3 The isomorphism extension theorem

We begin by proving the converse to Lemma 2.5 in a special case. Suppose that $E = F(\alpha)$ is a simple extension of $F$ and let $f = \text{irr}(\alpha, F)$. If $\sigma: F \rightarrow K$ is a homomorphism, $L$ is an extension field of $K$, and $\varphi: E \rightarrow L$ is an extension of $\sigma$, then Lemma 2.5 implies that $\varphi(\alpha)$ is a root of $\sigma(f)$. The following is the converse to this statement.

**Lemma 3.1.** Let $F$ be a field, let $E = F(\alpha)$ be a simple extension of $F$, where $\alpha$ is algebraic over $F$ and $f = \text{irr}(\alpha, F)$, let $\sigma: F \rightarrow K$ be a homomorphism from $F$ to a field $K$, and let $L$ be an extension of $K$. If $\beta \in L$ is a root of $\sigma(f)$, then there is a unique extension of $\sigma$ to a homomorphism $\varphi: E \rightarrow L$ such that $\varphi(\alpha) = \beta$.

Hence there is a bijection from the set of homomorphisms $\varphi: E \rightarrow L$ such that $\varphi(a) = \sigma(a)$ for all $a \in F$ to the set of roots of the polynomial $\sigma(f)$ in $L$, where $\sigma(f) \in K[x]$ is the polynomial obtained by applying the homomorphism $\sigma$ to coefficients of $f$.

**Proof.** Let $\beta \in L$ be a root of $\sigma(f)$. We know by basic field theory that there is an isomorphism $\rho: F(\alpha) \cong F[x]/(f)$ with the property that $\rho(a) = a + (f)$ for $a \in F$ and $\rho(\alpha) = x + (f)$. Here $\rho = \tilde{\text{ev}}_{\alpha}^{-1}$, where $\tilde{\text{ev}}_{\alpha}: F[x]/(f) \rightarrow F(\alpha)$ is the isomorphism induced by ev$_\alpha: F[x] \rightarrow F(\alpha)$ with Ker ev$_\alpha = (f)$.

Let $\text{ev}_\beta \circ \sigma$ be the homomorphism $F[x] \rightarrow L$ defined as follows: given a polynomial $g \in F[x]$, let (as above) $\sigma(g)$ be the polynomial obtained by applying $\sigma$ to the coefficients of $g$, and let $\text{ev}_\beta \circ \sigma(g) = \sigma(g)(\beta) = \text{ev}_\beta(\sigma(g))$ be the evaluation of $\sigma(g)$ at $\beta$. Then $\text{ev}_\beta \circ \sigma$ is a homomorphism from $F[x]$ to $K$. For $a \in F$, $\text{ev}_\beta \circ \sigma(a) = \sigma(a)$, and $\text{ev}_\beta \circ \sigma(x) = \beta$. Moreover $f \in \text{Ker ev}_\beta \circ \sigma$, since $\sigma(f)(\beta) = 0$ by hypothesis. Thus $(f) \subseteq \text{Ker ev}_\beta \circ \sigma$ and hence $(f) = \text{Ker ev}_\beta \circ \sigma$ since $(f)$ is a maximal ideal and $\text{ev}_\beta \circ \sigma$ is not the trivial homomorphism. Then there is an induced homomorphism $e : F[x]/(f) \rightarrow L$. Let $\varphi$ be the induced homomorphism $e \circ \rho: F(\alpha) \rightarrow L$. It is easily checked to satisfy: $\varphi(a) = \sigma(a)$ for all $a \in F$ and $\varphi(\alpha) = \beta$. 

10
Next we claim that $\varphi$ is uniquely specified by the conditions $\varphi(a) = \sigma(a)$ for all $a \in F$ and $\varphi(\alpha) = \beta$. In fact, every element of $E = F(\alpha)$ can be written as $\sum_{i=0}^{N} a_i \alpha^i$ for some $a_i \in N$. Then
\[
\varphi(\sum_{i=0}^{N} a_i \alpha^i) = \sum_{i=0}^{N} \varphi(a_i) \varphi(\alpha)^i = \sum_{i=0}^{N} \sigma(a_i) \beta^i.
\]
Thus $\varphi$ is uniquely specified by the conditions above. In summary, then, every extension $\varphi$ of $\sigma$ satisfies: $\varphi(\alpha)$ is a root of $\sigma(f)$, $\varphi$ is uniquely determined by the value $\varphi(\alpha) \in L$, and all possible roots of $\sigma(f)$ in $L$ arise as $\varphi(\alpha)$ for some extension $\varphi$ of $\sigma$. Thus the function $\varphi \mapsto \varphi(\alpha)$ is a function from the set of extensions $\varphi$ of $\sigma$ to the set of roots of $\sigma(f)$ in $L$. This function is injective (by the uniqueness statement) and surjective (by the existence statement), and thus defines the bijection in the second paragraph of the statement of the lemma.

