1 Galois extensions

1.1 Overview

Let $L \mid K$ be a field extension. Recall that $\mathrm{Aut}_K(L)$ is the group of K-linear field isomorphisms $L \to L$.

Also, if $G \subseteq \mathrm{Aut}_K(L)$ is a subgroup then we let $L^G = \{a \in L : g(a) = a \text{ for all } g \in G\}$.

The following general principle, while confusing to express in symbols, can be useful to remember.

Proposition. One always has $\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L) = \mathrm{Aut}_K(L)$.

Proof. If $g \in \mathrm{Aut}_K(L)$ then g fixes every element of $L^{\mathrm{Aut}_K(L)}$ so g is $L^{\mathrm{Aut}_K(L)}$-linear and in $\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L)$.
Conversely, if $g \in \mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L)$ then g is K-linear since $K \subseteq L^{\mathrm{Aut}_K(L)}$ so $g \in \mathrm{Aut}_K(L)$. □

Definition. A field extension $L \mid K$ with $K \subseteq L$ is called a *Galois extension* if $L^{\mathrm{Aut}_K(L)} = K$.

A general field extension $\iota : K \hookrightarrow L$ is a *Galois extension* if $L^{\mathrm{Aut}_K(L)} = \iota(K)$.

Recall that an algebraic field extension $L \mid K$ is *normal* (respectively, *separable*) if the minimal polynomial over K of any element in L splits in L (respectively, is separable).

Last time we proved that the following properties are equivalent for a finite field extension $L \mid K$:

(a) $L \mid K$ is a Galois extension.

(b) L is the splitting field of a separable polynomial over K.

(c) The extension $L \mid K$ is normal and separable.

From this, we see that if $L \mid K$ is finite Galois extension that is the composition of two extensions

$$K \hookrightarrow K_1 \hookrightarrow L$$

then $L \mid K_1$ is also a finite Galois extension. However, in this setup $K_1 \mid K$ can fail to be Galois.

The *Galois group* of a Galois extension $L \mid K$ is

$$\mathrm{Gal}(L \mid K) := \mathrm{Aut}_K(L)$$

If $L \mid K$ is a finite extension, then this is a finite group by the main theorems in the previous lecture.

Let K be a field and suppose $P(x) \in K[x]$ is a separable polynomial.

Let $L \mid K$ be a splitting field for $P(x)$.

We shall sometimes write $\mathrm{Gal}(P) = \mathrm{Gal}(P(x))$ for $\mathrm{Gal}(L \mid K)$.

Although this definition relies of the choice of splitting field, the isomorphism class of $\mathrm{Gal}(P)$ does not.

We will prove a more detailed version of the following theorem later:

Theorem (*Fundamental theorem of Galois theory*)**.** Assume $\iota : K \hookrightarrow L$ is a finite Galois extension.

Then the map

$$\Big\{\text{subfields of } L \text{ containing } \iota(K)\Big\} \mapsto \Big\{\text{subgroups of } \mathrm{Gal}(L \mid K)\Big\}$$

given by $M \mapsto \mathrm{Gal}(L \mid M)$ is a bijection.

Example. We shall compute the Galois group of the extension $\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}$ and of its subfields.
Note that $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of $(x^2 - 2)(x^2 + 1)$, whose roots are $\pm\sqrt{2}$ and $\pm i$.
Thus $\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}$ is the splitting field of a separable polynomial, so is a Galois extension.

We have successive extensions $\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$.
The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.
Similarly, the polynomial $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$.
Thus we conclude from the tower law that $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 2 \cdot 2 = 4$.

We deduce from the main theorem last time that $\#\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}) = 4$.
Let $G := \operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q})$. Then we either have $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \cong \mathbb{Z}/4\mathbb{Z}$.

Now note that $\#\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(i)) = 2$ as the extension $\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(i)$ is not trivial.
Similarly, $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(\sqrt{2})) = 2$.
Since the only group of order 2 is $\mathbb{Z}/2\mathbb{Z}$, we conclude that

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(i)) \cong \mathbb{Z}/2\mathbb{Z} \qquad \text{and} \qquad \operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/2\mathbb{Z}.$$

By the fundamental theorem of Galois theory, the subgroups

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(\sqrt{2})) \subseteq G \qquad \text{and} \qquad \operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}(i)) \subseteq G$$

cannot coincide, because they correspond to different subfields of $\mathbb{Q}(\sqrt{2}, i)$.
Thus we conclude that G has two distinct subgroups of order 2, and hence

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has three nontrivial subgroups, which are all of order 2:

$$\mathbb{Z}/2\mathbb{Z} \times \{0\}, \quad \{0\} \times \mathbb{Z}/2\mathbb{Z}, \quad \text{and} \quad \{(a \pmod 2, a \pmod 2) : a \in \mathbb{Z}\}$$

We conclude that $\mathbb{Q}(\sqrt{2}, i)$ contains three nontrivial subfields.
(These subfields automatically contain $\mathbb{Q}$ since they have characteristic zero).
We have already found two of them: $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$.
The third subfield is $\mathbb{Q}(i\sqrt{2})$, since we clearly have $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(i\sqrt{2})$ and also $\mathbb{Q}(i) \neq \mathbb{Q}(i\sqrt{2})$.

