Splitting fields and Galois groups

Let $f(x) \in F[x]$ be a polynomial with coefficients in a field F. A field extension E over F is called a *splitting field* for the polynomial $f(x)$ if there are $\alpha_1, \ldots, \alpha_n \in E$ such that $E = F(\alpha_1, \ldots, \alpha_n)$ and the polynomial splits into linear factors

$$f(x) = a(x - \alpha_1)\cdots(x - \alpha_n)$$

for some non-zero constant $a \in F$.

Examples

1. Let $f(x)$ be the polynomial $x^2 + 1 \in \mathbb{R}[x]$. As $f(x) = (x - i)(x + i)$ as a polynomial in $\mathbb{C}[x]$, a splitting field for $f(x)$ is given by $\mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C}$.

2. Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Then $f(x) = (x - \sqrt{2})(x + \sqrt{2})$. Thus a splitting field is given by the field extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

3. Let $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. A splitting field for this polynomial is given by the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

4. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. The complex roots of this polynomial are as follows:

$$\sqrt[3]{2}, \qquad \sqrt[3]{2} \cdot e^{2\pi i/3}, \qquad \sqrt[3]{2} \cdot e^{-2\pi i/3}$$

Thus a splitting field for $f(x)$ is given by $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{-2\pi i/3})$. Note that

$$\sqrt[3]{2} \cdot e^{-2\pi i/3} = \left(\sqrt[3]{2}\right)^2 \left(\sqrt[3]{2} \cdot e^{2\pi i/3}\right)^{-1}$$

so the third root is already in the field which is generated by the first two roots. In other words, our splitting field can be written $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})$. Furthermore, clearly $\sqrt[3]{2}e^{2\pi i/3}$ can be replaced by $e^{2\pi i/3}$ so that $E = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. Finally,

$$e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

and so $e^{2\pi/3}$ can be replaced by $\sqrt{-3}$. In summary, we have the identification

$$E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

We leave as an exercise that also $E = \mathbb{Q}(\sqrt[3]{2} + e^{2\pi i/3})$.

5. Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. The complex roots of this polynomial are $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$. We have the splitting field $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$.

It is a basic result, which we omit, that for a given non-constant polynomial $f(x) \in F[x]$, a splitting field exists for $f(x)$; and moreover, any two such splitting fields are isomorphic. Thus given $f(x) \in F[x]$ we may speak of *the* splitting field of $f(x)$.

▶ **Given a field extension E over F, we define**

$$\textbf{Aut}(E/F) = \{\sigma : E \to E \,:\, \sigma \textbf{ is an isomorphism}, \ \sigma(a) = a \textbf{ for all } a \in F\}$$

This is naturally a group, called the automorphism group of the field extension.

Proof. Let $\sigma, \sigma' \in \mathrm{Aut}(E/F)$ so that $\sigma, \sigma' : E \to E$ are isomorphisms each fixing F, i.e. $\sigma(a) = \sigma'(a) = a$ for all $a \in F$. Then the composition $\sigma \circ \sigma'$ is an isomorphism of E and $(\sigma \circ \sigma')(a) = \sigma(\sigma'(a)) = \sigma(a) = a$. Thus $\sigma \circ \sigma' \in \mathrm{Aut}(E/F)$. Further, $a = \mathrm{id}_E(a) = (\sigma^{-1} \circ \sigma)(a) = \sigma^{-1}(\sigma(a)) = \sigma^{-1}(a)$ and thus $\sigma^{-1} \in \mathrm{Aut}(E/F)$. Thus $\mathrm{Aut}(E/F)$ is a group. □

A finite field extension E over a subfield of $\mathbb{C}$ is called *Galois* if it is a splitting field of some polynomial $f(x) \in \mathbb{Q}[x]$. All examples above are Galois extensions. More generally, a finite extension E over an arbitrary field F is *Galois* if it is the splitting field of a polynomial $f(x) \in F[x]$ which has no repeated roots in E. We mainly focus on finite extensions of $\mathbb{Q}$ and other subfields of $\mathbb{C}$, in which case Galois fields can be identified with splitting fields.

▶ **If E is a Galois extension of a field F we write**

$$\textbf{Gal}(E/F) = \textbf{Aut}(E/F)$$

and call this the *Galois group* of the field extension.

As a (finite) Galois extension E over F is the splitting field of some polynomial $f(x) \in F[x]$, we also call $\mathrm{Gal}(E/F)$ the *Galois group of the polynomial* $f(x)$.

▶ **Let $E = F(\alpha_1, \ldots, \alpha_n)$ be the splitting field of $f(x) \in F[x]$ whose roots in E are $\alpha_1, \ldots, \alpha_n$. Then there is a 1-1 homomorphism**

$$\phi : \textbf{Gal}(E/F) \longrightarrow S_n$$

to the symmetric group S_n. If $f(x) \in F[x]$ is irreducible, then the image subgroup $\textbf{im}(\phi) \subset S_n$ is a transitive subgroup of S_n.

We remark that a *transitive subgroup* $G \subset S_n$ is a subgroup of the symmetric group S_n such that for all $i, j \in \{1, \ldots, n\}$ there is a permutation $f \in G$ such that $f(i) = j$.

