over $F'(\beta)$, and $[E : F(\alpha)] < [E : F]$, we may apply our induction hypothesis to these field extensions. By induction, the number of extensions of τ to σ is $\leq [E : F(\alpha)]$, with equality if $f(x)$ has distinct roots.

From $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ it follows that the number of extensions of φ to σ is $\leq [E : F]$. We have equality if $p(x)$ and $f(x)$ have distinct roots, which is equivalent to $f(x)$ having distinct roots since $p(x)$ is a factor of $f(x)$, completing the proof by induction.

In the particular case when $F = F'$ and φ is the identity map we have $f(x) = f'(x)$ and $E = E'$ so the isomorphisms of E to E' restricting to φ on F are the automorphisms of E fixing F. We state this as follows:

Proposition 5. Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then

$$|\mathrm{Aut}(E/F)| \leq [E : F]$$

with equality if $f(x)$ is separable over F.

Remark: While we were primarily interested in counting the automorphisms of E which fix F (which is the situation of $F = F'$, $\varphi = 1$ above), it would still have been necessary to consider the situation of more general φ (and different fields F') because of the induction step in the proof (which involves the fields $F(\alpha)$ and $F(\beta)$ for two roots of the same polynomial $p(x)$).

One can modify the proof above to show more generally that $|\mathrm{Aut}(K/F)| \leq [K : F]$ for *any* finite extension K/F (we shall prove this in the next section from a slightly different point of view). This gives us a notion of field extensions with "enough" automorphisms.

Definition. Let K/F be a finite extension. Then K is said to be *Galois* over F and K/F is a *Galois* extension if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois the group of automorphisms $\mathrm{Aut}(K/F)$ is called the *Galois group of K/F*, denoted $\mathrm{Gal}(K/F)$.

Remark: The Galois group of an extension K/F is sometimes defined to be the group of automorphisms $\mathrm{Aut}(K/F)$ for all K/F. We have chosen the definition above so that the notation $\mathrm{Gal}(K/F)$ will emphasize that the extension K/F has the maximal number of automorphisms.

Corollary 6. If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.

We shall see in the next section that the converse is also true, which will completely characterize Galois extensions.

Note also that Corollary 6 implies that the splitting field of *any* polynomial over $\mathbb{Q}$ is Galois, since the splitting field of $f(x)$ is clearly the same as the splitting field of the product of the irreducible factors of $f(x)$ (i.e., the polynomial obtained by removing multiple factors), which is separable (Corollary 13.34).

Definition. If $f(x)$ is a separable polynomial over F, then the *Galois group of $f(x)$ over F* is the Galois group of the splitting field of $f(x)$ over F.

Examples

(1) The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois with Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ where σ is the automorphism

$$\begin{aligned} \sigma : \mathbb{Q}(\sqrt{2}) &\xrightarrow{\sim} \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} &\longmapsto a - b\sqrt{2}. \end{aligned}$$

(2) More generally, any quadratic extension K of any field F of characteristic different from 2 is Galois. This follows from the discussion of quadratic extensions following Corollary 13.13, which shows that any extension K of degree 2 of F (where the characteristic of F is not 2) is of the form $F(\sqrt{D})$ for some D hence is the splitting field of $x^2 - D$ (since if $\sqrt{D} \in K$ then also $-\sqrt{D} \in K$).

(3) The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois since its group of automorphisms is only of order 1.

(4) The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over $\mathbb{Q}$ since it is the splitting field of the polynomial $(x^2-2)(x^2-3)$. Any automorphism σ is completely determined by its action on the generators $\sqrt{2}$ and $\sqrt{3}$, which must be mapped to $\pm\sqrt{2}$ and $\pm\sqrt{3}$, respectively. Hence the only possibilities for automorphisms are the maps

$$\begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \quad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}.$$

Since the Galois group is of order 4, *all* these elements are in fact automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

Define the automorphisms σ and τ by

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

or, more explicitly, by

$$\begin{aligned} \sigma &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ \tau &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \end{aligned}$$

(since, for example,

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = (-\sqrt{2})(\sqrt{3}) = -\sqrt{6} \quad).$$

Then $\sigma^2(\sqrt{2}) = \sigma(\sigma\sqrt{2}) = \sigma(-\sqrt{2}) = \sqrt{2}$ and clearly $\sigma^2(\sqrt{3}) = \sqrt{3}$. Hence $\sigma^2 = 1$ is the identity automorphism. Similarly, $\tau^2 = 1$. The automorphism $\sigma\tau$ can be easily computed:

$$\sigma\tau(\sqrt{2}) = \sigma(\tau(\sqrt{2})) = \sigma(\sqrt{2}) = -\sqrt{2}$$

and

$$\sigma\tau(\sqrt{3}) = \sigma(\tau(\sqrt{3})) = \sigma(-\sqrt{3}) = -\sqrt{3}$$

so that $\sigma\tau$ is the remaining nontrivial automorphism in the Galois group. Since this automorphism also evidently has order 2 in the Galois group, we have

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$$

i.e., the Galois group is isomorphic to the Klein 4-group.

