K$ ;
- (ii)  $\beta = g(\theta_i)$  за някой корен  $\theta_i$  на минималния полином  $f_\theta(x) \in K[x]$  на  $\theta$  над  $K$ ;
- (iii)  $\beta = \varphi(\alpha)$  за някакъв елемент  $\varphi \in \text{Gal}(K(\theta)/K)$  на групата на Galois на  $K(\theta)$  над  $K$ .

**Доказателство:** (i)  $\Rightarrow$  (ii) Нека  $\theta_1 = \theta, \theta_2, \dots, \theta_n$  са всички различни корени на минималния полином  $f_\theta(x) \in K[x]$  на  $\theta$  над  $K$  от степен  $n = \deg f_\theta = [K(\theta) : K]$ . Твърдим, че полиномът

$$h(x) := \prod_{i=1}^n (x - g(\theta_i))$$

е с коефициенти от  $K$ . Наистина, коефициентите на  $h(x)$  са симетрични полиноми на  $\theta_1, \dots, \theta_n$ . Съгласно Основната теорема за симетричните полиноми и формулите на Виет за  $f_\theta(x)$ , коефициентите на  $h(x)$  са полиноми на коефициентите на  $f_\theta(x) \in K[x]$  с коефициенти от  $K$  и принадлежат на  $K$ . От  $h(\alpha) = h(g(\theta)) = 0$  следва, че минималният полином  $f_\alpha(x) \in K[x]$  на  $\alpha$  над  $K$  дели  $h(x)$ . Оттук, всеки спрегнат  $\beta$  на  $\alpha$  над  $K$  или всеки корен  $\beta$  на  $f_\alpha(x)$  е от вида  $\beta = g(\theta_i)$  за някакъв корен  $\theta_i$  на  $f_\theta(x)$ .

(ii)  $\Rightarrow$  (iii) Трябва да докажем съществуването на автоморфизъм

$$\varphi : K(\theta) = K + K\theta + \dots + K\theta^{n-1} \longrightarrow K + K\theta_i + \dots + K\theta_i^{n-1} = K(\theta_i) = K(\theta),$$

$$\varphi(k_0 + k_1\theta + \dots + k_{n-1}\theta^{n-1}) = k_0 + k_1\theta_i + \dots + k_{n-1}\theta_i^{n-1}$$

от групата на Galois  $\text{Gal}(K(\theta)/K)$ , трансформиращ  $\theta$  в  $\theta_i$ . За целта използваме, че разширението  $K(\theta) \supset K$  е нормално, така че  $\theta_i \in K(\theta)$  и  $K(\theta_i) \subseteq K(\theta)$ .

Поради своята неразложимост над  $K$ ,  $f_\theta(x) \in K[x]$  е минималният полином на  $\theta_i$  над  $K$  и

$$[K(\theta) : K(\theta_i)] = \frac{[K(\theta) : K]}{[K(\theta_i) : K]} = \frac{n}{n} = 1,$$

така че  $K(\theta_i) = K(\theta)$ . Мономите  $1, \theta, \dots, \theta^{n-1}$  образуват базис на  $n$ -мерното линейно пространство  $K(\theta)$  над  $K$ , както и мономите  $1, \theta_i, \dots, \theta_i^{n-1}$ . Следователно еднозначно определеното  $K$ -линейно изображение  $\varphi : K(\theta) \rightarrow K(\theta_i) = K(\theta)$ , трансформиращо базиса  $1, \theta, \dots, \theta^{n-1}$  на  $K(\theta)$  над  $K$  в базиса  $1, \theta_i, \dots, \theta_i^{n-1}$  на  $K(\theta)$  над  $K$  е  $K$ -линеен изоморфизъм. Остава да проверим, че  $\varphi$  е хомоморфизъм на пръстени, за да получим, че  $\varphi \in \text{Gal}(K(\theta)/K)$ . За целта да напомним, че елементите на  $K(\theta)$  имат еднозначно определени преставаания като полиноми на  $\theta$  от степен  $\leq n-1$ . За произволни  $g_1, g_2 \in K[x]$  от степен  $\deg g_1 \leq n-1$ ,  $\deg g_2 \leq n-1$  нека  $g_1 g_2 = f_\theta q + r$  е делението с частно  $q \in K[x]$  и остатък  $r \in K[x]$  от степен  $\deg r \leq n-1$ . Тогава  $g_1(\theta)g_2(\theta) = r(\theta)$  и формулата за умножение в  $K(\theta)$ . За произволен корен  $\theta_i$  на минималния полином  $f_\theta(x) \in K[x]$  на  $\theta$  над  $K$  имаме същата формула  $g_1(\theta_i)g_2(\theta_i) = r(\theta_i)$  за умножение в  $K(\theta_i) = K(\theta)$ . Следователно

$$\varphi(g_1(\theta)g_2(\theta)) = \varphi(r(\theta)) = r(\theta_i) = g_1(\theta_i)g_2(\theta_i) = \varphi(g_1(\theta))\varphi(g_2(\theta))$$

и  $\varphi : K(\theta) \rightarrow K(\theta_i) = K(\theta)$  е автоморфизъм от групата на Galois  $\text{Gal}(K(\theta)/K)$ .

(iii)  $\Rightarrow$  (i) Нека  $\beta = \varphi(\alpha)$  за някакво  $\varphi \in \text{Gal}(K(\theta)/K)$  и  $f_\alpha(x) = \sum_{i=0}^m a_i x^i \in K[x]$  е минималният полином на  $\alpha$  над  $K$ . Тогава

$$0 = \varphi(0) = \varphi(f_\alpha(\alpha)) = \varphi\left(\sum_{i=0}^m a_i \alpha^i\right) = \sum_{i=0}^m a_i \varphi(\alpha)^i = \sum_{i=0}^m a_i \beta^i = f_\alpha(\beta),$$

така че  $\beta$  е спрегнат на  $\alpha$  над  $K$ , Q.E.D.

**ТВЪРДЕНИЕ 2.9.** Ако  $F \supset K$  е крайно сепарабелно разширение с група на Galois  $\text{Gal}(F/K)$ , то

$$|\text{Gal}(F/K)| \leq [F : K]$$

с равенство  $|\text{Gal}(F/K)| = [F : K]$  тогава и само тогава, когато  $F \supset K$  е разширение на Galois.

**Доказателство:** Съгласно Теорема 1 за примитивния елемент, разширението  $F = K(\theta)$  е просто алгебрично. Следователно всеки елемент  $\varphi \in \text{Gal}(F/K)$  на групата на Galois се определя напълно от образа  $\varphi(\theta)$  на примитивния елемент  $\theta$  на  $F$  над  $K$ . Ако  $f_\theta(x) \in K[x]$  е минималният полином на  $\theta$  над  $K$ , то  $\varphi(\theta)$  е корен на  $f_\theta(x)$ , така че за  $\varphi(\theta)$  има най-много  $n = \deg(f_\theta) = [K(\theta) : K]$  възможности.

Ако разширението  $F = K(\theta) \supset K$  е нормално, то всички корени  $\theta_1 = \theta, \theta_2, \dots, \theta_n$  на минималния полином  $f_\theta(x) \in K[x]$  на  $\theta$  над  $K$  принадлежат на  $K(\theta)$  и за  $\forall 1 \leq i \leq n$  съществува автоморфизъм  $\varphi_i \in \text{Gal}(K(\theta)/K)$  с

$$\varphi_i(k_0 + k_1\theta + \dots + k_{n-1}\theta^{n-1}) = k_0 + k_1\theta_i + \dots + k_{n-1}\theta_i^{n-1}$$

за произволни  $k_0, \dots, k_{n-1} \in K$ . Това е установено в доказателството на импликацията (ii)  $\Rightarrow$  (iii) от Лема 2.8. Следователно  $|\text{Gal}(K(\theta)/K)| = [K(\theta) : K]$ , ако  $K(\theta) \supset K$  е крайно разширение на Galois.

Да допуснем, че  $|\text{Gal}(K(\theta)/K)| = [K(\theta) : K] = \deg f_\theta = n$ , но  $K(\theta) \subset K$  не е разширение на Galois. Тогава съществува елемент  $\alpha = g(\theta) \in K[\theta] = K(\theta)$  с  $g(x) \in K[x]$  от степен  $\deg g \leq n-1$  и с поне един спрегнат  $\beta \notin K(\theta)$ . В доказателството на (i)  $\Rightarrow$  (ii) от Лема 2.8 не използвахме нормалността на разширението  $K(\theta) \supset K$ . Следователно  $\beta = g(\theta_j)$  за някой корен  $\theta_j$  на минималния полином  $f_\theta(x) \in K[x]$  на  $\theta$  над  $K$ . Всеки автоморфизъм  $\psi \in \text{Gal}(K(\theta)/K)$  се

определя напълно от  $\psi(\theta) \in \{\theta_1 = \theta, \theta_2, \dots, \theta_n\}$ . Ако  $|Gal(K(\theta)/K)| = n$ , то за  $\forall 1 \leq i \leq n$  съществува  $\psi_i \in Gal(K(\theta)/K)$  с  $\psi_i(\theta) = \theta_i$ . Оттук,  $\theta_i \in K(\theta)$  за  $\forall 1 \leq i \leq n$  и  $\beta = g(\theta_j) \in K(\theta)$ , противно на допускането  $\beta \notin K(\theta)$ . Това доказва нормалността на крайното сепарабельно разширение  $K(\theta) \supset K$  при  $|Gal(K(\theta)/K)| = [K(\theta) : K]$ , Q.E.D.

**ЗАДАЧА 2.10.** Нека  $\zeta = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$  е примитивен трети корен на единицата.

Да се докаже, че:

(i) разширението  $\mathbb{Q}(\sqrt[3]{2}, \zeta)$  е линейно пространство над  $\mathbb{Q}$  с базис

$$1, \zeta, \sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{4}, \sqrt[3]{4}\zeta;$$

(ii) съществуват еднозначно определени елементи  $a \in Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}(\zeta))$  с  $a(\sqrt[3]{2}) = \sqrt[3]{2}\zeta$  и  $b \in Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}(\sqrt[3]{2}))$  с  $b(\zeta) = \zeta^2$ ;

(iii)  $Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}) = \langle a, b \mid a^3 = Id, b^2 = Id, bab^{-1} = a^{-1} \rangle \simeq S_3$ ;

(iv)  $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{Id\}$ .

**ЗАДАЧА 2.11.** Нека  $\zeta_5 = \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right) \in \mathbb{C}$  е примитивен пети корен на единицата. Да се докаже, че  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}$  и  $\mathbb{Q}(\zeta_5) \supset \mathbb{Q}$  са разширения на Galois с групи  $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$  и  $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq (\mathbb{Z}_4, +)$ .

**ЛЕМА 2.12.** Полето на разлагане  $K(\alpha_1, \dots, \alpha_m)$  на произволен сепарабелен полином  $f(x) \in K[x] \setminus K$  над  $K$  е крайно разширение на Galois.