Proof. First, write $f(x) = a_n x^n + \cdots + a_0$ where each $a_i \in F$. Consider a root $\alpha_i \in E$ of $f(x)$, and some $\sigma \in \mathrm{Gal}(E/F)$. Using that $\sigma : E \to E$ is a homomorphism fixing F we compute:

$$\begin{aligned} f(\sigma(\alpha_i)) &= a_n(\sigma(\alpha_i))^n + a_{n-1}(\sigma(\alpha_i))^{n-1} + \cdots + a_1\sigma(\alpha_i) + a_0 \\ &= a_n(\sigma(\alpha_i^n)) + a_{n-1}(\sigma(\alpha_i^{n-1})) + \cdots + a_1\sigma(\alpha_i) + a_0 \\ &= \sigma(a_n(\alpha_i^n)) + \sigma(a_{n-1}(\alpha_i^{n-1})) + \cdots + \sigma(a_1\alpha_i) + \sigma(a_0) \\ &= \sigma(a_n\alpha_i^n + a_{n-1}\alpha_i^{n-1} \cdots + a_1\alpha_i + a_0) = \sigma(0) = 0 \end{aligned}$$

Thus $\sigma(\alpha_i)$ is also a root of $f(x)$, and therefore $\sigma(\alpha_i) = \alpha_j$ for some $j \in \{1, \ldots, n\}$. Since E is Galois over F, the roots are distinct, so the index j is uniquely determined.

Next, define $\phi : \mathrm{Gal}(E/F) \to S_n$ by $\phi(\sigma)(i) = j$ if and only if $\sigma(\alpha_i) = \alpha_j$. In other words, we look at how the automorphism $\sigma : E \to E$ permutes the roots $\alpha_1, \ldots, \alpha_n$. It is straightforward from this construction that ϕ is a homomorphism.

Next, recall $E = F(\alpha_1, \ldots, \alpha_n)$. As $\sigma \in \mathrm{Gal}(E/F)$ fixes F, it is entirely determined by where it sends the elements α_i. This shows that ϕ is 1-1.

Finally, suppose $f(x)$ is irreducible. Then $F(\alpha_i) \cong F[x]/f(x)$ for any root α_i of $f(x)$. In particular, for α_i and α_j any two roots of $f(x)$ that lie in E we have an isomorphism $F(\alpha_i) \cong F[x]/f(x) \cong F(\alpha_j)$. This can be extended to an isomorphism $E \to E$ (we omit this step), from which the result follows. □

The above result shows that the Galois group of E over F is isomorphic to a subgroup of S_n, which has order $n!$. We obtain:

▶ **Let E be the splitting field of $f(x) \in F[x]$ whose degree is n. Then**

$$|\mathbf{Gal}(E/F)| \quad \textbf{divides} \quad n!.$$

Examples

1. Let $f(x)$ be the polynomial $x^2 + 1 \in \mathbb{R}[x]$, whose splitting field is $\mathbb{C} = \mathbb{R}(i, -i)$. Label the roots of $f(x)$ by $\alpha_1 = i$ and $\alpha_2 = -i$. Note that complex conjugation $\sigma : \mathbb{C} \to \mathbb{C}$ defined by

$$\sigma(a + bi) = a - bi$$

is an element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ of order 2. Thus $\{\mathrm{id}_{\mathbb{C}}, \sigma\} \subset \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. As the Galois group has order dividing $2! = 2$, this is in fact an equality of groups. Thus $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$.

2. Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ with splitting field $\mathbb{Q}(\sqrt{2})$. Similar to the previous example, there is only one non-trivial automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ and it is given by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. We have $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2$.

3. Let $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ with splitting field $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recall that any element in E can be written uniquely as

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$$

where $a, b, c, d \in \mathbb{Q}$. Define automorphisms $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Gal}(E/\mathbb{Q})$ by

$$\begin{aligned}
\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3} \\
\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{2}\sqrt{3} \\
\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}) &= a - b\sqrt{2} - c\sqrt{3} - d\sqrt{2}\sqrt{3}
\end{aligned}$$

Labelling the roots of $f(x)$ as $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}$ we have

$$\phi(\sigma_1) = (12), \quad \phi(\sigma_2) = (34), \quad \phi(\sigma_3) = (12)(34)$$

Because no automorphism can interchange $\pm\sqrt{2}$ with $\pm\sqrt{3}$, these are all of them. Thus

$$\mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}_E, \sigma_1, \sigma_2, \sigma_3\} \cong \{e, (12), (34), (12)(34)\} \subset S_4$$

Note that this group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note in this example that $f(x)$ is not irreducible, and that the corresponding permutation group is not transitive.

4. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ with splitting field $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. The roots of $f(x)$ are

$$\alpha_1 = \sqrt[3]{2}, \qquad \alpha_2 = \sqrt[3]{2} \cdot e^{2\pi i/3}, \qquad \alpha_3 = \sqrt[3]{2} \cdot e^{-2\pi i/3}$$

A direct computation shows that every permutation of these 3 roots extends to define an automorphism, and thus $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

5. Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ with splitting field $E = \mathbb{Q}(\sqrt[4]{2}, i)$. The roots of $f(x)$ are

$$\alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = -\sqrt[4]{2}, \quad \alpha_3 = \sqrt[4]{2}i, \quad \alpha_4 = -\sqrt[4]{2}i$$

Note an automorphism of this extension is determined by where it sends $\alpha_1 = \sqrt[4]{2}$ and i. There are automorphisms $\sigma, \tau \in \mathrm{Gal}(E/\mathbb{Q})$ such that:

$$\sigma(\sqrt[4]{2}) = \sqrt[4]{2}i, \qquad \sigma(i) = i$$

$$\tau(\sqrt[4]{2}) = \sqrt[4]{2}, \qquad \tau(i) = -i$$

We have $\phi(\sigma) = (1324)$ and $\phi(\tau) = (34)$. Any other automorphism is a composition of these two automorphisms. The Galois group is isomorphic to the following subgroup of S_4:

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \{e, (12), (34), (12)(34), (1324), (1423), (13)(24), (14)(23)\} \subset S_4$$

In fact this subgroup is isomorphic to the dihedral group D_4, the symmetries of a square.