4. Stopy, normy a báze

Připomeňme si, že je-li $\mathbf{F}_{q^m} \supseteq \mathbf{F}_q$, tak všechny automorfismy $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$ jsou tvaru $\alpha \to \alpha^{q^i}$ pro $i = 0, 1, 2, \ldots, m-1$ a libovolné $\alpha \in \mathbf{F}_{q^m}$.

V dalším bude často používat označení $\mathbf{F} = \mathbf{F}_{q^m}$ a $\mathbf{K} = \mathbf{F}_q$.

Definice. Nechť $\mathbf{F} = \mathbf{F}_{q^m}$, $\mathbf{K} = \mathbf{F}_q$ a $\alpha \in \mathbf{F}$. Pak definujeme prvek $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}}$ a nazýváme ho *stopa* α nad $\mathbf{K}$.

Je-li $\mathbf{K}$ prvotěleso v $\mathbf{F}$, potom zapisujeme $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \mathrm{Tr}_{\mathbf{F}}(\alpha)$ a prvek $\mathrm{Tr}_{\mathbf{F}}(\alpha)$ nazýváme *absolutní stopa* $\alpha \in \mathbf{F}$.

Lemma 4.1. *Platí* $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) \in \mathbf{K}$ *pro libovolné* $\alpha \in \mathbf{F}$.

Důkaz. Nechť $f(x) = x^d + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in \mathbf{K}[x]$ je minimální polynom prvku $\alpha \in \mathbf{F}$ nad $\mathbf{K}$. Protože $f(x) | x^{q^m} - x$, platí $d | m$. Polynom $f(x)^{\frac{m}{d}} = g(x)$ se nazývá charakteristický polynom α nad $\mathbf{K}$. Kořeny $f(x)$ jsou $\alpha, \alpha^q, \alpha^{q^2}, \ldots \alpha^{q^{d-1}}$ a všechny prvky konjugované k α nad $\mathbf{K}$ jsou právě všechny prvky kořeny polynomu $g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0 = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\ldots(x-\alpha^{q^{m-1}})$. Tedy $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = -b_{m-1} \in \mathbf{K}$. □

Poznámka. Tedy platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}} : \mathbf{F} \to \mathbf{K}$.

Věta 4.2 (O stopě)**.** *Nechť* $\mathbf{F} = \mathbf{F}_{q^m}$ *a* $\mathbf{K} = \mathbf{F}_q$. *Potom* $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}$ *má následující vlastnosti*

(1) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha + \beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) + \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta)$ *pro všechny* $\alpha, \beta \in \mathbf{F}$
(2) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c \cdot \alpha) = c \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *pro všechna* $c \in \mathbf{K}$ *a* $\alpha \in \mathbf{F}$
(3) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}} : \mathbf{F} \to \mathbf{K}$ *je lineární zobrazení na celé těleso* $\mathbf{K}$
(4) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(a) = m.a$ *pro všechna* $a \in \mathbf{K}$
(5) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *pro všechna* $\alpha \in \mathbf{F}$

Důkaz.
(1) Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha+\beta) = (\alpha+\beta) + (\alpha+\beta)^q + (\alpha+\beta)^{q^2} + \ldots + (\alpha+\beta)^{q^{m-1}} = \alpha + \beta + \alpha^q + \beta^q + \alpha^{q^2} + \beta^{q^2} + \ldots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) + \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta)$.
(2) Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c\cdot\alpha) = c\cdot\alpha + (c\cdot\alpha)^q + \ldots + (c\cdot\alpha)^{q^{m-1}} = c\cdot\alpha + c\cdot\alpha^q + c\cdot\alpha^{q^2} + \ldots + c\cdot\alpha^{q^{m-1}} = c\cdot\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$, protože $c \in \mathbf{K} = \mathbf{F}_q$.
(3) Lineárnost zobrazení plyne z předchozích dvou bodů. Stačí tedy najít $\alpha \in \mathbf{F}$, pro které $0 \neq \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$. Je-li $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = 0$, je α kořen rovnice $x + x^q + \ldots + x^{q^{m-1}} \in \mathbf{K}[x]$. Takových je nejvýše $q^{m-1} < q^m$.
(4) Pro $a \in \mathbf{K}$ platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(a) = a + a^q + a^{q^2} + \ldots + a^{q^{m-1}} = \underbrace{a + a + \ldots + a}_{m\text{-krát}} = m.a$
(5) Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \alpha^q + (\alpha^q)^q + \ldots + (\alpha^q)^{q^{m-2}} + (\alpha^q)^{q^{m-1}} = \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}} + \alpha = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$

□

Věta 4.3. *Nechť* $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$. *Pak všechna lineární zobrazení z* $\mathbf{F}$ *do* $\mathbf{K}$ *jsou tvaru* $L_\beta(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha\cdot\beta)$ *pro* $\beta \in \mathbf{F}$.