**Доказателство:** Съгласно Теорема-Определение 1 и Твърдение 2.2, разширението  $K(\alpha_1, \dots, \alpha_m) \supset K$  чрез сепарабелни над  $K$  елементи  $\alpha_1, \dots, \alpha_m$  е сепарабелно над  $K$ . Достатъчно е да докажем, че

$$|Gal(K(\alpha_1, \dots, \alpha_m)/K)| = [K(\alpha_1, \dots, \alpha_m) : K],$$

за да приложим Твърдение 2.9 и да получим нормалността на разширението  $K(\alpha_1, \dots, \alpha_m) \supset K$ . За целта разглеждаме редицата от разширения

$$K \subset K(\alpha_1) \subset \dots \subset K(\alpha_1, \dots, \alpha_{i-1}) \subset K(\alpha_1, \dots, \alpha_{i-1}, \alpha_i) \subset \dots \subset K(\alpha_1, \dots, \alpha_m)$$

с  $m = \deg(f)$ . С индукция по  $1 \leq i \leq m$  ще докажем, че съществуват  $n_i = [K(\alpha_1, \dots, \alpha_i) : K]$  различни хомоморфизми на пръстени

$$\varphi : K(\alpha_1, \dots, \alpha_i) \longrightarrow K(\alpha_1, \dots, \alpha_m)$$

с  $\varphi|_K = Id_K$ . Всички такива  $\varphi$  са влагания, защото полето  $K(\alpha_1, \dots, \alpha_i)$  няма нетривиални идеали и  $\varphi|_K = Id_K$ . При  $i = m$  влаганията

$$\varphi : K(\alpha_1, \dots, \alpha_m) \rightarrow K(\alpha_1, \dots, \alpha_m)$$

са сюрективни. По-точно  $\varphi(\alpha_1), \dots, \varphi(\alpha_m)$  са  $m$  различни корена на сепарабелния полином  $f(x)$  от степен  $\deg(f) = m$ , така че  $\{\varphi(\alpha_1), \dots, \varphi(\alpha_m)\} = \{\alpha_1, \dots, \alpha_m\}$  и  $\varphi(K(\alpha_1, \dots, \alpha_m)) = K(\varphi(\alpha_1), \dots, \varphi(\alpha_m)) = K(\alpha_1, \dots, \alpha_m)$ . Автоморфизмите  $\varphi : K(\alpha_1, \dots, \alpha_m) \rightarrow K(\alpha_1, \dots, \alpha_m)$  с  $\varphi|_K = Id_K$  са елементите на групата на Galois  $Gal(K(\alpha_1, \dots, \alpha_m)/K)$ , така че оттук следва

$$|Gal(K(\alpha_1, \dots, \alpha_m)/K)| = n_m = [K(\alpha_1, \dots, \alpha_m) : K]$$

и  $K(\alpha_1, \dots, \alpha_m) \supset K$  е разширение на Galois.

Да проследим по-подробно разглежданията с индукция по  $1 \leq i \leq m$ . В случая  $i = 1$  нека  $f_1(x) \in K[x] \setminus K$  е минималният полином на  $\alpha_1$  над  $K$ . От  $f(\alpha_1) = 0$  следва, че  $f_1(x)$  дели  $f(x)$  и има  $n_1$  различни корена  $\alpha_{i_1}, \dots, \alpha_{i_{n_1}} \in \{\alpha_1, \dots, \alpha_m\}$ . Тогава за всяко  $1 \leq s \leq n_1$  съществува хомоморфизъм на пръстени  $\varphi : K(\alpha_1) \rightarrow K(\alpha_1, \dots, \alpha_m)$  с  $\varphi(\alpha_1) = \alpha_{j_s}$  и  $\varphi|_K = Id_K$ . Да допуснем, че съществуват  $n_i = [K(\alpha_1, \dots, \alpha_i) : K]$  различни хомоморфизми на пръстени  $\varphi : K(\alpha_1, \dots, \alpha_i) \rightarrow K(\alpha_1, \dots, \alpha_m)$  с  $\varphi|_K = Id_K$ . Ако  $\deg_{K(\alpha_1, \dots, \alpha_i)} \alpha_{i+1} =$

$[K(\alpha_1, \dots, \alpha_i, \alpha_{i+1}) : K(\alpha_1, \dots, \alpha_i)] = d_i$ , то минималният полином  $f_{i+1}(x) \in K(\alpha_1, \dots, \alpha_i)[x] \setminus K(\alpha_1, \dots, \alpha_i)$  на  $\alpha_{i+1}$  над  $K(\alpha_1, \dots, \alpha_i)$  е от степен  $d_i$  и

$$\begin{aligned} n_{i+1} &= [K(\alpha_1, \dots, \alpha_i, \alpha_{i+1}) : K] = \\ &= [K(\alpha_1, \dots, \alpha_i, \alpha_{i+1}) : K(\alpha_1, \dots, \alpha_i)][K(\alpha_1, \dots, \alpha_i) : K] = d_i n_i. \end{aligned}$$

Съгласно  $f(\alpha_{i+1}) = 0$  полиномът  $f_{i+1}(x)$  дели полинома  $f(x)$  над  $K(\alpha_1, \dots, \alpha_i)$  и  $f_{i+1}(x)$  има  $d_i$  различни корена  $\alpha_{j_s} \in \{\alpha_1, \dots, \alpha_m\}$ ,  $1 \leq s \leq d_i$ . Всеки хомоморфизъм на пръстени  $\varphi : K(\alpha_1, \dots, \alpha_i) \rightarrow K(\alpha_1, \dots, \alpha_m)$  се продължава до хомоморфизъм на пръстени

$$\psi : K(\alpha_1, \dots, \alpha_i, \alpha_{i+1}) = K(\alpha_1, \dots, \alpha_i)(\alpha_{i+1}) \longrightarrow K(\alpha_1, \dots, \alpha_m)$$

с  $\psi|_{K(\alpha_1, \dots, \alpha_i)} = \varphi$  и  $\psi(\alpha_{i+1}) = \alpha_{j_s}$  за някое  $1 \leq s \leq d_i$ . По индукционно предположение съществуват  $n_i$  различни хомоморфизми на пръстени  $\varphi : K(\alpha_1, \dots, \alpha_i) \rightarrow K(\alpha_1, \dots, \alpha_m)$  с  $\varphi|_K = \text{Id}_K$ . Всеки от тях има  $d_i$  различни продължения  $\psi : K(\alpha_1, \dots, \alpha_i, \alpha_{i+1}) \rightarrow K(\alpha_1, \dots, \alpha_m)$ , така че съществуват  $n_i d_i = n_{i+1}$  различни хомоморфизми на пръстени

$$\psi : K(\alpha_1, \dots, \alpha_i, \alpha_{i+1}) \longrightarrow K(\alpha_1, \dots, \alpha_m) \quad \text{с} \quad \psi|_K = \text{Id}_K.$$

При  $i = m$  получаваме наличието на  $n_m = [K(\alpha_1, \dots, \alpha_m) : K]$  различни хомоморфизми на пръстени  $\varphi : K(\alpha_1, \dots, \alpha_m) \rightarrow K(\alpha_1, \dots, \alpha_m)$  с  $\varphi|_K = \text{Id}_K$ , за които докажахме, че са автоморфизми от групата на Galois  $\text{Gal}(K(\alpha_1, \dots, \alpha_m)/K)$ , Q.E.D.

**ТВЪРДЕНИЕ 2.13.** Нека  $F \supset K$  е крайно разширение на Galois,  $F \supset E \supset K$ . Тогава:

- (i) произволен автоморфизъм  $f \in \text{Gal}(E/K)$  се продължава до автоморфизъм  $\varphi \in \text{Gal}(F/K)$ ;
- (ii) множеството

$$F^{\text{Gal}(F/K)} = \{a \in F \mid \psi(a) = a \quad \text{за} \quad \forall \psi \in \text{Gal}(F/K)\}$$

на фиксираните точки на  $\text{Gal}(F/K)$  от  $F$  съвпада с  $K$ .

**Доказателство:** (i) Разширението  $F \supset E$  е крайно и сепарабелно, защото минималният полином  $g_a(x) \in E[x]$  на произволен елемент  $a \in F$  над  $E$  дели минималния полином  $f_a(x) \in K[x]$  на  $a$  над  $K$  и разширението  $F \supset K$  е крайно и сепарабелно. Следователно съществува примитивен елемент  $\theta$  на  $F$  над  $E$  с минимален полином  $g_\theta(x) \in E[x]$  над  $E$  от степен  $\deg(g_\theta) = [F = E(\theta) : E] = n$ . Полиномът  $g_\theta(x)$  дели минималния полином  $f_\theta(x) \in K[x]$  на  $\theta$  над  $K$  и се разлага в линейни множители над  $F$ , съгласно нормалността на разширението  $F \supset K$ . За произволен корен  $\theta_2 \in F = E(\theta)$  на  $g_\theta(x)$ , изображението

$$\varphi : F = E(\theta) \longrightarrow E(\theta_2) \subseteq E(\theta),$$

$$\varphi \left( \sum_{i=0}^{n-1} e_i \theta^i \right) = \sum_{i=0}^{n-1} \varphi(e_i) \theta_2^i$$

е хомоморфизъм на пръстени, продължаващ  $\varphi \in \text{Gal}(E/K)$ . Ядрото на  $\varphi$  е  $\ker(\varphi) = \{0\}$ , така че  $\varphi : E(\theta) \rightarrow E(\theta_2)$  е изоморфизъм на пръстени. Елементите  $\theta$  и  $\theta_2$  имат един и същи минимален полином  $g_\theta(x) \in E[x]$  над  $E$ , така че  $[E(\theta_2) : E] = \deg(g_\theta) = [E(\theta) : E]$  и  $E(\theta_2) = E(\theta)$ . Това доказва взаимната еднозначност на  $\varphi : E(\theta) \rightarrow E(\theta)$  и  $\varphi \in \text{Gal}(F/K)$ .

(ii) Да допуснем, че съществува  $a \in F \setminus K$  с  $\psi(a) = a$  за  $\forall \psi \in \text{Gal}(F/K)$ . Ако  $E = K(a = a_1, \dots, a_m)$  е поето на разлагане на минималния полином  $f_a(x) \in K[x]$  на  $a$  над  $K$  и  $[K(a_1, \dots, a_{i-1}, a_i) : K(a_1, \dots, a_{i-1})] = d_i$  за  $\forall 1 \leq i \leq m$ , то групата на Galois  $\text{Gal}(E/K)$  има  $d_1 \dots d_m$  елемента, съгласно Лема 2.12. Доказателството на споменатата лема показва, че  $(d_1 - 1)d_2 \dots d_m$  от тях не



фиксираме  $a = a_1$ . Прилагаме (i) към произволен автоморфизъм  $f \in Gal(E/K)$  с  $f(a) \neq a$  и получаваме  $\varphi \in Gal(F/K)$  с  $\varphi(a) \neq a$ . Противоречието доказва, че  $F^{Gal(F/K)} = K$ .