**Corollary 3.2.** Let $E$ be a finite extension of a field $F$, and suppose that $E = F(\alpha)$ for some $\alpha \in E$, i.e. $E$ is a simple extension of $F$. Let $K$ be a field and let $\sigma : F \to K$ be a homomorphism. Then:

(i) For every extension $L$ of $K$, there exist at most $[E : F]$ homomorphisms $\varphi : E \to L$ extending $\sigma$, i.e. such that $\varphi(\alpha) = \sigma(\alpha)$ for all $\alpha \in F$.

(ii) There exists an extension field $L$ of $K$ and a homomorphism $\varphi : E \to L$ extending $\sigma$.

(iii) If $F$ has characteristic zero (or $F$ is finite or more generally perfect), then there exists an extension field $L$ of $K$ such that there are exactly $[E : F]$ homomorphisms $\varphi : E \to L$ extending $\sigma$.

**Proof.** Let $n = \deg f = [E : F]$. Then $\deg \sigma(f) = n$ as well. Lemma 3.1 implies that the extensions of $\sigma$ to a homomorphism $\varphi : F(\alpha) \to L$ are in one-to-one correspondence with the $\beta \in K$ such that $\beta$ is a root of $\sigma(f)$, where $f = \text{irr}(\alpha, F)$. In this case, since $\sigma(f)$ has at most $n = [E : F]$ roots in any extension field $L$, there are at most $n$ extensions of $\sigma$, proving (i). To see (ii), choose an extension field $L$ of $K$ such that $\sigma(f)$ has a root $\beta$ in $L$. Thus there will be at least one homomorphism $\varphi : F(\alpha) \to L$ extending $\sigma$.

To see (iii), choose an extension field $L$ of $K$ such that $\sigma(f)$ factors into a product of linear factors in $L$. Under the assumption that the characteristic of $F$ is zero, or $F$ is finite or perfect, the irreducible polynomial $f \in F[x]$ has no multiple roots in any extension field, and the same will be true of the
polynomial $\sigma(f) \in \sigma(F)[x]$, where $\sigma(F)$ is the image of $F$ in $K$, since $\sigma(f)$ is also irreducible. Thus there are $n$ distinct roots of $\sigma(f)$ in $L$, and hence $n$ different extensions of $\sigma$ to a homomorphism $\varphi : F(\alpha) \to L$. \hfill \Box$

The situation of fields in the second and third statements of the corollary can be summarized by the following diagram:

$$
\begin{array}{ccc}
E & \longrightarrow & L \\
\sigma & \quad & \\
F & \longrightarrow & K
\end{array}
$$

Let us give some examples to show how one can use Lemma 3.1, especially in case the homomorphism $\sigma$ is not the identity:

**Example 3.3.** (1) Consider the sequence of extensions $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. As we have seen, there are two different automorphisms of $\mathbb{Q}(\sqrt{2})$, $\text{Id}$ and $\psi$, where $\psi(a + b\sqrt{2}) = a - b\sqrt{2}$. We have seen that $f = x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$. Since in fact $f \in \mathbb{Q}[x]$, $\sigma(f) = f$, and clearly $\text{Id}(f) = f$. In particular, the roots of $\sigma(f) = f$ are $\pm \sqrt{3}$. Applying Lemma 3.1 to the case $F = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = K$, and $\sigma = \text{Id}$ or $\sigma = \psi$, we see that there are two extensions of $\text{Id}$ to a homomorphism (necessarily an automorphism) $\varphi : E \to E$. One of these satisfies $\varphi(\sqrt{3}) = \sqrt{3}$, hence $\varphi = \text{Id}$, and the other satisfies $\varphi(\sqrt{3}) = -\sqrt{3}$, hence $\varphi = \sigma_2$ in the notation of (3) of Example 2.10. Likewise, there are two extensions of $\psi$ to an automorphism $\varphi : E \to E$. One of these satisfies $\varphi(\sqrt{3}) = \sqrt{3}$, hence $\varphi = \sigma_1$, and the other satisfies $\varphi(\sqrt{3}) = -\sqrt{3}$, hence $\varphi = \sigma_3$ in the notation of (3) of Example 2.10. In particular, we see that $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ has order 4, giving another argument for (3) of Example 2.10.