Je-li $\beta \neq \gamma$, *pak* $L_\beta \neq L_\gamma$.

Důkaz. Nejprve dokážeme, že $L_\beta(\alpha)$ je lineární zobrazení. Platí $L_\beta(\alpha_1+\alpha_2) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}((\alpha_1+\alpha_2)\beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_1\beta) + \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_2\beta) = L_\beta(\alpha_1) + L_\beta(\alpha_2)$ pro všechny $\alpha_1, \alpha_2 \in \mathbf{F}$. Podobně $L_\beta(c\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c\alpha\beta) = c\cdot\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha\beta) = c\cdot L_\beta(\alpha)$.

Je-li $\beta \neq \gamma$, potom existuje prvek $\alpha \in \mathbf{F}$ takový, že $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}((\beta-\gamma)\alpha) \neq 0$ a tedy $L_\beta(\alpha) \neq L_\gamma(\alpha)$. Počet lineárních zobrazení z $\mathbf{F}$ do $\mathbf{K}$ je q^m, tedy stejný jako počet zobrazení L_β. □

Věta 4.4. *Nechť $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$. Potom pro $\alpha \in \mathbf{F}$ platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = 0$ právě tehdy, když $\alpha = \beta^q - \beta$ pro nějaké $\beta \in \mathbf{F}$.*

Důkaz. ($\Rightarrow$) Plyne z Věty 4.2 (5), protože $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta^q-\beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta^q) - \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta) - \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta) = 0$.

($\Leftarrow$) Nechť $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = 0$. Vezmeme polynom $x^q - x - \alpha \in \mathbf{F}[x]$. Buď β kořen polynomu $x^q-x-\alpha$ v nějakém rozšíření $\mathbf{E} \supseteq \mathbf{F}$. Platí $\beta^q-\beta = \alpha$. Zbývá dokázat, že $\beta \in \mathbf{F}_{q^m}$. Platí $0 = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha+\alpha^q+\alpha^{q^2}+\ldots+\alpha^{q^{m-1}} = \beta^q-\beta+(\beta^q-\beta)^q+(\beta^q-\beta)^{q^2}+\ldots+(\beta^q-\beta)^{q^{m-1}} = (\beta^q-\beta)+(\beta^{q^2}-\beta^q)+(\beta^{q^3}-\beta^{q^2})+\ldots+(\beta^{q^m}-\beta^{q^{m-1}}) = \beta^{q^m}-\beta$. Tedy $\beta^{q^m}-\beta = 0$ a proto $\beta \in \mathbf{F}_{q^m}$. □

Věta 4.5 (O tranzitivitě stopy)**.** *Jsou-li $\mathbf{K} = \mathbf{F}_q \subseteq \mathbf{F} = \mathbf{F}_{q^m} \subseteq \mathbf{E} = \mathbf{F}_{q^{m.n}}$ konečná tělesa, pak $\mathrm{Tr}_{\mathbf{E}/\mathbf{K}} = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}} \circ \mathrm{Tr}_{\mathbf{E}/\mathbf{F}}$.*

Důkaz. Je-li $\alpha \in \mathbf{E}$, pak

$$\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\mathrm{Tr}_{\mathbf{E}/\mathbf{F}}(\alpha)) = \sum_{i=0}^{m-1} (\mathrm{Tr}_{\mathbf{E}/\mathbf{F}}(\alpha))^{q^i} = \sum_{i=0}^{m-1} (\sum_{j=0}^{n-1} (\alpha^{q^m})^j)^{q^i}$$

a dále

$$\sum_{i=0}^{m-1} (\sum_{j=0}^{n-1} (\alpha^{q^m})^j)^{q^i} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{mj+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{\mathbf{E}/\mathbf{K}}(\alpha).$$

□

Definice. Nechť $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$. Pak prvek

$$\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdot \ldots \cdot \alpha^{q^{m-1}} = \alpha^{\frac{q^m-1}{q-1}}$$

nazýváme *norma* $\alpha \in \mathbf{F}$ nad $\mathbf{K}$.