Доказателството на (i)  $\Rightarrow$  (ii) от Лема 2.8 дава втори начин за установяване на включването  $F^{Gal(F/K)} \subseteq K$ . При допускане на обратното съществува  $\alpha \in F^{Gal(F/K)} \setminus K$ . Минималният полином  $f_\alpha(x) \in K[x]$  на  $\alpha$  над  $K$  е от степен  $\deg f_\alpha \geq 2$  и има поне един корен  $\alpha_2 \neq \alpha$ . Ако  $\theta$  е примитивен елемент на  $F = K(\theta)$  над  $K$ , то  $\alpha = g(\theta)$  за полином  $g(x) \in K[x]$ ,  $\deg g < [K(\theta) : K]$  и спрегнатият  $\alpha_2$  на  $\alpha$  над  $K$  е от вида  $\alpha_2 = g(\theta_2)$  за някой корен  $\theta_2 \neq \theta$  на минималния полином  $f_\theta(x) \in K[x]$  на  $\theta$  над  $K$ . Разширението  $K(\theta) \supset K$  е нормално, така че  $\theta_2 \in K(\theta)$  и съществува  $\varphi \in Gal(K(\theta)/K)$  с  $\varphi(\theta) = \theta_2$ . Но тогава

$$\varphi(\alpha) = \varphi(g(\theta)) = g(\varphi(\theta)) = g(\theta_2) \neq g(\theta) = \alpha$$

противоречи на избора на  $\alpha \in F^{Gal(F/K)}$  и доказва, че  $F^{Gal(F/K)} = K$ , Q.E.D.

**ТВЪРДЕНИЕ 2.14.** *Всяко крайно разширение  $\mathbb{F}_{q^m} \supset \mathbb{F}_q$  на крайни полета е разширение на Galois с циклична група*

$$Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \Phi_q \rangle \simeq (\mathbb{Z}_m, +)$$

от ред  $m$ , породена от автоморфизма на Frobenius

$$\Phi_q : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m},$$

$$\Phi_q(x) = x^q \quad \text{за} \quad \forall x \in \mathbb{F}_{q^m}.$$

**Доказателство:** Съгласно Следствие 1.25, всеки пораждащ  $\alpha$  на мултипликативната група  $\mathbb{F}_{q^m}^*$  на  $\mathbb{F}_{q^m}$  е примитивен елемент на  $\mathbb{F}_{q^m} = \mathbb{F}_p(\alpha)$  над простото подполе  $\mathbb{F}_p \subseteq \mathbb{F}_q \subset \mathbb{F}_{q^m}$ . От  $\mathbb{F}_{q^m} = \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^m}$  се вижда, че  $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$  и  $\alpha$  е примитивен елемент на  $\mathbb{F}_{q^m}$  над  $\mathbb{F}_q$ . Минималният полином  $f_\alpha(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$  на  $\alpha$  над  $\mathbb{F}_q$  дели сепарабелния полином  $x^{q^m} - x \in \mathbb{F}_q[x]$  с корен  $\alpha$ , така че  $f_\alpha(x)$  няма кратни корени и  $\alpha$  е сепарабелен над  $\mathbb{F}_q$ . Съгласно Твърдение 2.2, разширението  $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) \supset \mathbb{F}_q$  е сепарабелно. Всички корени на  $x^{q^m} - x$  принадлежат на  $\mathbb{F}_{q^m}$ , така че и всички корени на  $f_\alpha(x)$  са в  $\mathbb{F}_{q^m}$  и  $\mathbb{F}_{q^m} \supset \mathbb{F}_q$  е нормално разширение. Това доказва, че всяко крайно разширение  $\mathbb{F}_{q^m} \supset \mathbb{F}_q$  на крайни полета е разширение на Galois.

ТВЪРДИМ, че  $\Phi_q : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ ,  $\Phi_q(x) = x^q$  за  $\forall x \in \mathbb{F}_{q^m}$  е автоморфизъм на полето  $\mathbb{F}_{q^m}$ . Наистина, допускането  $\alpha^q = \Phi_q(\alpha) = \Phi_q(\beta) = \beta^q$  за  $q = p^n$ ,  $p = char(\mathbb{F}_q) = char(\mathbb{F}_{q^m})$ ,  $n \in \mathbb{N}$  води до  $0 = \alpha^q - \beta^q = (\alpha - \beta)^q$ , откъдето  $\alpha = \beta$ . Следователно  $\Phi_q(\alpha) \neq \Phi_q(\beta)$  за различни  $\alpha, \beta \in \mathbb{F}_{q^m}$  и  $\Phi_q : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$  е взаимно-еднозначно изображение. Съгласно

$$\Phi_q(\alpha + \beta) = (\alpha + \beta)^q = \alpha^q + \beta^q = \Phi_q(\alpha) + \Phi_q(\beta) \quad \text{и}$$

$$\Phi_q(\alpha\beta) = (\alpha\beta)^q = \alpha^q\beta^q = \Phi_q(\alpha)\Phi_q(\beta) \quad \text{за} \quad \forall \alpha, \beta \in \mathbb{F}_{q^m},$$

изображението  $\Phi_q$  е хомоморфизъм, а оттам и автоморфизъм на  $\mathbb{F}_{q^m}$ .

За  $\forall a \in \mathbb{F}_q$  е в сила  $a^q = a$ , така че  $\Phi_q(a) = a$  и  $\Phi_q \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ .

ТВЪРДИМ, че  $\Phi_q$  е елемент от ред  $m$  на групата на Galois  $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ , защото  $(\Phi_q)^m = \Phi_{q^m}$  действа тъждествено върху  $\mathbb{F}_{q^m}$  и  $(\Phi_q)^r = \Phi_{q^r} \neq Id_{\mathbb{F}_{q^m}}$  за  $\forall r \in \mathbb{N}$ ,  $1 \leq r \leq m - 1$ .

Следователно  $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$  съдържа цикличната група  $\langle \Phi_q \rangle \simeq (\mathbb{Z}_m, +)$  и редът на групата на Galois е  $|Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)| \geq m$ . Да напомним, че произволен пораждащ  $\alpha$  на  $\mathbb{F}_{q^m}^*$  е примитивен елемент на  $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$  над  $\mathbb{F}_q$  от степен  $m$ . Ако  $\alpha = \alpha_1, \dots, \alpha_m$  са корените на минималния полином на  $\alpha$  над  $\mathbb{F}_q$ , то произволен елемент  $\varphi \in Gal(\mathbb{F}_q(\alpha)/\mathbb{F}_q)$  се определя еднозначно от  $\varphi(\alpha) \in \{\alpha = \alpha_1, \alpha_2, \dots, \alpha_m\}$ , така че  $|Gal(\mathbb{F}_q(\alpha)/\mathbb{F}_q)| \leq m$ . В резултат,

$|Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)| = m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$  и сепарабелното разширение  $\mathbb{F}_{q^m} \supset \mathbb{F}_q$  е нормално, Q.E.D.

**ЗАДАЧА 2.15.** Нека  $\alpha_j$ ,  $1 \leq j \leq 2$  са пораждащи на мултипликативната група  $\mathbb{F}_9^*$  на полето  $\mathbb{F}_9 = \{a + b\alpha_j \mid a, b \in \mathbb{F}_3\}$  с 9 елемента, които имат минимални полиноми

$$f_1(x) = x^2 - x - 1, \quad \text{съответно,} \quad f_2(x) = x^2 + x - 1$$

над  $\mathbb{F}_3$ . Да се намерят орбитите

$$Orb_G(1 + \alpha_j) = \{g(1 + \alpha_j) \mid g \in G\}$$

на  $1 + \alpha_j$  под действие на групата на Galois  $G = Gal(\mathbb{F}_9/\mathbb{F}_3) = \langle \Phi_3 \rangle \simeq (\mathbb{Z}_2, +)$ .

### 3. Алгебрична и сепарабелна обвивка на поле

Да напомним накратко конструкцията на алгебрична обвивка  $\overline{K}$  на поле  $K$ . Започваме с построение на разширение  $L_1 \supset K$ , в което  $\forall f(x) \in K[x] \setminus K$  има корен. По-точно, на всеки полином  $f(x) \in K[x] \setminus K$  съпоставяме променлива  $x_f$  и означаваме с  $X$  обединението на всички  $x_f$ . В пръстена на полиномите  $K[X]$  разглеждаме идеала  $I$ , породен от  $f(x_f)$  за  $\forall f(x) \in K[x] \setminus K$ . Този идеал е собствен, защото в противен случай съществуват  $f_1, \dots, f_n, f_{n+1}, \dots, f_m \in K[x] \setminus K$ , така че

$$f_1(x_{f_1})g_1(x_{f_1}, \dots, x_{f_m}) + \dots + f_n(x_{f_n})g_n(x_{f_1}, \dots, x_{f_m}) = 1. \quad (2.1)$$

В полето на разлагане на  $f_1(x_{f_1}) \dots f_n(x_{f_n})$  над  $K$  избираме корени  $\alpha_i$  на  $f_i$  и заместваем  $x_{f_i} = \alpha_i$  в (2.1). Това дава  $0 = 1$ , което е противоречие, доказващо  $I \neq K[X]$ . За произволен максимален идеал  $\mathfrak{M} \triangleleft K[X]$ , съдържащ  $I$ , полето

$$K[X]/\mathfrak{M} = (K + \mathfrak{M}/\mathfrak{M})[X + \mathfrak{M}] \simeq (K/K \cap \mathfrak{M})[X + \mathfrak{M}] = K[X + \mathfrak{M}],$$

съдържа подполе, изоморфно на  $K$ . В резултат,  $L_1 = K[X]/\mathfrak{M} \supset K$  е разширение, в което  $\forall f(x) \in K[x] \setminus K$  има корен  $x_f + \mathfrak{M}$ . По-точно  $f(x_f + \mathfrak{M}) = f(x_f) + \mathfrak{M}$ , съгласно правилата за събиране и умножение във фактор-пръстена  $L_1 = K[X]/\mathfrak{M}$ . Но  $f(x_f) \in I \subseteq \mathfrak{M}$ , така че  $f(x_f) + \mathfrak{M} = \mathfrak{M}$ .

Продължаваме по същия начин, като за всяко естествено  $n$  избираме  $L_n$  да е разширение на  $L_{n-1}$ , в което всеки полином  $f(x) \in L_{n-1}[x] \setminus L_{n-1}$  има корен. Обединението  $L = \cup_{n=1}^{\infty} L_n$  на редицата

$$K \subset L_1 \subset L_2 \subset \dots \subset L_{n-1} \subset L_n \subset \dots$$

е поле, защото ако  $\alpha, \beta \in L$ ,  $\beta \neq 0$ , то  $\alpha \in L_m$ ,  $\beta \in L_n$  за някои  $m, n \in \mathbb{N}$ . Ако  $k = \max(m, n)$ , то  $\alpha, \beta \in L_k$ , така че  $\alpha - \beta, \frac{\alpha}{\beta} \in L_k \subset L$ . Полето  $L$  е алгебрично затворено, т.е. всеки полином  $f(x) \in L[x] \setminus L$  има корен в  $L$ . По-точно, ако  $f(x) = \sum_{i=0}^m c_i x^i \in L[x] \setminus L$  и  $c_i \in L_{n_i}$ , то за  $n = \max(n_0, \dots, n_m)$  имаме  $f(x) \in L_n[x] \setminus L_n$ , така че  $f(x)$  има корен в  $L_{n+1} \subset L$ .