Example. We mentions some field extensions that are not Galois:

(i) We saw last time that $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ is not a normal extension. Thus it is not Galois.

(ii) We saw earlier that $\mathbb{F}_2(t)[x]/(x^2 - t) \mid \mathbb{F}_2(t)$ is not a separable extension, so it is also not Galois.

1.2 Artin's lemma

Artin's lemma is the following basic but fundamental statement.

Here we let $\mathrm{Aut}(K)$ denote the group of all field isomorphisms $K \xrightarrow{\sim} K$.

Theorem (Artin's lemma)**.** Let K be a field and let $G \subseteq \mathrm{Aut}(K)$ be a finite subgroup.

Then $K \mid K^G$ is a finite Galois extension and $G = \mathrm{Aut}_{K^G}(K)$.

The key point of Artin's lemma is the fact that $K \mid K^G$ is a finite extension.

This is a consequence of the following lemma.

Lemma. Let K be a field and let $G \subseteq \mathrm{Aut}(K)$ be a finite subgroup. Then $[K : K^G] \leq |G|$.

Proof. Suppose $[K : K^G] > |G|$.

Then for some $d > |G|$ there are elements $\alpha_1, \ldots, \alpha_d \in K$ that are linearly independent over K^G.

Let $n = |G|$ and list the elements of the group as $\sigma_1, \ldots, \sigma_n \in G$. Consider the matrix

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_d) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_d) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_d) \end{bmatrix}.$$

Since $d > n$ the columns of this matrix are linearly dependent over K.

Hence there are elements $\beta_1, \ldots, \beta_d \in K$ that are not all zero such that

$$\sum_{i=1}^{d} \beta_i \sigma_k(\alpha_i) = 0 \quad \text{for all } k = 1, \ldots, n. \tag{*}$$

Choose such a sequence with $r > 0$ nonzero terms and assume that r is minimal.

By renumbering, we may assume that $\beta_1, \ldots, \beta_r \neq 0$ and $\beta_{r+1} = \cdots = \beta_d = 0$.

Dividing by β_r, we may also assume $\beta_r = 1$.

Since $\alpha_1, \ldots, \alpha_d$ are linearly independent over K^G, there exists $i_0 \in \{1, \ldots, r\}$ such that $\beta_{i_0} \notin K^G$.

After renumbering just $\beta_1, \ldots, \beta_r$, we may assume that $\beta_1 \notin K^G$.

Now let $k_0 \in \{1, \ldots, n\}$ be such that $\sigma_{k_0}(\beta_1) \neq \beta_1$. Applying σ_{k_0} to the equations (*), we obtain

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)\sigma_{k_0}\sigma_k(\alpha_i) = 0 \quad \text{for all } k \in \{1, \ldots, n\}.$$

Since $\{\sigma_{k_0}\sigma_k : 1 \leq k \leq n\} = \{\sigma_k : 1 \leq k \leq n\} = G$ this means that

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)\sigma_k(\alpha_i) = 0 \quad \text{for all } k \in \{1, \ldots, n\}.$$

Subtracting (*) from this gives

$$\sum_{i=1}^{d}(\sigma_{k_0}(\beta_i)-\beta_i)\sigma_k(\alpha_i)=0 \quad \text{for all } k\in\{1,\dots,n\}.$$

Since $\beta_r=1$ we have $\sigma_{k_0}(\beta_r)-\beta_r=0$, so as $\beta_{r+1}=\cdots=\beta_d=0$ we obtain

$$\sum_{i=1}^{r-1}(\sigma_{k_0}(\beta_i)-\beta_i)\sigma_k(\alpha_i)=0 \quad \text{for all } k\in\{1,\dots,n\}.$$

This contradicts the minimality of r because $\sigma_{k_0}(\beta_1)-\beta_1\neq 0$. Hence $d>n$. □

Now we are able to prove Artin's lemma.

Proof. Recall that K is a field and $G\subseteq \mathrm{Aut}(K)$ is a finite subgroup.
We wish to show that $K \mid K^G$ is a finite Galois extension and that $G=\mathrm{Aut}_{K^G}(K)$.

The extension $K \mid K^G$ is finite by the lemma.
We also have $K^G=K^{\mathrm{Aut}_{K^G}(K)}$ since

- the left side is contained in the right by definition (one always has $F\subseteq K^{\mathrm{Aut}_F(K)}$), and
- the right side is contained in the left as $G\subset \mathrm{Aut}_{K^G}(K)$.

Thus $K \mid K^G$ is a finite Galois extension.

By results last time, $K \mid K^G$ is a splitting extension of a separable polynomial with coefficients in K^G.
Also, we have $[K:K^G]=|\mathrm{Aut}_{K^G}(K)|$.

Now we know from the lemma that $[K:K^G]\leq |G|$. Thus $|\mathrm{Aut}_{K^G}(K)|\leq |G|$.
But $G\subseteq \mathrm{Aut}_{K^G}(K)$ so the reverse inequality $|\mathrm{Aut}_{K^G}(K)|\geq |G|$ holds.
We therefore conclude that $|G|=|\mathrm{Aut}_{K^G}(K)|$ and $G=\mathrm{Aut}_{K^G}(K)$. □