19. Galois groups and Galois extensions

Definition. Let K/F be a field extension. Let $\mathrm{Aut}(K/F)$ denote the set of all F-automorphisms of K, that is,

$$\mathrm{Aut}(K/F) = \{\varphi \in \mathrm{Aut}(K) : \varphi_{|F} = id_F\}.$$

Then $\mathrm{Aut}(K/F)$ is clearly a group, called the automorphism group of K/F or the Galois group of K/F.

Definition. A field extension is called Galois if it is normal and separable.

Theorem 19.1. *Let K/F be a finite extension. Then $|\mathrm{Aut}(K/F)| \leq [K : F]$, and equality holds if and only if K/F is Galois.*

Proof. Fix an algebraic closure $\overline{F}$ of F with $K \subseteq \overline{F}$. Note that any element of $\mathrm{Aut}(K/F)$ can be thought of as an F-embedding of K into $\overline{F}$, and thus we have a map $T : \mathrm{Aut}(K/F) \to Emb_F(K, \overline{F})$.

The map T is clearly injective, and given $\sigma \in Emb_F(K, \overline{F})$ we have $\sigma \in \mathrm{Im}(T) \iff \sigma(K) = K$. Hence, T is surjective $\iff$ K/F is normal. Therefore, we always have $|\mathrm{Aut}(K/F)| \leq |Emb_F(K, \overline{F})|$, and equality holds if and only if K/F is normal.

On the other hand, by Theorem 18.3 we have $|Emb_F(K, \overline{F})| \leq [K : F]$, where equality holds if and only if K/F is separable. Combining this two results, we deduce Theorem 19.1. □

While the question of determining the Galois group $\mathrm{Aut}(K/F)$ makes sense for any extension K/F, one is usually interested in the case of Galois extensions.

Notation: If K/F is a Galois extension, we will usually write $\mathrm{Gal}(K/F)$ instead of $\mathrm{Aut}(K/F)$.

19.1. **Computing Galois groups.** If K/F is a finite Galois extension, there are two standard ways to describe the Galois group $\mathrm{Gal}(K/F)$. First, we can choose a set of field generators for K over F, that is, write $K = F(\alpha_1, \ldots, \alpha_n)$, and describe the elements of $\mathrm{Gal}(K/F)$ by where they map $\alpha_1, \ldots, \alpha_n$. In some cases, we may simply want to determine $\mathrm{Gal}(K/F)$ up to isomorphism. Let us obtain descriptions of both kind in our standard example $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$.

Example 19.1: Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

First note that the extension $K/\mathbb{Q}$ is indeed Galois – it is separable since $\mathrm{char}\mathbb{Q} = 0$ and normal since K is a splitting field for $x^3 - 2$ over $\mathbb{Q}$.

In order to describe the elements of $\mathrm{Gal}(K/\mathbb{Q})$ by where they map $\sqrt[3]{2}$ and ω, we argue similarly to Example 18.2. Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is determined by the images of $\sqrt[3]{2}$ and ω, and each element must be mapped to an element with the same minimal polynomial over $\mathbb{Q}$. Thus, $\sqrt[3]{2}$ can go to $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$, and ω can go to ω or ω^2. Overall, there are $3 \cdot 2 = 6$ possibilities.

On the other hand, since $K/\mathbb{Q}$ is Galois we know that $|\mathrm{Aut}(K/\mathbb{Q})| = 6$, so each of the above 6 possibilities does correspond to an F-automorphism of K. We conclude that $\mathrm{Gal}(K/\mathbb{Q})$ has six elements $\{\sigma_{i,j} : 0 \leq i \leq 2, 1 \leq j \leq 2\}$ given by $\sigma_{i,j}(\sqrt[3]{2}) = \omega^i\sqrt[3]{2}$ and $\sigma_{i,j}(\omega) = \omega^j$.

The argument used in this example can be generalized as follows. Suppose K/F is a finite Galois extension, and K is given in the form $K = F(\alpha_1, \ldots, \alpha_n)$. For $1 \leq i \leq n$ let $K_i = F(\alpha_1, \ldots, \alpha_i)$. Let $d_i = \deg_F(\alpha_i)$ and $e_i = \deg_{K_{i-1}}(\alpha_i)$. Then $e_i \leq d_i$, and since $e_i = [K_{i-1}(\alpha_i) : K_{i-1}] = [K_i : K_{i-1}]$, we have $[K : F] = \prod_{i=1}^{n} e_i$.