Associated to each subgroup of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ is the corresponding fixed subfield of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. For example, the subfield corresponding to $\{1,\sigma\tau\}$ is the set of elements fixed by the map

$$\sigma\tau : a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$$

which is the set of elements $a+d\sqrt{6}$, i.e., the field $\mathbb{Q}(\sqrt{6})$. One can similarly determine the fixed fields for the other subgroups of the Galois group:

subgroup	fixed field
$\{1\}$	$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$\{1,\sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1,\sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1,\tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1,\sigma,\tau,\sigma\tau\}$	$\mathbb{Q}$

(5) The splitting field of x^3-2 over $\mathbb{Q}$ is Galois of degree 6. The roots of this equation are $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$ where $\rho=\zeta_3=\dfrac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity. Hence the splitting field can be written $\mathbb{Q}(\sqrt[3]{2},\rho\sqrt[3]{2})$. Any automorphism maps each of these two elements to one of the roots of x^3-2, giving 9 possibilities, but since the Galois group has order 6 not every such map is an automorphism of the field.

To determine the Galois group we use a more convenient set of generators, namely $\sqrt[3]{2}$ and ρ. Then any automorphism σ maps $\sqrt[3]{2}$ to one of $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$ and maps ρ to ρ or $\rho^2=\dfrac{-1-\sqrt{-3}}{2}$ since these are the roots of the cyclotomic polynomial $\Phi_3(x)=x^2+x+1$. Since σ is completely determined by its action on these two elements this gives only 6 possibilities and so each of these possibilities is actually an automorphism. To give these automorphisms explicitly, let σ and τ be the automorphisms defined by

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 = -1-\rho. \end{cases}$$

As before, these can be given explicitly on the elements of $\mathbb{Q}(\sqrt[3]{2},\rho)$, which are linear combinations of the basis $\{1,\sqrt[3]{2},(\sqrt[3]{2})^2,\rho,\rho\sqrt[3]{2},\rho(\sqrt[3]{2})^2\}$. For example

$$\begin{aligned}\sigma(\rho\sqrt[3]{2}) &= (\rho)(\rho\sqrt[3]{2}) = \rho^2\sqrt[3]{2} = (-1-\rho)\sqrt[3]{2}\\ &= -\sqrt[3]{2}-\rho\sqrt[3]{2}\end{aligned}$$

and we may similarly determine the action of σ on the other basis elements. This gives

$$\begin{aligned}\sigma :\quad & a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\rho+e\rho\sqrt[3]{2}+f\rho\sqrt[3]{4} \quad \longmapsto \\ & a-e\sqrt[3]{2}+(f-c)\sqrt[3]{4}+d\rho+(b-e)\rho\sqrt[3]{2}-c\rho\sqrt[3]{4}.\end{aligned} \tag{14.1}$$

The other elements of the Galois group are

$$1 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho^2\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases}$$

$$\tau\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho^2 \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases} \qquad \tau\sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

Computing $\sigma\tau$ we have

$$\sigma\tau : \begin{cases} \sqrt[3]{2} \overset{\tau}{\mapsto} \sqrt[3]{2} \overset{\sigma}{\mapsto} \rho\sqrt[3]{2} \\ \rho \overset{\tau}{\mapsto} \rho^2 \overset{\sigma}{\mapsto} \rho^2 \end{cases}$$

i.e.,

$$\sigma\tau : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

so that $\sigma\tau = \tau\sigma^2$. Similarly one computes that $\sigma^3 = \tau^2 = 1$. Hence

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$$

is the symmetric group on 3 letters. Alternatively (and less computationally), since $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$ acts as permutations of the 3 roots of $x^3 - 2$, G is a subgroup of S_3, hence must be S_3 since it is of order 6. The computations above explicitly identify the automorphisms in G and give an explicit isomorphism of G with S_3.

As in the previous example we can determine the fixed fields for any of the subgroups of the Galois group. For example, consider the fixed field of the subgroup $\{1, \sigma, \sigma^2\}$ generated by σ. These are just the elements fixed by σ (given explicitly in equation (1)) since if an element is fixed by σ then it is also fixed by σ^2. (In general, the fixed field of some subgroup is the field fixed by a set of generators for the subgroup.) The elements fixed by σ are those with

$$a = a \quad b = -e \quad c = f - c \quad d = d \quad e = b - e \quad f = -c$$

which is equivalent to $b = c = f = e = 0$. Hence the fixed field of $\{1, \sigma, \sigma^2\}$ is the field $\mathbb{Q}(\rho)$.

Remark: This example shows that some care must be exercised in determining Galois groups from the actions on generators. As mentioned, not every map taking $\sqrt[3]{2}$ and $\rho\sqrt[3]{2}$ to roots of $x^3 - 2$ gives rise to an automorphism of the field (for example, the map

$$\sqrt[3]{2} \mapsto \rho\sqrt[3]{2}$$
$$\rho\sqrt[3]{2} \mapsto \rho\sqrt[3]{2}$$

clearly cannot be an automorphism since it is evidently not an injection). The point is that there may be (sometimes very subtle) algebraic relations among the generators and these relations must be respected by an automorphism. For example, the quotient of the generators here is ρ, which is mapped to 1 and not to a root of the minimal polynomial for ρ. Put another way, the quotient of these generators satisfies a quadratic equation and this map does not respect that property.

For another (less trivial) example, compare with the discussion of the splitting field of $x^8 - 2$ in Section 2.