Обединението  $\overline{K}$  на алгебричните над  $K$  елементи на  $L$  образува подполе на  $L$ , защото за  $\forall \alpha, \beta \in \overline{K}$ ,  $\beta \neq 0$  крайно породеното разширение  $K(\alpha, \beta) \supset K$  чрез алгебрични над  $K$  елементи  $\alpha$  и  $\beta$  е крайно. Съгласно  $\alpha - \beta, \frac{\alpha}{\beta} \in K(\alpha, \beta)$  имаме  $[K(\alpha - \beta) : K] < \infty$ ,  $[K(\frac{\alpha}{\beta}) : K] < \infty$ , откъдето  $\alpha - \beta, \frac{\alpha}{\beta} \in \overline{K}$ . Подполето  $\overline{K} \subseteq L$  е алгебрично затворено. Достатъчно е да проверим, че корените  $\alpha \in L$  на полиноми  $f(x) = \sum_{i=0}^n a_i x^i \in \overline{K}[x] \setminus \overline{K}$  са алгебрични над  $K$ . Наистина,  $\alpha$  е алгебричен над полето  $K(a_0, \dots, a_n)$ . Крайно породеното алгебрично разширение  $K(a_0, \dots, a_n) \supset K$  е крайно, така че

$$[K(a_0, \dots, a_n, \alpha) : K] = [K(a_0, \dots, a_n, \alpha) : K(a_0, \dots, a_n)][K(a_0, \dots, a_n) : K] < \infty$$

и  $[K(\alpha) : K] \leq [K(a_0, \dots, a_n, \alpha) : K] < \infty$ . Оттук  $\alpha$  е алгебрично над  $K$  и  $\alpha \in \overline{K}$ . Алгебрично затворено алгебрично разширение  $\overline{K} \supset K$  се нарича алгебрична обвивка на  $K$ .

**ЛЕМА 2.16.** *Нека  $L$  и  $L'$  са алгебрично затворени полета, съдържащи  $K$  и построени както е описано по-горе, а  $\overline{K} \subset L$  и  $\overline{K}' \subset L'$  са алгебричните обвивки на  $K$  в  $L$  и  $L'$ . Тогава съществува изоморфизъм на пръстени*

$$\varphi : \overline{K} \longrightarrow \overline{K}',$$

който се ограничава до  $\varphi|_K = \text{Id}_K$ .

**Доказателство:** Посредством Лемата на Цорн ще установим съществуването на хомоморфизъм на пръстени  $\varphi : \overline{K} \rightarrow \overline{K}'$ . За целта разглеждаме множеството  $\Sigma$  на наредените двойки  $(F, \varphi_F)$ , където  $K \subset F \subseteq \overline{K}$  е подполе на  $\overline{K}$ , съдържащо  $K$ , а  $\varphi_F : F \rightarrow \overline{K}'$  е хомоморфизъм на пръстени с  $\varphi_F|_K = \text{Id}_K$ . Въвеждаме частична наредба в  $\Sigma$ , постулирайки  $(F_1, \varphi_{F_1}) \leq (F_2, \varphi_{F_2})$ , ако  $F_1 \subseteq F_2$  и  $\varphi_{F_2}|_{F_1} = \varphi_{F_1}$ . Всяко линейно наредено подмножество  $\{(F_\alpha, \varphi_{F_\alpha})\}_{\alpha \in A} \subseteq \Sigma$  има точна горна граница  $(F := \cup_{\alpha \in A} F_\alpha, \varphi_F)$  с  $\varphi_F(\lambda_\alpha) := \varphi_{F_\alpha}(\lambda_\alpha)$  за  $\forall \lambda_\alpha \in F_\alpha$ . Ако  $\lambda_\alpha \in F_\alpha \cap F_\beta$ , то  $(F_\alpha, \varphi_{F_\alpha}) \leq (F_\beta, \varphi_{F_\beta})$  след евентуална размяна на  $(F_\alpha, \varphi_{F_\alpha})$  с  $(F_\beta, \varphi_{F_\beta})$ , съгласно линейната нареденост на  $\{(F_\alpha, \varphi_{F_\alpha})\}_{\alpha \in A}$ . Следователно  $\varphi_{F_\beta}(\lambda_\alpha) = \varphi_{F_\alpha}(\lambda_\alpha)$  и  $\varphi_F : F \rightarrow \overline{K}'$  е коректно зададен хомоморфизъм на пръстени. По Лемата на Цорн съществува максимален елемент  $(E, \varphi_E) \in \Sigma$ . Ако  $E \subsetneq \overline{K}$ , то съществува  $\alpha \in \overline{K} \setminus E$ . Елементът  $\alpha$  е алгебричен над  $K$  и минималният му полином  $f_\alpha(x) \in K[x] \setminus K$  на  $\alpha$  над  $K$  има различни корени  $\alpha = \alpha_1, \dots, \alpha_m \in \overline{K}$ . Нека  $\alpha'_1, \dots, \alpha'_n \in \overline{K}'$  са различните корени на  $f_\alpha(x)$  в  $\overline{K}'$ . От  $K \subseteq E$  следва, че  $\alpha$  е алгебричен над  $E$  и минималният полином  $g_\alpha(x) \in E[x] \setminus E$  на  $\alpha$  над  $E$  дели  $f_\alpha(x)$  в  $E[x]$ , т.е.  $f_\alpha(x) = g_\alpha(x)h_\alpha(x)$  за  $h_\alpha(x) \in E[x]$ . Хомоморфизмът  $\varphi_E : E \rightarrow \overline{K}'$  има  $\ker \varphi_E = \{0\}$  т.к.  $\varphi_E|_K = \text{Id}_K$  и може да се разглежда като изоморфизъм на полета  $\varphi_E : E \rightarrow \varphi_E(E)$ . Продължаваме  $\varphi_E$  до хомоморфизъм

$$\begin{aligned} \varphi_E : E[x] &\longrightarrow \varphi_E(E)[x], \\ \varphi_E \left( \sum_{i=0}^s e_i x^i \right) &:= \sum_{i=0}^s \varphi_E(e_i) x^i \end{aligned}$$

на съответните полиномиални пръстени. Тогава  $f_\alpha = \varphi_E(f_\alpha) = \varphi_E(g_\alpha)\varphi_E(h_\alpha)$  и различните корени  $\alpha'_1, \dots, \alpha'_r$  на  $\varphi_E(g_\alpha)$  в  $\overline{K}'$  се съдържат в различните корени  $\{\alpha'_1, \dots, \alpha'_n\}$  на  $f_\alpha$  в  $\overline{K}'$ . Изображението

$$\varphi' : E(\alpha) = E[\alpha] \longrightarrow \varphi_E(E)[\alpha'_1] = \varphi_E(E)(\alpha'_1)$$

е хомоморфизъм на пръстени, продължаващ  $\varphi_E$  върху подполето  $K \subseteq E(\alpha) \subseteq \overline{K}$ . Това противоречи на максималността на  $(E, \varphi_E) \in \Sigma$  и доказва, че  $E = \overline{K}$ . Хомоморфизмът  $\varphi : \overline{K} \rightarrow \overline{K}'$  с ядро  $\ker \varphi = \{0\}$  задава изоморфизъм на полета  $\varphi : \overline{K} \rightarrow \varphi(\overline{K})$  и има обратен  $\varphi^{-1} : \varphi(\overline{K}) \rightarrow \overline{K}$ . Да допуснем, че съществува  $\alpha' \in \overline{K}' \setminus \varphi(\overline{K})$ . Тогава  $\alpha'$  е алгебричен над  $K$  и минималният му полином  $f_{\alpha'}(x) \in K[x] \setminus K$  има корени  $\alpha' = \alpha'_1, \dots, \alpha'_n \in \overline{K}'$ , броени без кратности. Нека  $\alpha_1, \dots, \alpha_m \in \overline{K}$  са различните корени на  $f_{\alpha'}(x)$  в  $\overline{K}$ . Елементът  $\alpha'$  е алгебричен над  $\varphi(\overline{K})$  и минималният му полином  $g_{\alpha'}(x) \in \varphi(\overline{K})[x] \setminus \varphi(\overline{K})$  над  $\varphi(\overline{K})$  е от степен  $\deg g_{\alpha'}(x) \geq 2$ , защото  $\alpha' \notin \varphi(\overline{K})$ . Разлагаме  $f_{\alpha'}(x) = g_{\alpha'} h_{\alpha'}(x)$  с  $h_{\alpha'}(x) \in \varphi(\overline{K})[x]$  и забелязваме, че

$$f_{\alpha'} = \varphi^{-1}(f_{\alpha'}) = \varphi^{-1}(g_{\alpha'})\varphi^{-1}(h_{\alpha'})$$

с  $\varphi^{-1}(g_{\alpha'}), \varphi^{-1}(h_{\alpha'}) \in \overline{K}[x]$ . Но тогава  $\varphi^{-1}(g_{\alpha'})$  се разлага в линейни множители над  $\overline{K}$  поради алгебричната затвореност на  $\overline{K}$  и  $\varphi^{-1}(g_{\alpha'})$  има корен  $\alpha \in \overline{K}$ . Действайки с  $\varphi$  върху  $\varphi^{-1}(g_{\alpha'})$  ( $\alpha = 0$ ) получаваме

$$g_{\alpha'}(\varphi(\alpha)) = \varphi(\varphi^{-1}(g_{\alpha'})(\alpha)) = \varphi(0) = 0,$$

така че  $g_{\alpha'}(x) \in \varphi(\overline{K})[x]$  има корен в  $\varphi(\overline{K})$  и  $g_{\alpha'}(x) \in \varphi(\overline{K})[x]$  е разложим над  $\varphi(\overline{K})$ . Противоречието доказва, че  $\varphi(\overline{K}) = \overline{K}'$  и  $\varphi : \overline{K} \rightarrow \overline{K}'$  е изоморфизъм на полета, Q.E.D.

**ЛЕМА-ОПРЕДЕЛЕНИЕ 2.17.** (i) Множеството  $K^{sep}$  на сепарабелните над  $K$  елементи на алгебричната обвивка  $\overline{K}$  е подполе на  $\overline{K}$ , което се нарича сепарабелна обвивка на  $K$  (в  $\overline{K}$ ).

(ii) Сепарабелната обвивка  $K^{sep} = \cup_{F \supset K} F$  съвпада с обединението на всички крайни сепарабелни разширения  $F \supset K$ .

**Доказателство:** (i) Достатъчно е да отбележим, че за произволни  $\alpha, \beta \in K^{sep} \subseteq \overline{K}$ ,  $\beta \neq 0$ , елементите  $\alpha - \beta, \frac{\alpha}{\beta} \in \overline{K}$  са сепарабелни над  $K$ . Съгласно Теорема 1 за примитивния елемент, съществува сепарабелен примитивен елемент на  $K(\alpha, \beta) = K(\theta)$  над  $K$ . Прилагаме Лема 2.2 към  $\alpha - \beta, \frac{\alpha}{\beta} \in K(\alpha, \beta) = K(\theta)$  и получаваме, че множеството  $K^{sep}$  на сепарабелните над  $K$  елементи на  $\overline{K}$  е подполе на  $\overline{K}$ .