(2) Taking $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, and $K = \mathbb{Q}(\sqrt{2}, \omega)$, we see that there are three injective homomorphisms from $E$ to $K$ since there are three roots in $K$ of the polynomial $x^3 - 2 = \text{irr}(\sqrt{2}, \mathbb{Q})$, namely $\sqrt{2}$, $\omega \sqrt{2}$, and $\omega^2 \sqrt{2}$. On the other hand, consider also the sequence $\mathbb{Q} \leq \mathbb{Q}(\omega) \leq \mathbb{Q}(\sqrt{2}, \omega)$. As we have seen, if the roots of $x^3 - 2$ in $\mathbb{C}$ are labeled as $\alpha_1 = \sqrt{2}$, $\alpha_2 = \omega \sqrt{2}$, and $\alpha_3 = \omega^2 \sqrt{2}$ and $\sigma$ is complex conjugation, then $\sigma$ corresponds to the permutation $(23)$. We claim that $f = x^3 - 2$ is irreducible in $\mathbb{Q}(\omega)$. In fact, since $\deg f = 3$, $f$ is reducible in $\mathbb{Q}(\omega) \iff$ there exists a root $\alpha$ of $f$ in $\mathbb{Q}(\omega)$. But then $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\omega)$ and we would have $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$
dividing $2 = [\mathbb{Q}(\omega) : \mathbb{Q}]$, which is impossible. Hence $x^3 - 2$ is irreducible in $\mathbb{Q}(\omega)[x]$. (Alternatively, note that $\omega \notin \mathbb{Q}(\sqrt[3]{2})$ since $\omega$ is not real but $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$, hence

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 6$$

and so $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)] = 3$.)

Considering the simple extension $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ of $\mathbb{Q}(\omega)$, we see that the homomorphisms of $K$ into $K$ (necessarily automorphisms) which are the identity on $\mathbb{Q}(\omega)$, i.e. the elements of $\text{Gal}(K/\mathbb{Q}(\omega))$, correspond to the roots of $x^3 - 2$ in $K$. Thus for example, there is an automorphism $\rho : \mathbb{Q}(\sqrt[3]{2}, \omega) \to \mathbb{Q}(\sqrt[3]{2}, \omega)$ such that $\rho(\omega) = \omega$ and $\rho(\sqrt[3]{2}) = \omega \sqrt[3]{2}$. This completely specifies $\rho$. For example, the above says that $\rho(\alpha_1) = \alpha_2$. Also,

$$\rho(\alpha_2) = \rho(\omega \sqrt[3]{2}) = \rho(\omega)\rho(\sqrt[3]{2}) = \omega \cdot \omega \sqrt[3]{2} = \omega^2 \sqrt[3]{2} = \alpha_3.$$

Similarly $\rho(\alpha_3) = \alpha_1$. So $\rho$ corresponds to the permutation (123). Then $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ is isomorphic to a subgroup of $S_3$ containing a 2-cycle and a 3-cycle and hence is isomorphic to $S_3$.

