Je-li $\alpha_1, \ldots, \alpha_m$ báze $\mathbf{F} = \mathbf{F}_{q^m}$ nad $\mathbf{K} = \mathbf{F}_q$, potom libovolný prvek $\alpha \in \mathbf{F}_{q^m}$ můžeme vyjádřit jednoznačně ve tvaru

$$\alpha = c_1(\alpha) \cdot \alpha_1 + c_2(\alpha) \cdot \alpha_2 + \ldots + c_m(\alpha) \cdot \alpha_m$$

kde $c_i(\alpha) \in \mathbf{F}_q$ pro $i = 1, \ldots, m$.

Každé zobrazení $c_i(\alpha) : \mathbf{F}_{q^m} \to \mathbf{F}_q$ je lineární funkcionál. Pro každé $i = 1, \ldots, m$ existuje $\beta_i \in \mathbf{F}_{q^m}$ takové, že

$$c_i(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha\beta_i)$$

Je-li $\alpha = \alpha_j$, pak

$$c_i(\alpha_j) = \delta_{ij} = \begin{cases} 0, & i \neq j \\ 1, & i = j. \end{cases}$$

Tedy $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_j\beta_i) = \delta_{ij}$.

Posloupnost $\beta_1, \ldots, \beta_m$ je lineárně nezávislá nad $\mathbf{F}_q$, neboť z rovnosti

$$d_1\beta_1 + \ldots + d_m\beta_m = 0$$

pro $d_1, \ldots, d_m \in \mathbf{F}_q$ plyne pro každé $j = 1, \ldots, m$

$$d_1\beta_1\alpha_j + \ldots + d_m\beta_m\alpha_j = 0,$$

$$\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(d_1\beta_1\alpha_j + \ldots + d_m\beta_m\alpha_j) = 0,$$

$$d_1\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta_1\alpha_j) + \ldots + d_m\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta_m\alpha_j) = 0$$

$$d_j \cdot 1 = 0.$$

Proto $\beta_1, \ldots, \beta_m$ je opět báze $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$.

Definice. Báze $\beta_1 \ldots, \beta_m$ se nazývá *duální báze* k bázi $\alpha_1, \ldots, \alpha_m$ v $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$.

Poznámka. Duální báze k bázi $\alpha_1, \ldots, \alpha_m$ je určena jednoznačně bází $\alpha_1, \ldots, \alpha_m$. To plyne ze vztahu $c_i(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha\beta_i)$. Proto duální báze k bázi $\beta_1, \ldots, \beta_m$ je původní báze $\alpha_1, \ldots, \alpha_m$.

Příklad. Nechť $\mathbf{F}_8 \supseteq \mathbf{F}_2$ je kořenové rozšíření $\mathbf{F}_2$ určené polynomem $f(x) = x^3 + x^2 + 1 \in \mathbf{F}_2[x]$. Buď $\alpha \in \mathbf{F}_8$ kořen $f(x)$. Uvažujme prvky $\alpha, \alpha^2, \alpha^3 = \alpha^2 + 1, \alpha^4 = \alpha(\alpha^2+1) = \alpha^3+\alpha = \alpha^2+\alpha+1, \alpha^5 = \alpha(\alpha^2+\alpha+1) = \alpha^3+\alpha^2+\alpha = \alpha^2+1+\alpha^2+\alpha = \alpha+1, \alpha^6 = \alpha(\alpha+1) = \alpha^2+\alpha, \alpha^7 = 1$.

Prvky $\alpha, \alpha^2, \alpha^4$ tvoří bázi $\mathbf{F}_8$ nad $\mathbf{F}_2$. Ukážeme, že $\beta_1 = \alpha, \beta_2 = \alpha^2, \beta_3 = \alpha^2 + \alpha + 1$ je duální báze k $\alpha, \alpha^2, \alpha^2 + \alpha + 1$. Plyne to z následujících rovností.