(ii) Ако  $\alpha \in \overline{K}$  е сепарабелен над  $K$ , то  $K(\alpha) \supset K$  е крайно сепарабелно разширение, така че  $K^{sep} \subseteq \cup_{F \supset K} F$ . По определение, ако  $F \supset K$  е крайно сепарабелно разширение, то  $\forall x \in F$  е сепарабелно над  $K$ , откъдето  $\cup_{F \supset K} F \subseteq K^{sep}$  и  $\cup_{F \supset K} F = K^{sep}$ , Q.E.D.

**ТЕОРЕМА 3.** Алгебричната обвивка  $\overline{\mathbb{F}_q}$  на крайно поле  $\mathbb{F}_q$  съвпада със сепарабелната обвивка  $\mathbb{F}_q^{sep}$  на  $\mathbb{F}_q$  и е равна на обединението  $\overline{\mathbb{F}_q} = \cup_{n=1}^{\infty} \mathbb{F}_{q^n}$  на всички крайни полета, съдържащи  $\mathbb{F}_q$ , т.е.

$$\overline{\mathbb{F}_q} = \cup_{n=1}^{\infty} \mathbb{F}_{q^n} = \mathbb{F}_q^{sep}.$$

**Доказателство:** Включването  $\overline{\mathbb{F}_q} \subseteq \cup_{n=1}^{\infty} \mathbb{F}_{q^n}$  следва от това, че  $\forall \alpha \in \overline{\mathbb{F}_q}$  е алгебрично над  $\mathbb{F}_q$ . Ако  $\deg_{\mathbb{F}_q} \alpha = n$ , то  $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$ , така че  $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$  и  $\alpha \in \mathbb{F}_{q^n}$ . За  $\cup_{n=1}^{\infty} \mathbb{F}_{q^n} \subseteq \mathbb{F}_q^{sep}$  използваме, че всяко крайно разширение  $\mathbb{F}_{q^n} \supset \mathbb{F}_q$  е сепарабелно, така че се съдържа в сепарабелната обвивка  $\mathbb{F}_q^{sep}$  на  $\mathbb{F}_q$ . Това дава  $\overline{\mathbb{F}_q} \subseteq \cup_{n=1}^{\infty} \mathbb{F}_{q^n} \subseteq \mathbb{F}_q^{sep}$ . Комбинирайки с  $\mathbb{F}_q^{sep} \subseteq \overline{\mathbb{F}_q}$  получаваме равенствата  $\overline{\mathbb{F}_q} = \cup_{n=1}^{\infty} \mathbb{F}_{q^n} = \mathbb{F}_q^{sep}$ , Q.E.D.

Като непосредствено следствие от Теорема 3 получаваме, че алгебричната обвивка  $\overline{\mathbb{F}_p}$  на крайно поле  $\mathbb{F}_p$  съвпада с алгебричната обвивка  $\overline{\mathbb{F}_p}$  на простото подполе  $\mathbb{F}_p$ . По-точно, теоремата дава

$$\overline{\mathbb{F}_p} = \cup_{m=1}^{\infty} \mathbb{F}_{p^{m^n}} \subseteq \cup_{m=1}^{\infty} \mathbb{F}_{p^m} = \overline{\mathbb{F}_p}.$$

Всеки елемент  $\alpha \in \overline{\mathbb{F}_p}$  е алгебричен над  $\mathbb{F}_p$ , а оттам и над  $\mathbb{F}_{p^n}$ . Следователно  $\overline{\mathbb{F}_p} \subseteq \overline{\mathbb{F}_{p^n}}$  и  $\overline{\mathbb{F}_p} = \overline{\mathbb{F}_{p^n}}$ .

#### 4. Абсолютна група на Galois на поле

Съгласно Лема-Определение 2.17 (ii), можем да разглеждаме сепарабелната обвивка  $K^{sep} \supset K$  като "граница" на крайните сепарабелни разширения  $F \supset K$ . Затова абсолютната група на Galois  $Gal(K^{sep}/K)$  на  $K$  е проективна граница на групите на Galois  $Gal(F/K)$  на крайните сепарабелни нормални разширения  $F \supset K$ . За да прецизираме това твърдение чрез проективни граници на крайни групи (т.е. про-крайни групи), трябва да напомним няколко определения.

Частична наредба  $\leq$  в множество  $I$  е релация  $i \leq j$  между някои двойки  $i, j \in I$  със свойствата:

- (i) рефлексивност -  $i \leq i$  за  $\forall i \in I$ ;
- (ii) анти-симетричност - ако  $i \leq j$  и  $j \leq i$ , то  $i = j$ ;
- (iii) транзитивност - от  $i \leq j$  и  $j \leq k$  следва  $i \leq k$ .

Нека  $m \leq n$  за  $m, n \in \mathbb{N}$ , ако  $m$  дели  $n$ . Тогава " $\leq$ " е частична наредба в множеството  $\mathbb{N}$  на естествените числа.

**ОПРЕДЕЛЕНИЕ 2.18.** Частично нареденото множество  $I$  е насочена система, ако за произволни  $i, j \in I$  съществува  $k \in I$ , така че  $i \leq k$  и  $j \leq k$ .

Множеството  $\mathbb{N}$  на естествените числа е насочена система относно частичната наредба " $\leq$ ", защото за произволни  $m, n \in \mathbb{N}$ , най-малкото общо кратно  $\mu = LCM(m, n) \in \mathbb{N}$  се дели на  $m$  и на  $n$ .

**ОПРЕДЕЛЕНИЕ 2.19.** Проективна система от групи е фамилия  $\{G_i\}_{i \in I}$  от групи  $G_i$ , индексирани с насочена система  $I$  и фамилия от епиморфизми

$\varphi_i^j : G_j \rightarrow G_i$  за  $\forall j \geq i$ , така че

- (i)  $\varphi_i^i = \text{Id}_{G_i}$  за  $\forall i \in I$ ;
- (ii)  $\varphi_i^j \varphi_j^k = \varphi_i^k$  за  $\forall k \geq j \geq i$ .

Проективната граница  $\varprojlim G_i$  е подгрупата на директното произведение  $\prod_{i \in I} G_i$ ,

съставена от съгласуваните чрез  $\varphi_i^j$  елементи,

$$\varprojlim G_i = \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \mid g_i = \varphi_i^j(g_j) \quad \text{за} \quad \forall i \leq j \right\}.$$

Твърдим, че проекциите  $\pi_i : \varprojlim G_i \rightarrow G_i$ ,  $\pi_i(g_s)_{s \in I} = g_i$  са епиморфизми. Наистина, за  $\forall g_i \in G_i$  и  $\forall j \in I$ ,  $j \geq i$  имаме епиморфизъм  $\varphi_i^j : G_j \rightarrow G_i$ . Избираме  $g_j \in (\varphi_i^j)^{-1}(g_i)$  от праобраза на  $g_i$  под действие на този епиморфизъм. За  $j \in I$ ,  $j \leq i$  полагаме  $g_j := \varphi_j^i(g_i)$ . За онези  $k \in I$ , които не са сравними с  $i \in I$  относно частичната наредба  $\leq$  няма значение какви  $g_k \in G_k$  са избрани. Например, можем да вземем  $g_k = e_k$  да съвпадат с неутралните елементи  $e_k$  на  $G_k$ . Така образуваният елемент  $(g_s)_{s \in I} \in \prod_{s \in I} G_s$  изпълнява условията за съгласуваност и попада в  $\varprojlim G_s$ . Проекцията му върху  $G_i$  е  $g_i$ .

Множеството  $\{(\mathbb{Z}_n, +)\}_{n=1}^\infty$  на крайните фактор-групи  $(\mathbb{Z}_n, +)$  на безкрайната циклична група  $(\mathbb{Z}, +)$  е проективна система, индексирана с  $(\mathbb{N}, \leq)$ . Поточно, ако  $m \in \mathbb{N}$  дели  $n \in \mathbb{N}$ , то

$$\varphi_m^n : (\mathbb{Z}_n, +) \longrightarrow (\mathbb{Z}_m, +),$$

$$\varphi_m^n(a + n\mathbb{Z}) = a + m\mathbb{Z} \quad \text{за} \quad \forall a \in \mathbb{Z}$$

е коректно определен епиморфизъм на групи, защото от  $a' - a \in n\mathbb{Z}$  следва  $a' - a \in m\mathbb{Z}$  и

$$\begin{aligned} \varphi_m^n((a + n\mathbb{Z}) + (b + n\mathbb{Z})) &= \varphi_m^n(a + b + n\mathbb{Z}) = a + b + m\mathbb{Z} = \\ &= (a + m\mathbb{Z}) + (b + m\mathbb{Z}) = \varphi_m^n(a + n\mathbb{Z}) + \varphi_m^n(b + n\mathbb{Z}). \end{aligned}$$

Ясно е, че  $\varphi_n^n = \text{Id}_{\mathbb{Z}_n}$ . Ако  $m \in \mathbb{N}$  дели  $n \in \mathbb{N}$  и  $n$  дели  $k \in \mathbb{N}$ , то  $\varphi_m^k = \varphi_m^n \circ \varphi_n^k$  съгласно

$$\varphi_m^n \circ \varphi_n^k(a + k\mathbb{Z}) = \varphi_m^n(a + n\mathbb{Z}) = a + m\mathbb{Z} = \varphi_m^k(a + k\mathbb{Z}) \quad \text{за} \quad \forall a \in \mathbb{Z}.$$

**ОПРЕДЕЛЕНИЕ 2.20.** Проективните граници на крайни групи се наричат про-крайни групи.

Проективната граница  $\widehat{\mathbb{Z}} = \varprojlim (\mathbb{Z}_n, +)$  на системата  $\{(\mathbb{Z}_n, +)\}_{(n \in \mathbb{N}, " \leq ")}$  на крайните фактор-групи  $(\mathbb{Z}_n, +)$  на  $(\mathbb{Z}, +)$  се нарича про-крайна обвивка на  $\mathbb{Z}$ .

**ТЕОРЕМА 4.** (i) *Групите на Galois  $Gal(F/K)$  на крайните разширения на Galois  $F \supset K$  образуват проективна система относно ограничението на автоморфизъм на поле до подполе.*

(ii) *Абсолютната група на Galois  $Gal(K^{sep}/K)$  на поле  $K$  е изоморфна на проективна граница*

$$Gal(K^{sep}/K) \simeq \varprojlim Gal(F/K)$$

на групите на Galois на крайните разширения на Galois  $F \supset K$ .

