4 Galois Groups

definitions

Galois extension A **Galois extension** is an algebraic, normal, separable extension.

Galois group The **Galois group**, $\mathrm{Gal}(E : F) = \mathrm{Aut}(E : F)$.

facts

Proposition 4.1. *(*) Suppose $\mathbb{K}$ splitting field of $f(x) \in F[x]$ irreducible. Then for any $\sigma \in$ Aut(K : F), $\sigma\alpha$ a root of $f(x)$ if α a root of $f(x)$ (σ permutes the roots of irreducible polynomials).*

Proposition 4.2. *If K is the splitting field over F of a separable polynomial $f(x)$, then $K : F$ is Galois.*

Theorem 4.3 (Fundamental Theorem of Galois Theory)**.** *Let $K : F$ be a Galois extension, G = Gal(K : F). Then there is a bijection $\{$subfields E of K containing $F\} \leftrightarrow \{$subgroups H of $G\}$ under the correspondance $E \to$ elements of G which fix E and $H \to$ fixed field of H such that*

(i) If $E_1 \leftrightarrow H_1$, $E_2 \leftrightarrow H_2$, then $E_1 \subseteq E_2 \iff H_1 \geq H_2$ and $E_1 \cap E_2 = \langle H_1, H_2 \rangle$ and $E_1E_2 = H_1 \cap H_2$, so there lattice structure in the diagrams are upside down to each other.

(ii) $[K : E] = |H|$ and $[E : F]$ is the order of H over G.

(iii) $K : E$ is Galois with Galois group H.

(iv) $E : F$ is Galois $\iff$ H normal, in which case Gal(E : F) $= {}^{G}\!/_{H}$.

5 Finite Fields

definitions

characteristic of a field: The **characteristic of a field** $\mathbb{F}$ is defined to be the smallest possible integer p such that $p \cdot 1 = 0$ if such a p exists and zero else.