$\mathrm{Tr}(\alpha_1\beta_1) = \mathrm{Tr}(\alpha\alpha) = \mathrm{Tr}(\alpha^2) = \alpha^2 + \alpha^4 + \alpha^8 = \alpha^2 + \alpha^2 + \alpha + 1 + \alpha = 1$.

$\mathrm{Tr}(\alpha_1\beta_2) = \mathrm{Tr}(\alpha\alpha^2) = \mathrm{Tr}(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^{12} = \alpha^2 + 1 + \alpha^2 + \alpha + \alpha + 1 = 0$.

Analogicky dál.

Definice. Báze $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$ tvaru $\alpha, \alpha^q, \alpha^{q^2} \ldots, \alpha^{q^{m-1}}$ pro nějaké $\alpha \in \mathbf{F}_{q^m}$ se nazývá *normální báze* $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$.

Věta 4.8. *Je-li $\mathbf{F}_{q^m}$ rozšíření $\mathbf{F}_q$, pak existuje v $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$ normální báze. Dokonce existuje normální báze tvořená primitivními prvky $\mathbf{F}_{q^m}$.*

Definice. Nechť $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$ a $\alpha_1, \ldots, \alpha_m \in \mathbf{F}$. Označme $B = (\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_i, \alpha_j))_{i,j}$. Čili B je čtvercová matice řádu m, která má na místě (i, j) prvek $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_i, \alpha_j)$. Pak $\Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \ldots, \alpha_m) = \det B$ se nazývá *diskriminant* $\alpha_1, \ldots, \alpha_m$ nad $\mathbf{F}_q$.

Věta 4.9. *Prvky $\alpha_1, \ldots, \alpha_m \in \mathbf{F}$ tvoří bázi $\mathbf{F} = \mathbf{F}_{q^m}$ nad $\mathbf{K} = \mathbf{F}_q$ právě tehdy, když $\Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \ldots, \alpha_m) \neq 0$.*

Důkaz. ($\Rightarrow$) Nechť $\alpha_1, \ldots, \alpha_m$ je báze $\mathbf{F}$ nad $\mathbf{K}$. Ukážeme, že řádky matice B jsou lineárně nezávislé. Je-li $d_1 \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_1\alpha_j) + d_2 \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_2\alpha_j) + \ldots + d_m \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_m\alpha_j) = 0$ pro nějaké $d_1, \ldots, d_m \in \mathbf{K}$ a každé $j = 1, \ldots, m$, pak platí

$$\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}((d_1\alpha_1 + \ldots + d_m\alpha_m) \cdot \alpha_j) = 0$$

pro $j = 1, \ldots, m$. Označme si $\beta = d_1\alpha_1 + \ldots + d_m\alpha_m$. Tedy $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta\alpha_j) = 0$ pro $j = 1, \ldots, m$. Protože $\alpha_1, \ldots, \alpha_m$ je báze $\mathbf{F}$ nad $\mathbf{K}$, plyne odtud $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta\alpha) = 0$ pro libovolné $\alpha \in \mathbf{F}_{q^m}$. Proto $\beta = 0$, neboli $d_1\alpha_1 + \ldots + d_m\alpha_m = 0$. Protože $\alpha_1, \ldots, \alpha_m$ je báze $\mathbf{F}$ nad $\mathbf{K}$, platí $d_1 = d_2 = \ldots = d_m = 0$.

($\Leftarrow$) Nechť $\Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \ldots, \alpha_m) \neq 0$ a $c_1\alpha_1 + \ldots + c_m\alpha_m = 0$ pro nějaké $c_1, \ldots, c_m \in \mathbf{K}$. Pak platí $c_1\alpha_1\alpha_j + \ldots + c_m\alpha_m\alpha_j = 0$ pro libovolné $j = 1, \ldots, m$. Proto $0 = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c_1\alpha_1\alpha_j + \ldots + c_m\alpha_m\alpha_j) = c_1 \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_1\alpha_j) + \ldots + c_m \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_m\alpha_j)$ pro $j = 1, \ldots, m$. Tedy lineární kombinace řádků matice B s koeficienty $c_1, \ldots, c_m$ se rovná 0. Protože $\det B = \Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \ldots, \alpha_m) \neq 0$, jsou řádky matice B lineárně nezávislé a proto $c_1 = \ldots = c_m = 0$. Tedy $\alpha_1, \ldots, \alpha_m$ jsou lineárně nezávislé nad $\mathbf{K}$ a tvoří bázi $\mathbf{F}$ nad $\mathbf{K}$. □