(3) Consider the case of $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q})$, with $\beta_1 = \sqrt[3]{2}$, $\beta_2 = i \sqrt[3]{2}$, $\beta_3 = -\sqrt[3]{2}$, and $\beta_4 = -i \sqrt[3]{2}$. Then if $\varphi \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q})$, it follows that $\varphi(\beta_1) = \beta_k$ for some $k$, $1 \leq k \leq 4$ and $\varphi(i) = \pm i$. In particular $\#(\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q})) \leq 8$. As in (2), complex conjugation $\sigma$ is an element of $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q})$ corresponding to $(24) \in S_4$. Next we claim that $x^4 - 2$ is irreducible in $\mathbb{Q}(i)$. In fact, there is no root of $x^4 - 2$ in $\mathbb{Q}(i)$, either by inspection (the $\beta_i$ are not elements of $\mathbb{Q}(i)$) or because $x^4 - 2$ is irreducible in $\mathbb{Q}[x]$ and $4 = \deg(x^4 - 2)$ does not divide $2 = [\mathbb{Q}(i) : \mathbb{Q}]$. If $x^4 - 2$ factors into a product of quadratic polynomials in $\mathbb{Q}(i)[x]$, then a homework problem says that $\pm 2$ is a square in $\mathbb{Q}(i)$. But $2 = (a + bi)^2$ implies either $a$ or $b$ is 0 and $2 = a^2$ or $2 = -b^2$ where $a$ or $b$ are rational, both impossible. Hence $x^4 - 2$ is irreducible in $\mathbb{Q}(i)$. (Here is another argument that $x^4 - 2$ is irreducible in $\mathbb{Q}(i)$: As in (2), we could note that $i \notin \mathbb{Q}(\sqrt[3]{2})$ since $i$ is not real but $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$, hence

$$[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 8$$

and so $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(i)] = 4$.)

As $\mathbb{Q}(\sqrt[3]{2}, i)$ is then a simple extension of $\mathbb{Q}(i)$ corresponding to the polynomial $x^4 - 2$ which is irreducible in $\mathbb{Q}(i)[x]$, a homomorphism from $\mathbb{Q}(\sqrt[3]{2}, i)$
to $\mathbb{Q}(\sqrt{2}, i)$ which is the identity on $\mathbb{Q}(i)$ corresponds to the choice of a root of $x^4 - 2$ in $\mathbb{Q}(\sqrt{2}, i)$. In particular, there exists $\rho \in \text{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(i)) \leq \text{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ such that $\rho(i) = i$ and $\rho(i) = \beta$. Then $\rho(\beta) = \rho(i\beta_1) = \rho(i)\rho(\beta_1) = \beta_2 = \beta_3$ and likewise $\rho(\beta_3) = \rho(-\beta_1) = -\rho(\beta_1) = -\beta_2 = \beta_4$ and $\rho(\beta_4) = \beta_1$.

It follows that $\rho$ corresponds to $(1234) \in S_4$. From this it is easy to see that the image of the Galois group in $S_4$ is the dihedral group $D_4$.

Another way to see that, unlike in the previous example, the Galois group is not all of $S_4$ is as follows: the roots $\beta_1, \beta_2, \beta_3, \beta_4$ satisfy: $\beta_3 = -\beta_1$ and $\beta_4 = -\beta_2$. Thus, if $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$, then $\sigma(\beta_3) = -\sigma(\beta_1)$ and $\sigma(\beta_4) = -\sigma(\beta_2)$. This says that not all permutations of the set $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ can arise; for example, $(1243)$ is not possible.

The following is one of many versions of the isomorphism extension theorem for finite extensions of fields. It eliminates the hypothesis that $E$ is a simple extension of $F$.

**Theorem 3.4 (Isomorphism Extension Theorem).** Let $E$ be a finite extension of a field $F$. Let $K$ be a field and let $\sigma : F \to K$ be a homomorphism. Then:

(i) There exist at most $[E : F]$ homomorphisms $\varphi : E \to K$ extending $\sigma$, i.e. such that $\varphi(\alpha) = \sigma(\alpha)$ for all $\alpha \in F$.

(ii) There exists an extension field $L$ of $K$ and a homomorphism $\varphi : E \to L$ extending $\sigma$.

(iii) If $F$ has characteristic zero (or $F$ is finite or more generally perfect), then there exists an extension field $L$ of $K$ such that there are exactly $[E : F]$ homomorphisms $\varphi : E \to L$ extending $\sigma$.

**Proof.** Since $E$ is a finite extension of $F$, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in E$. The proof is by induction on $n$. The case $n = 1$, i.e. the case of a simple extension, is true by Corollary 3.2.