**Доказателство:** (i) Теоретико-множественото включване е частична наредба в множеството на крайните разширения на Galois  $F \supset K$ . Ако  $F_1 \supset K$  и  $F_2 \supset K$  са крайни разширения на Galois, то  $F_j = K(\theta_j)$  са прости сепарабелни разширения чрез подходящи примитивни елементи  $\theta_j$  и  $K(\theta_1, \theta_2) = K(\theta) \supset K$  е просто крайно сепарабелно разширение на  $K$ , съгласно Теорема-Определение 1 за примитивния елемент и Лема 2.2. Ако полето  $K$  е безкрайно, то в доказателството на Теорема 1 избираме примитивния елемент във вида  $\theta = \theta_1 + c\theta_2$  за подходящо  $c \in K$ . Корените на минималния полином  $f_\theta(x) \in K[x] \setminus K$  на  $\theta$  над  $K$  са от вида  $\theta_1^{(i)} + c\theta_2^{(j)}$ , където  $\theta_1^{(i)}$  е корен на минималния полином  $f_1(x) \in K[x] \setminus K$  на  $\theta_1$  над  $K$ , а  $\theta_2^{(j)}$  е корен на минималния полином  $f_2(x) \in K[x] \setminus K$  на  $\theta_2$  над  $K$ . По предположение, разширенията  $F_s = K(\theta_s) \supset K$  са нормални, така че всички корени  $\theta_1^{(i)}$  на  $f_1(x)$  са от  $F_1$  и всички корени  $\theta_2^{(j)}$  на  $f_2(x)$  са от  $F_2$ . Съгласно  $F_s = K(\theta_s) \subset K(\theta_1, \theta_2) = K(\theta)$ , всички корени  $\theta_1^{(i)} + c\theta_2^{(j)}$  на  $f_\theta(x)$  са от  $K(\theta)$ . В резултат, съществуват  $\deg(f_\theta)$  автоморфизма от  $Gal(K(\theta)/K)$  и  $|Gal(K(\theta)/K)| = [K(\theta) : K]$ . Съгласно Твърдение 2.9, оттук следва, че  $K(\theta) \supset K$  е нормално разширение. По този начин доказахме, че за произволни крайни разширения на Galois  $F_j = K(\theta_j) \supset K$  на безкрайно поле  $K$  съществува крайно разширение на Galois  $K(\theta_1, \theta_2) \supset K$ , което ги съдържа. Същото е вярно и за крайно поле  $K$ , защото произволни крайни разширения на крайни полета са разширения на Galois. В частност, крайните разширения на Galois  $\mathbb{F}_{q^m} \supset \mathbb{F}_q$  и  $\mathbb{F}_{q^n} \supset \mathbb{F}_q$  се съдържат в крайното разширение на Galois  $\mathbb{F}_{q^{LCM(m,n)}} \supset \mathbb{F}_q$ , където  $LCM(m,n) \in \mathbb{N}$  е най-малкото общо кратно на  $m$  и  $n$ . По този начин, за произволно фиксирано поле  $K$ , крайните разширения на Galois  $F \supset K$  образуват насочена система относно теоретико-множественото включване.

Ако  $F_1 \supset K$  и  $F_2 \supset K$  са крайни разширения на Galois на  $K$  и  $F_1$  е подполе на  $F_2$ , то ограничението

$$\text{rest}_{F_1}^{F_2} : Gal(F_2/K) \longrightarrow Gal(F_1/K),$$

$$\text{rest}_{F_1}^{F_2}(g) = g|_{F_1}$$

е хомоморфизъм на групи. Тук използваме, че  $g(F_1) \subseteq F_1$  за  $\forall g \in Gal(F_2/K)$ , защото всеки алгебричен над  $K$  елемент на  $F_1$  се трансформира с корен на минималния си полином над  $K$  и разширението  $F_1 \supset K$  е нормално. Хомоморфизмите  $\text{rest}_{F_1}^{F_2}$  са епиморфизми съгласно Лема 2.13. Условието  $\text{rest}_F^F = \text{Id}_F$  и  $\text{rest}_{F_1}^{F_3} = \text{rest}_{F_1}^{F_2} \circ \text{rest}_{F_2}^{F_3}$  за  $F_3 \supset F_2 \supset F_1$  следват непосредствено. Това доказва, че групите на Galois  $Gal(F/K)$  на крайните разширения на Galois  $F \supset K$  образуват проективна система относно хомоморфизмите на ограничение.

(ii) За да построим изоморфизъм на групи  $Gal(K^{sep}/K) \rightarrow \varprojlim Gal(F/K)$ , да разгледаме хомоморфизмите на ограничение

$$\text{rest}_F : Gal(K^{sep}/K) \longrightarrow Gal(F/K)$$

и фамилията

$$\text{rest} = (\text{rest}_F) : \text{Gal}(K^{\text{sep}}/K) \longrightarrow \prod_{F \supset K} \text{Gal}(F/K),$$

образувана от тях, която също е хомоморфизъм. Ако  $F_j \supset K$ ,  $1 \leq j \leq 2$  са крайни разширения на Galois и  $F_1 \subset F_2$ , то  $\text{rest}_{F_1} = \text{rest}_{F_1}^{F_2} \circ \text{rest}_{F_2}$ , така че образът на  $\text{rest}$  се съдържа в  $\varprojlim \text{Gal}(F/K)$  и получаваме хомоморфизъм на групи

$$\text{rest} : \text{Gal}(K^{\text{sep}}/K) \longrightarrow \varprojlim \text{Gal}(F/K).$$

Ще проверим, че хомоморфизмът на ограничение  $\text{rest}$  е инективен и сюрективен. Наистина, за  $\forall g \in \text{Gal}(K^{\text{sep}}/K) \setminus \{\text{Id}_{K^{\text{sep}}}\}$  съществува  $\alpha \in K^{\text{sep}}$  с  $g(\alpha) \neq \alpha$ . Полето на разлагане  $F = K(\alpha = \alpha_1, \dots, \alpha_m)$  на минималния полином  $f(x) \in K[x] \setminus K$  на  $\alpha = \alpha_1$  над  $K$  е крайно нормално разширение на  $K$ , съгласно Лема 2.12. Образът  $\text{rest}_F(g) \in \text{Gal}(F/K) \setminus \{\text{Id}_F\}$ , така че  $\text{rest}$  е влагане.

За да установим сюрективността на  $\text{rest}$ , фиксираме  $\varphi = (\varphi_F)_F \in \varprojlim \text{Gal}(F/K)$ .

Ако  $a \in K^{\text{sep}}$ , то минималният полином  $f_a(x) = \prod_{i=1}^n (x - a_i) \in K[x]$  на  $a = a_1$  над  $K$  е сепарабелен и полето на разлагане  $K(f_a) := K(a_1, \dots, a_n)$  на  $f_a(x)$  над  $K$  е крайно разширение на Galois на  $K$ . Действието на  $\varphi_{K(f_a)} \in \text{Gal}(K(f_a)/K)$  върху  $f_a(a) = 0$  дава  $0 = \varphi_{K(f_a)}(0) = \varphi_{K(f_a)}(f_a(a)) = f_a(\varphi_{K(f_a)}(a))$ , така че  $\varphi_{K(f_a)}(a) \in \{a_1, \dots, a_n\}$  е корен на  $f_a(x)$  и изображението

$$\psi : K^{\text{sep}} \longrightarrow K^{\text{sep}},$$

$$\psi(a) := \varphi_{K(f_a)}(a) \in K(f_a) = K(a_1, \dots, a_n) \subset K^{\text{sep}}$$

е коректно определено. Ако  $F \supset K$  е крайно разширение на Galois и  $a \in F$ , то спрегнатите  $a_2, \dots, a_n \in F$  на  $a$  над  $K$  са от  $F$ , така че  $K(f_a) \subseteq F$  и  $\varphi_F(a) = \varphi_{K(f_a)}(a)$ .

За произволни  $a, b \in K^{\text{sep}}$  избираме крайно разширение на Galois  $F \supset K$  с  $a, b \in F$  и проверяваме, че

$$\psi(a + b) = \varphi_F(a + b) = \varphi_F(a) + \varphi_F(b) = \varphi_{K(f_a)}(a) + \varphi_{K(f_b)}(b) = \psi(a) + \psi(b) \quad \text{и}$$

$$\psi(ab) = \varphi_F(ab) = \varphi_F(a)\varphi_F(b) = \varphi_{K(f_a)}(a)\varphi_{K(f_b)}(b) = \psi(a)\psi(b).$$

Това доказва, че  $\psi : K^{\text{sep}} \rightarrow K^{\text{sep}}$  е хомоморфизъм на пръстени. За  $\forall a \in K$  имаме  $f_a(x) = x - a$  и  $K(f_a) = K$ , така че  $\psi(a) = \varphi_K(a) = a$  и  $\psi|_K = \text{Id}_K$ . Вземайки предвид, че единствените идеали на  $K^{\text{sep}}$  са  $0$  и  $K^{\text{sep}}$ , получаваме  $\ker \psi = 0$ . За да проверим, че  $\text{im} \psi = \psi(K^{\text{sep}}) = K^{\text{sep}}$ , фиксираме  $a = a_1 \in K$  с минимален полином  $f_a(x) = \prod_{i=1}^n (x - a_i) \in K[x]$  над  $K$  и разглеждаме полето на разлагане  $K(f_a) := K(a_1, \dots, a_n)$  на  $f_a(x)$  над  $K$ . Ограничението

$$\psi|_{K(f_a)} = \varphi_{K(f_a)} : K(f_a) \longrightarrow K(f_a)$$

съвпада с  $\varphi_{K(f_a)} \in \text{Gal}(K(f_a)/K)$  и образът  $\psi(K(f_a)) = \varphi(K(f_a)) = K(f_a)$ . В частност,  $a \in K(f_a) \in \psi(K(f_a)) \subseteq \psi(K^{\text{sep}})$  и  $\psi : K^{\text{sep}} \rightarrow K^{\text{sep}}$  е автоморфизъм на  $K^{\text{sep}}$ . Вече проверихме, че  $\psi|_K = \text{Id}_K$  и  $\text{rest}_F(\psi) = \varphi_F$  за всяко крайно разширение на Galois  $F \supset K$ . Следователно  $\text{rest}(\psi) = \varphi = (\varphi_F)_F \in \varprojlim \text{Gal}(F/K)$  и мономорфизмът  $\text{rest} : \text{Gal}(K^{\text{sep}}/K) \rightarrow \varprojlim \text{Gal}(F/K)$  е епиморфизъм, а оттам и изоморфизъм на групи, Q.E.D.