Označme si nyní

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \ldots & \alpha_m^q \\ \vdots & & & \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \ldots & \alpha_m^{q^{m-1}} \end{pmatrix} = (\alpha_j^{q^{i-1}})_{i,j}$$

Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_i\alpha_j) = \alpha_i\alpha_j + \alpha_i^q\alpha_j^q + \ldots + \alpha_i^{q^{m-1}}\alpha_j^{q^{m-1}}$. Proto platí $A^T \cdot A = B$ a tedy $\det B = (\det A)^2$.

Důsledek 4.10. *Prvky $\alpha_1, \ldots, \alpha_m$ tvoří bázi $\mathbf{F}$ nad $\mathbf{K}$ právě tehdy, když* $\det A \neq 0$.

5. Odmocniny z 1 a cyklotomické polynomy

Definice. Je-li $\mathbf{K}$ libovolné těleso, pak rozkladové rozšíření $\mathbf{K}$ určené polynomem $x^n - 1 \in \mathbf{K}[x]$ se nazývá *n-té cyklotomické těleso* nad $\mathbf{K}$ a označuje se $\mathbf{K}^{(n)}$. Množina všech kořenů polynomu $x^n - 1$ v $\mathbf{K}^{(n)}$ se označuje $\mathbf{E}^{(n)}$.

Věta 5.1. *Nechť $n > 0$ a $\mathbf{K}$ je těleso charakteristiky p. Pak platí*

(1) *pokud $p \nmid n$, pak $\mathbf{E}^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(\mathbf{K}^{(n)})^*$ tělesa $\mathbf{K}^{(n)}$,*
(2) *pokud $p|n$ a $n = p^l m$, kde $p \nmid m$, pak $\mathbf{K}^{(n)}$ se rovná $\mathbf{K}^{(m)}$ a kořeny polynomu $x^n - 1$ jsou prvky $\mathbf{E}^{(m)}$, každý s násobností p^l.*

Důkaz. (1) Platí, že $x^n - 1$ a $nx^n - 1$ nemají společný kořen v $\mathbf{K}[n]$, tedy jsou v $\mathbf{K}[x]$ nesoudělné a $x^n - 1$ nemá žádný vícenásobný kořen. Tedy $\mathbf{E}^{(n)}$ obsahuje přesně n prvků.

Jsou-li $\xi, \mu \in \mathbf{E}^{(n)}$, pak $(\xi\mu)^n = \xi^n\mu^n = 1$. Protože ξ je kořen $x^n - 1$, platí $\xi^n = 1$. Proto $(\xi^{-1})^n = 1.(\xi^{-1})^n = \xi^n.(\xi^{-1})^n = 1^n = 1$. Tedy $\mathbf{E}^{(n)}$ je podgrupa $(\mathbf{K}^{(n)})^*$.

Nechť $n = p_1^{l_1} \cdot \ldots \cdot p_t^{l_t}$ rozklad na prvočinitele. Pak pro každé $i = 0, \ldots, t$ existuje prvek $a_i \in \mathbf{E}^{(n)}$, pro který platí $a_i^{\frac{n}{p_i}} \neq 1$. Potom prvek $b_i = a_i^{\frac{n}{p_i^{l_i}}}$ má řád $p_i^{l_i}$ a $b_1, \ldots, b_t$ je generátor grupy $\mathbf{E}^{(n)}$.

(2) Platí $x^n - 1 = (x^m - 1)^{p^l}$ v $\mathbf{K}[x]$, odkud už tvrzení snadno plyne.

□