Def.: GALOISOVA GRUPA rozšíření $T \leq S$ je grupa

$$Gal(S/T) = (\{\varphi : S \to S \text{ } T\text{-izomorfismus}\}, \circ, ^{-1}, id)$$

říkáme tady T-automorfismus

Tvrzení: Buď $T \leq S$ rozšíření těles, $f \in T[x]$, $A = \{a \in S \setminus T : f(a) = 0\}$.

Pak $Gal(S/T) \to S_A$, $\varphi \mapsto \varphi \restriction A$ je (dobře definovaný) grupový homom.

↑ tj. $\varphi(a) \in A$ & $\varphi \restriction A$ je permutace

def.: GALOISOVA GRUPA rozšíření $T \leq S$ je grupa

$$Gal(S/T) = (\{\varphi: S \to S \text{ } T\text{-izomorfismus}\}, \circ, ^{-1}, id)$$

def.: GALOISOVA GRUPA polynomu $f \in T[x]$ je

$$Gal(f/T) = Gal(S/T),$$ kde S je rozkladové nadtěleso polynomu f nad T.

$Gal(f,T)$ je určena jednoznačně až na $\simeq$

Důkaz: $\psi: S_1 \to S_2$ T-izo. $\Rightarrow$ $Gal(S_1/T) \simeq Gal(S_2/T)$ grupový izo.

$$\varphi \mapsto \psi \circ \varphi \circ \psi^{-1}$$

Tvrzení: Buď T těleso, $f \in T[x]$ stupně ≥ 1, S rozkladové nadtěleso f nad T, označme $A = \{a \in S \setminus T : f(a) = 0\}$. Pak

(1) homomorfismus $Gal(S/T) \to S_A$ je prostý

$$\varphi \mapsto \varphi|_A$$

(2) je-li f ireducibilní, pak $Gal(S/T)$ působí tranzitivně na A.

tj. $\forall a, b \in A \ \exists \varphi \in Gal(S/T)$ t.ž. $\varphi(a) = b$