### 5. Структура на абсолютната група на Galois на крайно поле

За крайно поле  $\mathbb{F}_q$  да напомним, че всички крайни разширения  $\mathbb{F}_{q^m} \supset \mathbb{F}_q$  са разширения на Galois с група на Galois

$$\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \langle \Phi_q \rangle = \{ \Phi_{q^{s_m(\text{mod } m)}} \mid s_m \in \mathbb{Z} \} \simeq (\mathbb{Z}_m, +).$$

Ако  $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^{mn}}$ , то хомоморфизмът на ограничение

$$\text{rest}_{\mathbb{F}_{q^m}^{\mathbb{F}_{q^{mn}}}} : \text{Gal}(\mathbb{F}_{q^{mn}}/\mathbb{F}_q) \longrightarrow \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q),$$

$$\text{rest}_{\mathbb{F}_{q^m}^{\mathbb{F}_{q^{mn}}}}(\Phi_{q^{s_{mn}(\text{mod } mn)}}) = \Phi_{q^{s_{mn}(\text{ord } m)}}$$

е индуциран от хомоморфизма

$$\varphi_m^{mn} : (\mathbb{Z}_{mn}, +) \longrightarrow (\mathbb{Z}_m, +),$$

$$\varphi_m^{mn}(s_{mn}(\text{mod } mn)) = s_{mn}(\text{mod } m).$$

Изоморфизмът на групи

$$\text{rest} : \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \longrightarrow \varprojlim \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$$

от Теорема 4 действа по правилото

$$\text{rest}(\varphi) = (\varphi|_{\mathbb{F}_{q^m}} = \Phi_{q^{s_m(\text{mod } m)}})_{m \in \mathbb{N}} \in \prod_{m \in \mathbb{N}} \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$$

и изпълнява условията за съвместимост

$$\text{rest}_{\mathbb{F}_{q^m}^{\mathbb{F}_{q^{mn}}}}(\Phi_{q^{s_{mn}(\text{mod } mn)}}) = \Phi_{q^{s_{mn}(\text{mod } m)}} = \Phi_{q^{s_m(\text{mod } m)}} = \varphi|_{\mathbb{F}_{q^m}} \quad \text{за } \forall m, n \in \mathbb{N},$$

които се свеждат до

$$s_{mn} \equiv s_m(\text{mod } m) \quad \text{за } \forall m, n \in \mathbb{N}.$$

Съгласно резултат на Waterhouse, всяка про-крайна група може да се реализира като група на Galois на подходящо разширение на полета.

Ще опишем  $\widehat{\mathbb{Z}}$  чрез адитивните групи на целите  $p$ -адични числа  $\widehat{\mathbb{Z}}_p$ . За произволно просто  $p$  фамилията от крайни адитивни групи  $\{\mathbb{Z}_{p^n}\}_{n=1}^{\infty}$  образува проективна система относно обичайната наредба на естествените числа. Нейната проективна граница

$$\widehat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}_{p^n} = \left\{ (\overline{z_n})_{n=1}^{\infty} \in \prod_{n=1}^{\infty} \mathbb{Z}_{p^n} \mid z_n \equiv z_m(\text{mod } p^m) \quad \text{за } \forall m < n \right\}$$

е адитивната група на целите  $p$ -адични числа.

ТВЪРДЕНИЕ 2.21. (i) Про-крайната обвивка  $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}_n$  на  $(\mathbb{Z}, +)$  е изоморфна на директното произведение  $\prod_{\text{просто } p} \widehat{\mathbb{Z}}_p$  на адитивните групи  $\widehat{\mathbb{Z}}_p$  на целите  $p$ -адични числа за всички прости  $p$ .

(ii) Групата  $(\mathbb{Z}, +)$  е остатъчно крайна, т.е. диагонално изображение

$$\Delta : \mathbb{Z} \longrightarrow \widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}_n,$$

$$\Delta(z) = ((z_n = z(\text{mod } n)))_{n=1}^{\infty} \in \prod_{n=1}^{\infty} \mathbb{Z}_n$$

е влагане.



**Доказателство:** Естествената проекция

$$\Pi : \prod_{n=1}^{\infty} \mathbb{Z}_n \longrightarrow \prod_{\text{просто } p} \prod_{m=1}^{\infty} \mathbb{Z}_{p^m}$$

се ограничава до хомоморфизъм на групи

$$\Pi : \varprojlim \mathbb{Z}_n \longrightarrow \prod_{\text{просто } p} \widehat{\mathbb{Z}}_p,$$

защото съгласуваността на  $z_m$  със  $z_n$  за всички делители  $m$  на  $n$  води до съгласуваност на  $z_{p^k}$  със  $z_{p^l}$  за  $k < l$ .

За произволно  $\beta = (\beta_p)_p = (\beta_{p^m})_{p,m} \in \prod_{\text{просто } p} \widehat{\mathbb{Z}}_p$  ще докажем, че съществува единствено  $\alpha = (\alpha_n)_n \in \varprojlim \mathbb{Z}_n$  с  $\Pi(\alpha) = \beta$ . Работим с индукция по броя на простите делители на  $n \in \mathbb{N}$ . За целта представяме  $n = mp^k$  чрез взаимно прости  $m \in \mathbb{N}$  и  $p^k$  с просто  $p$ . Започваме конструкцията на  $\alpha$  с  $\alpha_{p^m} = \beta_{p^m}$  за всички прости  $p$  и естествени  $m$ . Избираме цели числа  $z_m, z_{p^k}$ , представлящи  $z_m \pmod{m} = \alpha_m$  и  $z_{p^k} \pmod{p^k} = \alpha_{p^k}$ . По Китайската Теорема за остатъците съществува  $z_n \in \mathbb{Z}$  със  $z_n \equiv z_m \pmod{m}$  и  $z_n \equiv z_{p^k} \pmod{p^k}$ . По-точно, ако  $u, v \in \mathbb{Z}$  изпълняват твърдението на Bezout  $mu + p^k v = 1$  за взаимно простите  $m$  и  $p^k$ , то  $z_n := z_m \cdot p^k v + z_{p^k} \cdot mu$  върши работа. Трябва да проверим съгласуваността на  $\alpha_n = z_n \pmod{n}$  с  $\alpha_d$  за всички делители  $d$  на  $n$ . Нека  $d = m_1 p^l$  за някакъв естествен делител  $m_1$  на  $m$  и  $0 \leq l \leq k$ . Достатъчно е да установим, че  $m_1$  и  $p^l$  делят  $z_n - z_d$ , за да твърдим, че  $z_n \equiv z_d \pmod{d}$ . Но  $z_n - z_d = (z_n - z_m) + (z_m - z_{m_1}) + (z_{m_1} - z_d)$  се представя като сума на цели числа, кратни на  $m_1$ , както и като сума  $z_n - z_d = (z_n - z_{p^k}) + (z_{p^k} - z_{p^l}) + (z_{p^l} - z_d)$  на цели числа, кратни на  $p^l$ . Това доказва съществуването на  $\alpha \in \varprojlim \mathbb{Z}_n$  с  $\Pi(\alpha) = \beta$ .

За единствеността на  $\alpha$  да предположим, че сме избрали  $\alpha_n = z_n \pmod{n}$  и  $\alpha'_n = z'_n \pmod{n}$  с  $z_n \equiv z_m \pmod{m}$ ,  $z'_n \equiv z'_m \pmod{m}$ ,  $z_n \equiv z_{p^k} \pmod{p^k}$ ,  $z'_n \equiv z'_{p^k} \pmod{p^k}$ . Тогава  $m$  дели  $z_n - z'_n = (z_n - z_m) + (z_m - z'_m) + (z'_m - z'_n)$  и  $p^k$  дели  $z_n - z'_n = (z_n - z_{p^k}) + (z_{p^k} - z'_{p^k}) + (z'_{p^k} - z'_n)$ . Поради взаимната простота на  $m$  и  $p^k$ , произведението им  $n = mp^k$  дели  $z_n - z'_n$  и  $\alpha_n = \alpha'_n$ .

(ii) Ако  $\Delta(z) = 0 \in \prod_{n=1}^{\infty} \mathbb{Z}_n$ , то всички естествени  $n$  делят цялото число  $z$  и  $z = 0$ , Q.E.D.

От Твърдение 2.21 следва, че

$$\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}} \simeq \prod_{\text{просто } p} \widehat{\mathbb{Z}}_p$$

## 6. Следа на крайно разширение на крайно поле

Ще завършим настоящия въпрос с някои сведения за норма и следа на крайни разширения на крайни полета. Нека  $F \supset K$  е крайно разширение на Galois. Тогава за  $\forall \alpha \in F$  сумата  $\sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha)$  е фиксирана от произволен елемент

$\tau \in \text{Gal}(F/K)$ ,

$$\tau \left( \sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) \right) = \sum_{\sigma \in \text{Gal}(F/K)} (\tau\sigma)(\alpha) = \sum_{\rho \in \text{Gal}(F/K)} \rho(\alpha),$$

защото елементите  $\tau\sigma \in \text{Gal}(F/K)$  с фиксирано  $\tau \in \text{Gal}(F/K)$  пробягват цялата група  $\text{Gal}(F/K)$ , когато  $\sigma$  пробягва  $\text{Gal}(F/K)$ . Съгласно Лема 2.13 (ii), отгук следва, че  $\sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) \in F^{\text{Gal}(F/K)} = K$ .

ОПРЕДЕЛЕНИЕ 2.22. Ако  $F \supset K$  е крайно разширение на Galois, то изображението

$$\begin{aligned} \text{Tr}_K^F : F &\longrightarrow K, \\ \text{Tr}_K^F(\alpha) &= \sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) \quad \text{за } \forall \alpha \in F \end{aligned}$$

се нарича следа на  $F$  над  $K$ .

ЛЕМА 2.23. Следата  $\text{Tr} = \text{Tr}_K^F : F \rightarrow K$  на крайно разширение на Galois  $F \supset K$  изпълнява следните свойства:

- (i)  $\text{Tr}(\alpha + \beta) = \text{Tr}(\alpha) + \text{Tr}(\beta)$  за  $\forall \alpha, \beta \in F$ ;
- (ii)  $\text{Tr}(t\alpha) = t\text{Tr}(\alpha)$  за  $\forall t \in K, \forall \alpha \in F$ ;
- (iii)  $\text{Tr}(\sigma(\alpha)) = \text{Tr}(\alpha)$  за  $\forall \alpha \in F, \forall \sigma \in \text{Gal}(F/K)$ .

**Доказателство:**

$$\begin{aligned} \text{(i)} \quad \text{Tr}(\alpha + \beta) &= \sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha + \beta) = \\ &= \sum_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) + \sum_{\sigma \in \text{Gal}(F/K)} \sigma(\beta) = \text{Tr}(\alpha) + \text{Tr}(\beta); \\ \text{(ii)} \quad \text{Tr}(t\alpha) &= \sum_{\sigma \in \text{Gal}(F/K)} \sigma(t\alpha) = \sum_{\sigma \in \text{Gal}(F/K)} t\sigma(\alpha) = t\text{Tr}(\alpha); \\ \text{(iii)} \quad \text{Tr}(\sigma(\alpha)) &= \sum_{\tau \in \text{Gal}(F/K)} \tau\sigma(\alpha) = \sum_{\tau \in \text{Gal}(F/K)} \tau(\alpha) = \text{Tr}(\alpha), \end{aligned}$$

Q.E.D.

Свойствата (i) и (ii) от Лема 2.23 означават, че следата  $\text{Tr}_K^F$  на крайно разширение на Galois  $F \supset K$  е  $K$ -линейно изображение.

ЛЕМА 2.24. Следата  $\text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$  на крайно разширение на крайни полета е сюрективно  $\mathbb{F}_q$ -линейно изображение, чието ядро

$$\ker \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} = \{(\Phi_q - \text{Id}_{\mathbb{F}_{q^m}})(\beta) = \beta^q - \beta \mid \beta \in \mathbb{F}_{q^m}\}$$

е с размерност  $m - 1$  над  $\mathbb{F}_q$ .