In our example we used the fact that $e_i = d_i$ for each i, in which case the following result holds:

Proposition 19.2. *In the above notations suppose that $e_i = d_i$ for each $1 \leq i \leq n$. Let Ω_i be the set of K-roots of $\mu_{\alpha_i,F}(x)$ (note that $|\Omega_i| = e_i = d_i$). Then for any elements $\beta_1 \in \Omega_1, \ldots, \beta_n \in \Omega_n$ there exists unique $\sigma \in \mathrm{Aut}(K/F)$ s.t. $\sigma(\alpha_1) = \beta_1, \ldots, \sigma(\alpha_n) = \beta_n$. Furthemore, every element of $\mathrm{Aut}(K/F)$ is of this form.*

Proof. Use the same reasoning as in Example 19.1. □

Let us go back to Example 19.1. We know that every group of order 6 is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ or S_3. From the description we obtained it is easy to see that the group $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ is non-abelian and thus must be isomorphic to S_3. However, there is a much nicer way to prove the latter.

Lemma 19.3. *Let K/F be a normal extension, and let $p(x) \in F[x]$ be an irreducible polynomial which has a root in K (and hence by normality splits completely over K). Let Ω be the set of K-roots of $p(x)$. The following hold:*

(a) *$\mathrm{Aut}(K/F)$ acts on Ω, and thus there is a natural homomorphism $\mathrm{Aut}(K/F) \to Sym(\Omega)$. Furthermore, the action of $\mathrm{Aut}(K/F)$ on Ω is transitive.*

(b) *Assume in addition that K is a splitting field for $p(x)$ over F. Then the action of* $\mathrm{Aut}(K/F)$ *on* Ω *is faithful, and thus* $\mathrm{Aut}(K/F)$ *embeds in* $Sym(\Omega)$.

Proof. (a) The group $\mathrm{Aut}(K/F)$ acts on Ω by Lemma 17.1 (we have already used this fact many times). Let us show that this action is transitive.

Take any $\alpha, \beta \in \Omega$. By the Simple Extension Lemma there exists an F-embedding $\sigma : F(\alpha) \to \overline{F}$ s.t. $\sigma(\alpha) = \beta$. By the Main Extension Lemma σ extends to an F-embedding $\sigma' : K \to \overline{F}$ with $\sigma'(\alpha) = \beta$. Since K/F is normal, we have $\sigma'(K) = K$, and thus σ' determines an element of $\mathrm{Aut}(K/F)$ which maps α to β.

(b) If K is a splitting field for $p(x)$, an element of $\mathrm{Aut}(K/F)$ is completely determined by its action on Ω. Thus, if $\sigma \in \mathrm{Aut}(K/F)$ acts trivially on Ω, then $\sigma = id$. □

Example 19.1 concluded: Since $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field for $x^3 - 2$ over $\mathbb{Q}$, Lemma 19.3 implies that $\mathrm{Gal}(K/\mathbb{Q})$ embeds in S_3. Since we already know that $|\mathrm{Gal}(K/\mathbb{Q})| = 6 = |S_3|$, we conclude that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

19.2. **Galois closure.** Let K/F be an algebraic extensions which is not Galois. Can we find an extension field L of K s.t. L/F is Galois? If K/F is not separable, this is clearly impossible (any element of K which is not separable over F will stay inseparable in any extension of K). On the other hand, as we show below, if K/F is separable, such L always exists. The minimal L with this property will be called the Galois closure of K over F.

Theorem 19.4. *Let K/F be a separable extension, and choose an algebraic closure $\overline{F}$ of F with $K \subseteq \overline{F}$. Then there is unique field L with $K \subseteq L \subseteq \overline{F}$ s.t.*

(i) *L/F is Galois*
(ii) *If M is any subfield of $\overline{F}$ s.t. $M \supseteq K$ and M/F is Galois, then $M \supseteq L$.*

The field L is called the Galois closure of K over F.

Proof. Let $\Omega = \{\mu_{\alpha,F}(x) : \alpha \in K\}$, let $A =$ the set of $\overline{F}$-roots of polynomials in Ω and $L = F(A) \supseteq K$. Then L is a splitting field for Ω, whence L/F is normal.

Since K/F is separable, each polynomial in Ω is separable. Hence any $\gamma \in A$ is separable over F, so L/F is separable by Corollary 18.6. Thus the extension L/F is Galois. Verification of condition (ii) and uniqueness of L are left as (easy) exercises. □