Poznámka. Pro všechna $\alpha \in \mathbf{F}$ je $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha) \in \mathbf{K}$, neboť je až na znaménko rovna absolutnímu členu charakteristického polynomu prvku α nad $\mathbf{K}$ - viz důkaz Lemma 4.1.

Věta 4.6 (O normě)**.** *Pro funkci $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$ platí*

(1) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha \cdot \beta) = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha) \cdot \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\beta)$ *pro všechna $\alpha, \beta \in \mathbf{F}$*
(2) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$ *je zobrazení z $\mathbf{F}$ na $\mathbf{K}$ a z $\mathbf{F}^*$ na $\mathbf{K}^*$*
(3) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(d) = d^m$ *pro všechna $d \in \mathbf{K}$*
(4) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *pro všechna $\alpha \in \mathbf{F}$*

Důkaz.
(1) Platí $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha \cdot \beta) = (\alpha \cdot \beta) \cdot (\alpha \cdot \beta)^q \cdot \ldots \cdot (\alpha \cdot \beta)^{q^{m-1}} = \alpha \cdot \alpha^q \cdot \ldots \cdot \alpha^{q^{m-1}} \cdot \beta \cdot \beta^q \cdot \ldots \cdot \beta^{q^{m-1}} = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha) \cdot \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\beta)$
(2) Podle (1) je $\mathrm{N}_{\mathbf{F}/\mathbf{K}} : \mathbf{F}^* \to \mathbf{K}^*$ homomorfismus grup. V jádru $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$ jsou kořeny rovnice
$$x^{\frac{q^m-1}{q-1}} - 1 \in \mathbf{K}[x].$$
Buď d počet prvků (řád) jádra $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$. Platí $d \leq (q^m-1)/(q-1)$ a současně $d|(q^m-1)$. Tedy $\mathrm{Im}(\mathrm{N}_{\mathbf{F}/\mathbf{K}})$ má velikost $(q^m-1)/d \geq q-1$, což je řád $\mathbf{K}^*$.

(3) Platí $\mathrm{N}_{\mathbf{F/K}}(d) = d \cdot d^q \cdot d^{q^2} \cdot \ldots \cdot d^{q^{m-1}} = \underbrace{d \cdot d \cdot \ldots \cdot d}_{m\text{-krát}} = d^m$

(4) Platí $\mathrm{N}_{\mathbf{F/K}}(\alpha^q) = \alpha^q \cdot (\alpha^q)^q \cdot \ldots \cdot (\alpha^q)^{q^{m-2}} \cdot (\alpha^q)^{q^{m-1}} = \alpha^q \cdot \alpha^{q^2} \cdot \ldots \cdot \alpha^{q^{m-1}} \cdot \alpha = \mathrm{N}_{\mathbf{F/K}}(\alpha)$

□

Věta 4.7 (O tranzitivitě normy)**.** *Jsou-li* $\mathbf{K} = \mathbf{F}_q \subseteq \mathbf{F} = \mathbf{F}_{q^m} \subseteq \mathbf{E} = \mathbf{F}_{q^{m.n}}$ *konečná tělesa, pak pro libovolné* $\alpha \in \mathbf{E}$ *platí* $\mathrm{N}_{\mathbf{E/K}}(\alpha) = \mathrm{N}_{\mathbf{F/K}}(\mathrm{N}_{\mathbf{E/F}}(\alpha))$.

Důkaz. Z definice platí $\mathrm{N}_{\mathbf{E/F}}(\alpha) = \alpha^{\frac{(q^m)^n - 1}{q^m - 1}}$. Pak platí

$$\mathrm{N}_{\mathbf{F/K}}(\mathrm{N}_{\mathbf{E/F}}(\alpha)) = (\mathrm{N}_{\mathbf{E/F}}(\alpha))^{\frac{q^m-1}{q-1}} = (\alpha^{\frac{(q^m)^n-1}{q^m-1}})^{\frac{q^m-1}{q-1}} = \alpha^{\frac{q^{m.n}-1}{q-1}} = \mathrm{N}_{\mathbf{E/K}}(\alpha).$$

□