# GALOIS THEORY

There are many ways to arrive at the main theorem of Galois theory. Although the details of the proofs differ based on the chosen route, there are certain statements that are the milestones in almost every approach. Here is a list of such statements.

**Proposition 1.** *Let $F \subset K$ be a finite extension of fields. Then*

$$|\operatorname{Aut}(K/F)| \leq \deg(K/F).$$

**Proposition 2.** *Let $F \subset K$ be a finite Galois extension and $G = \operatorname{Gal}(K/F)$. Then*

$$|G| = \deg(K/F).$$

**Proposition 3.** *Let $F \subset K$ be a finite Galois extension and $G = \operatorname{Gal}(K/F)$. Then*

$$K^G = F.$$

**Proposition 4.** *Let $F \subset K$ be the splitting field of a separable polynomial in $F[x]$. Then $F \subset K$ is Galois.*

**Proposition 5.** *Let $F \subset K$ be a finite Galois extension. Then $K$ is the splitting field of a separable polynomial in $F[x]$.*

**Proposition 6.** *Let $F \subset K$ be a finite Galois extension. If an irreducible polynomial $p(x) \in F[x]$ of degree $n$ has a root in $K$, then it has $n$ distinct roots in $K$. Moreover, $\operatorname{Gal}(K/F)$ acts transitively on these roots.*

**Proposition 7.** *Let $F \subset K$ be Galois and $E$ an intermediate field. Then $E \subset K$ is Galois.*

**Proposition 8.** *Let $K$ be a field and $H \subset \operatorname{Aut}(K)$ a finite subgroup. Then $K^H \subset K$ is a finite Galois extension with $\operatorname{Gal}(K/K^H) = H$.*

**Theorem 9** (Main theorem)**.** *Let $F \subset K$ be a finite Galois extension and $G = \operatorname{Gal}(K/F)$. Then there is a bijective correspondence*

$$\{\textit{Subfields of } K \textit{ containing } F\} \leftrightarrow \{\textit{Subgroups of } G\},$$

*where the left to right direction is given by*

$$E \mapsto \operatorname{Aut}(K/E),$$

*and the right to left direction by*

$$H \mapsto K^H.$$

*Moreover, the correspondence satisfies the following properties:*

*(1) It is inclusion reversing.*

*(2) If the subfield $E$ corresponds to the subgroup $H$, then*

$$\deg(K/E) = |H|, \quad \deg(E/F) = |G|/|H|.$$

*(3) $K/E$ is always Galois. $E/F$ is Galois if and only if the corresponding subgroup $H$ is a normal subgroup of $G$.*

The logical structure of our approach and the main ideas of the proofs can be summarized as follows.