**Доказателство:** Разглеждаме редицата

$$\mathbb{F}_{q^m} \xrightarrow{\Phi_q - \text{Id}_{\mathbb{F}_{q^m}}} \mathbb{F}_{q^m} \xrightarrow{\text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}} \mathbb{F}_q .$$

Вземайки предвид, че  $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \Phi_q \rangle \simeq \mathbb{Z}_m$ , характеризираме  $\alpha \in \ker \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}$  с уравнението  $\alpha + \alpha^q + \dots + \alpha^{q^{m-1}} = 0$ . Броят на корените на полинома  $x + x^q + \dots + x^{q^{m-1}} = 0$  не надминава степента му  $q^{m-1}$ . Следователно  $\ker \left( \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right)$  е с размерност  $\leq m - 1$  над  $\mathbb{F}_q$ . По Теоремата за ранг и дефект на линейно изображение,

$$m = \dim_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \dim_{\mathbb{F}_q} \left( \ker \left( \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right) \right) + \dim_{\mathbb{F}_q} \left( \text{im} \left( \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right) \right)$$

и  $\dim_{\mathbb{F}_q} \left( \text{im} \left( \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right) \right) \geq 1$ . Като подпространство на  $\mathbb{F}_q$ ,  $\text{im} \left( \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right)$  е с размерност  $\leq 1$ , откъдето  $\dim_{\mathbb{F}_q} \left( \text{im} \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right) = 1$  и  $\text{im} \left( \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right) = \mathbb{F}_q$ . В резултат,  $\dim_{\mathbb{F}_q} \left( \ker \left( \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \right) \right) = m - 1$ .

Изображението

$$\psi = \Phi_q - \text{Id}_{\mathbb{F}_{q^m}} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m},$$

$$\psi(\alpha) = \alpha^q - \alpha \quad \text{за } \forall \alpha \in \mathbb{F}_{q^m}.$$

е  $\mathbb{F}_q$ -линейно като разлика на  $\mathbb{F}_q$ -линейните  $\Phi_q$  и  $\text{Id}_{\mathbb{F}_{q^m}}$ . Ядрото  $\ker \psi = \mathbb{F}_q$ , защото  $\psi(\beta) = \beta^q - \beta = 0$  точно когато  $\beta \in \mathbb{F}_q$ . По теоремата за ранг и дефект на линейно изображение,

$$m = \dim_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \dim_{\mathbb{F}_q}(\ker(\psi)) + \dim_{\mathbb{F}_q}(\text{im}(\psi))$$

и  $\dim_{\mathbb{F}_q}(\text{im}(\psi)) = m - 1$ . Съгласно Лема 2.23 (iii) е изпълнено  $\text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} \psi(\alpha) = \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(\Phi_q(\alpha) - \alpha) = 0$ , така че  $\text{im} \psi(\alpha) \subseteq \ker \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}$ . В резултат,  $\text{im} \psi(\alpha)$  съвпада с  $\ker \text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}$ , Q.E.D.

**ЗАДАЧА 2.25.** Нека  $\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9} : \mathbb{F}_9 \rightarrow \mathbb{F}_3$  е  $\mathbb{F}_3$ -линейното изображение следа на крайното разширение  $\mathbb{F}_9 = \{a + b\alpha \mid a, b \in \mathbb{F}_3\} \supset \mathbb{F}_3$  с  $\alpha^2 = \alpha + 1$ . Да се намери базис на ядрото  $\ker(\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9})$  на  $\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}$  над  $\mathbb{F}_3$ .

## 7. Норма на крайно разширение на крайно поле

Ако  $F \supset K$  е крайно разширение на Galois, то за  $\forall \alpha \in F$  произведението  $\prod_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha)$  принадлежи на  $K$ , защото остава на място под действие на произволен автоморфизъм  $\tau \in \text{Gal}(F/K)$ ,

$$\tau \left( \prod_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) \right) = \prod_{\sigma \in \text{Gal}(F/K)} (\tau\sigma)(\alpha) = \prod_{\rho \in \text{Gal}(F/K)} \rho(\alpha).$$

**ОПРЕДЕЛЕНИЕ 2.26.** Ако  $F \supset K$  е крайно разширение на Galois, то изображението

$$\begin{aligned} \text{Nm}_K^F : F &\longrightarrow K, \\ \text{Nm}_K^F(\alpha) &= \prod_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) \quad \text{за } \forall \alpha \in F \end{aligned}$$

се нарича норма на  $F$  над  $K$ .

**ЛЕМА 2.27.** Нормата  $\text{Nm} = \text{Nm}_K^F : F \rightarrow K$  на разширение на Galois  $F \supset K$  от степен  $[F : K] = m$  има следните свойства:

- (i)  $\text{Nm}(\alpha\beta) = \text{Nm}(\alpha)\text{Nm}(\beta)$  за  $\forall \alpha, \beta \in F$ ;
- (ii)  $\text{Nm}(t\alpha) = t^m \text{Nm}(\alpha)$  за  $\forall t \in K, \forall \alpha \in F$ ;
- (iii)  $\text{Nm}(\sigma(\alpha)) = \text{Nm}(\alpha)$  за  $\forall \sigma \in \text{Gal}(F/K), \forall \alpha \in F$ .

**Доказателство:**

$$(i) \text{Nm}(\alpha\beta) = \prod_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha\beta) = \prod_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) \prod_{\sigma \in \text{Gal}(F/K)} \sigma(\beta) = \text{Nm}(\alpha)\text{Nm}(\beta).$$

$$(ii) \text{Ако } [F : K] = m \text{ и } t \in K, \text{ то } \text{Nm}(t) = \prod_{\sigma \in \text{Gal}(F/K)} \sigma(t) = t^{|\text{Gal}(F/K)|} = t^m.$$

$$(iii) \text{Nm}(\sigma(\alpha)) = \prod_{\tau \in \text{Gal}(F/K)} \tau\sigma(\alpha) = \prod_{\tau \in \text{Gal}(F/K)} \tau(\alpha) = \text{Nm}(\alpha),$$

Q.E.D.

Да отбележим, че всяко  $\alpha \in F^*$  има норма  $\text{Nm}_K^F(\alpha) = \prod_{\sigma \in \text{Gal}(F/K)} \sigma(\alpha) \in K^*$ ,

доколкото  $0 \in K$  остава на място под действие на произволен автоморфизъм на  $F$ . Свойство (i) от Лема 2.27 означава, че ограничението  $\text{Nm}_K^F : F^* \rightarrow K^*$  е хомоморфизъм на мултипликативните групи.

ЛЕМА 2.28. Ограничението  $\text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} : \mathbb{F}_q^* \rightarrow \mathbb{F}_q^*$  на нормата на крайно разширение на крайни полета  $\mathbb{F}_q^m \supset \mathbb{F}_q$  е сюрективен хомоморфизъм на мултипликативните групи, чието ядро

$$\ker \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} = \left\{ \frac{\Phi_q}{\text{Id}_{\mathbb{F}_q^m}}(\beta) = \beta^{q-1} \mid \beta \in \mathbb{F}_q^* \right\}$$

е изоморфно на циклична група от ред  $\frac{q^m-1}{q-1}$ .

**Доказателство:** Разглеждаме редицата

$$\mathbb{F}_q^* \xrightarrow{\frac{\Phi_q}{\text{Id}_{\mathbb{F}_q^m}}} \mathbb{F}_q^* \xrightarrow{\text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q}} \mathbb{F}_q^* .$$

Ядрото  $\ker \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q}$  се състои от корени  $\alpha \in \mathbb{F}_q^*$  на полинома

$$\text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q}(x) = x^{\sum_{i=0}^{m-1} q^i} = x^{\frac{q^m-1}{q-1}} = 1$$

и съдържа най-много  $\frac{q^m-1}{q-1}$  елемента. Съгласно теоремата за хомоморфизмите,

$$\mathbb{F}_q^* / \ker \left( \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} \right) \simeq \text{im} \left( \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} \right) .$$

Комбинирайки с теоремата на Лагранж за реда на крайна група получаваме

$$\left| \text{im} \left( \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} \right) \right| = \frac{|\mathbb{F}_q^*|}{\left| \ker \left( \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} \right) \right|} \geq q - 1 .$$

Вземайки предвид, че  $\mathbb{F}_q^* \simeq \mathbb{Z}_{q-1}$ , стигаме до извода, че  $\text{im} \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} = \mathbb{F}_q^*$ . Оттук  $\ker \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q}$  е подгрупа от ред  $\frac{q^m-1}{q-1}$  на цикличната група  $\mathbb{F}_q^* \simeq \mathbb{Z}_{q^m-1}$ . Следователно  $\ker \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} \simeq \mathbb{Z}_{\frac{q^m-1}{q-1}}$  е циклична група от ред  $\frac{q^m-1}{q-1}$ .

Да разгледаме хомоморфизма

$$\Psi : \frac{\Phi_q}{\text{Id}_{\mathbb{F}_q^*}} : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$$

$$\Psi(\alpha) = \frac{\Phi_q(\alpha)}{\alpha} = \alpha^{q-1} \quad \text{за } \forall \alpha \in \mathbb{F}_q^*$$

на мултипликативната група  $\mathbb{F}_q^*$ . Неговото ядро  $\ker \Psi = \mathbb{F}_q^*$ , така че  $\text{im} \Psi \simeq \mathbb{F}_q^* / \ker(\Psi)$  е подгрупа на  $\mathbb{F}_q^*$  от ред

$$\frac{|\mathbb{F}_q^*|}{|\ker(\Psi)|} = \frac{q^m - 1}{q - 1} .$$

Твърдим, че  $\text{im} \Psi \subseteq \ker \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q}$ . Наистина, за  $\forall \alpha \in \mathbb{F}_q^*$  е в сила

$$\text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q} \Psi(\alpha) = \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q}(\alpha^{q-1}) = (\alpha^{q-1})^{\frac{q^m-1}{q-1}} = \alpha^{q^m-1} = 1 .$$

Следователно  $\text{im} \Psi = \ker \text{Nm}_{\mathbb{F}_q^m}^{\mathbb{F}_q}$  съвпадат като циклични подгрупи от един и същи ред  $\frac{q^m-1}{q-1}$  в  $\mathbb{F}_q^* \simeq \mathbb{Z}_{q^m-1}$ , Q.E.D.

ЗАДАЧА 2.29. Нека  $\mathbb{F}_9^* \simeq (\mathbb{Z}_8, +)$  и  $\mathbb{F}_3^* \simeq (\mathbb{Z}_2, +)$  са мултипликативните групи на полетата  $\mathbb{F}_9$ , съответно  $\mathbb{F}_3$ , а  $\text{Nm}_{\mathbb{F}_3}^{\mathbb{F}_9} : \mathbb{F}_9^* \rightarrow \mathbb{F}_3^*$  е хомоморфизмът норма на мултипликативните групи на крайното разширение  $\mathbb{F}_9 \supset \mathbb{F}_3$ . Да се намери пораждащ на цикличното ядро  $\ker \left( \text{Nm}_{\mathbb{F}_3}^{\mathbb{F}_9} \right)$  на  $\text{Nm}_{\mathbb{F}_3}^{\mathbb{F}_9}$ .