In the general case, with $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in E$, let $F_1 = F(\alpha_1, \ldots, \alpha_{n-1})$ and let $\alpha = \alpha_n$, so that $E = F_1(\alpha)$. We thus have a sequence of extensions $F \leq F_1 \leq E$. Notice that, given an extension of $\sigma$ to a homomorphism $\varphi : F_1 \to K$ and an extension $\tau$ of $\varphi$ to a homomorphism $E \to K$, the homomorphism $\tau$ is also an extension of $\sigma$ to a homomorphism $E \to K$. Conversely, a homomorphism $\tau : E \to K$ extending $\sigma$ defines an extension $\varphi$ of $\sigma$ to $F_1$, by taking $\varphi(\alpha) = \tau(\alpha)$ for $\alpha \in F_1$ (i.e. $\varphi$ is the restriction of $\tau$ to $F_1$), and clearly $\tau$ is an extension of $\varphi$ to $F_1$. 

14
By assumption, $E = F_1(\alpha)$ and the inductive hypothesis applies to the extension $F_1$ of $F$. Given a homomorphism $\sigma : F \to K$, where $K$ is a field, by induction, there exist at most $[F_1 : F]$ extensions of $\sigma$ to a homomorphism $F_1 \to K$. Suppose that the set of all such homomorphisms is $\{\varphi_1, \ldots, \varphi_r\}$, with $r \leq [F_1 : F]$. Fix one such homomorphism $\varphi_i$. Applying Corollary 3.2 to the simple extension $F_1(\alpha) = E$ and the homomorphism $\varphi_i : F_1 \to K$, there are at most $s$ extensions of $\varphi_i$ to a homomorphism $\tau_i : F_1(\alpha) \to K$, where $s = [F_1(\alpha) : F_1] = [E : F_1]$. In all, since each of the $r$ extensions $\varphi_i$ has at most $s$ extensions to a homomorphism from $E$ to $K$, there are at most $rs$ extensions of $\sigma$ to a homomorphism $E \to K$. As $r \leq [F_1 : F]$ and $s = [E : F_1]$, we see that there are at most $[F_1 : F] [E : F_1] = [E : F]$ extensions of $\sigma$ to a homomorphism $E \to K$. This completes the inductive step for the proof of (i).

The proofs of (ii) and (iii) are similar. To see (ii), use the inductive hypothesis to find a field $F$ containing $\alpha$ and an extension of $\sigma$ to a homomorphism $\sigma_1 : F_1 \to L_1$. Let $f_1 = \text{irr}(\alpha, F_1)$. Adjoining a root of $\sigma_1(f_1)$ to $L_1$ if necessary, to obtain an extension field $L$ of $L_1$ containing a root of $\sigma_1(f_1)$, it follows from Corollary 3.2 that there exists a homomorphism $\varphi : F_1(\alpha) = E \to L$ extending $\sigma_1$, and hence extending $\sigma$. This completes the inductive step for the proof of (ii).

Finally, to see (iii), we examine the proof of the inductive step for (i) more carefully. Let $F$ be a field of characteristic zero (or more generally a field such that every irreducible polynomial in $F[x]$ does not have a multiple root in any extension field of $F$). Given the homomorphism $\sigma : F \to K$, where $K$ is a field, by the inductive hypothesis, after enlarging the field $K$ to some extension field $L_1$ if necessary, there exist exactly $[F_1 : F]$ extensions of $\sigma$ to a homomorphism $F_1 \to L_1$. Suppose that the set of all such homomorphisms is $\{\varphi_1, \ldots, \varphi_d\}$, with $d = [F_1 : F]$. As before, we let $f_1 = \text{irr}(\alpha, F_1)$. There exists a finite extension $L$ of the field $L_1$ such that every one of the (not necessarily distinct) irreducible polynomials $\varphi_i(f_1) \in \varphi_i(F_1)[x]$ splits into linear factors in $L$, and hence has $e$ distinct roots in $L$, where $e = \deg f_1 = [F_1(\alpha) : F_1] = [E : F_1]$. Fix one such homomorphism $\varphi_i$. Again applying Corollary 3.2 to the simple extension $F_1(\alpha) = E$ and the homomorphism $\varphi_i : F_1 \to L$, there are exactly $e$ extensions of $\varphi_i$ to a homomorphism $\tau_{ij} : F_1(\alpha) \to L$. In all, since each of the $d$ extensions $\varphi_i$ has $e$ extensions to a homomorphism from $E$ to $L$, there are exactly $de$ extensions of $\sigma$ to a homomorphism $E \to L$. As $d = [F_1 : F]$ and $e = [E : F_1]$, we see that there are exactly $[F_1 : F][E : F_1] = [E : F]$
extensions of $\sigma$ to a homomorphism $E \to L$. This completes the inductive step for the proof of (iii), and hence the proof of the theorem.

