

def.: GALOISOVA GRUPA rozširění  $T \leq S$  :

$$\text{Gal}(S/T) = ( \{ \varphi: S \rightarrow S \text{ } T\text{-izo. } \}, 0, 1, {}^{-1}, \text{id} )$$

Uvězření 1:  $T \leq S$  rozširění těles,  $f \in \text{TEX}$ ,  $A$  množina kořenů  $f$  v  $S \cdot T$ .

Paž  $\forall \varphi \in \text{Gal}(S/T)$  je  $\varphi|_A$  permutací na  $A$   $\mathcal{L}$

$$\boxed{\text{Gal}(S/T) \rightarrow SA} \\ \varphi \mapsto \varphi|_A$$

je grupový  
homomorfismus

def.: GALOISOVA GRUPA polynomu  $f \in \text{TEX}$  :  $(\text{deg } f \geq 1)$

$\text{Gal}(f/T)$  je říd.  $\text{Gal}(S/T)$ , kde  $S$  je rozkladové nad těleso  $F$  nad  $T$

Uvězření 2:  $f \in \text{TEX}$   $\text{st.} \geq 1$ ,  $S$  jeho rozkladové nad těleso nad  $T$ , paž

(1)  $\text{Gal}(S/T)$  je izomorfní podgrupě  $S_n$ , kde  $n = \#$  kořenů  $f$  v  $S \cdot T$

(2)  $\text{Gal}(S/T)$  působí tranzitivně na kořenech  $f$

je-li irreducibilní, paž

$\exists \varphi \in \text{Gal}(S/T)$   $\varphi(a) = b$ .

Shurthi:

$$\text{Gal}(f/T) \hookrightarrow S_{\text{kořenů}}$$

fixed.  $\Rightarrow$  Gal(f/T) transitivní

Trvání:  $\mathbb{Q} \leq T \leq \mathbb{C}$ ,  $n \in \mathbb{N}$ ,  $a \in T \Rightarrow$

- (1) Gal( $x^n - 1/T$ ) je abelovská
- (2) Gal( $x^n - a/T$ ) je abelovská
- (3) Gal( $x^n - a/T$ ) je řešitelná stupně  $\leq 2$

Trvání:  $p$  prvočísla,  $f \in \mathbb{Q}[x]$  ireducibilní stupně  $p$ , který má  $p-2$  reálných a 2 imaginárních kořenů

$$\Rightarrow \text{Gal}(f/\mathbb{Q}) \cong S_p$$