Clearly, the first statement of the Isomorphism Extension Theorem implies the following (take $K = E$ in the statement):

**Corollary 3.5.** Let $E$ be a finite extension of $F$. Then
$$
\#(\text{Gal}(E/F)) \leq [E : F].
$$

**Definition 3.6.** Let $E$ be a finite extension of $F$. Then $E$ is a separable extension of $F$ if, for every extension field $K$ of $F$, there exists an extension field $L$ of $K$ such that there are exactly $[E : F]$ homomorphisms $\varphi: E \to L$ with $\varphi(a) = a$ for all $a \in F$.

For example, if $F$ has characteristic zero or is finite or more generally is perfect, then every finite extension of $F$ is separable. It is not hard to show that, if $E$ is a finite extension of $F$, then $E$ is a separable extension of $F$ if and only if the polynomial $\text{irr}(\alpha, F)$ does not have multiple roots.

One basic fact about separable extensions, which we shall prove later, is:

**Theorem 3.7** (Primitive Element Theorem). Let $E$ be a finite separable extension of a field $F$. Then there exists an element $\alpha \in E$ such that $E = F(\alpha)$. In other words, every finite separable extension is a simple extension.

There are two reasons why, in the situation of Corollary 3.5, we might have strict inequality, i.e. $\#(\text{Gal}(E/F)) < [E : F]$. The first is that the extension might not be separable. As we have seen, this situation does not occur if $F$ has characteristic zero, and is in general somewhat anomalous. More importantly, though, we might, in the situation of the Isomorphism Extension Theorem, be able to construct $[E : F]$ homomorphisms $\varphi: E \to L$, where $L$ is some extension field of $E$, without being able to guarantee that $\varphi(E) = E$. For example, let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2})$, with $[E : F] = 3$. Let $L$ be an extension field of $\mathbb{Q}$ which contains the three cube roots of 2, namely $\sqrt[3]{2}$, $\omega \sqrt[3]{2}$, and $\omega^2 \sqrt[3]{2}$, where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. For example, we could take $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Then there are three homomorphisms $\varphi: E \to L$, but only one of these has image equal to $E$. We will fix this problem in the next section.

### 4 Splitting fields

**Definition 4.1.** Let $F$ be a field and let $f \in F[x]$ be a polynomial of degree at least 1. Then an extension field $E$ of $F$ is a splitting field for $f$ over $F$ if the following two conditions hold:
(i) In $E[x]$, there is a factorization $f = c \prod_{i=1}^{n}(x - \alpha_i)$. In other words, $f$ factors in $E[x]$ into a product of linear factors.

(ii) With the notation of (i), $E = F(\alpha_1, \ldots, \alpha_n)$. In other words, $E$ is generated as an extension field of $F$ by the roots of $f$.

Here the name “splitting field” means that, in $E[x]$, the polynomial $f$ splits into linear factors.

**Remark 4.2.** (i) Clearly, $E$ is a splitting field of $f$ over $F$ if (i) holds (factors in $E[x]$ into a product of linear factors) and there exist some subset $\{\alpha_1, \ldots, \alpha_k\}$ of the roots of $f$ such that $E = F(\alpha_1, \ldots, \alpha_k)$ (because, if $\alpha_{k+1}, \ldots, \alpha_n$ are the remaining roots, then they are in $E$ by (i) and thus $E = E(\alpha_{k+1}, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_k)(\alpha_{k+1}, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$).

(ii) If $E$ is a splitting field of $f$ over $F$ and $K$ is an intermediate field, i.e. $F \leq K \leq E$, then $E$ is also a splitting field of $f$ over $K$.

One can show that any two splitting fields of $f$ over $F$ are isomorphic, via an isomorphism which is the identity on $F$, and we sometimes refer incorrectly to the splitting field of $f$ over $F$.

**Example 4.3.**

1. The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$. More generally, if $F$ is any field, $f \in F[x]$ is an irreducible polynomial of degree 2, and $E = F(\alpha)$, where $\alpha$ is a root of $f$, then $E$ is a splitting field of $f$, since in $E[x]$, $f = (x - \alpha)g$, where $g$ has degree one, hence is linear, and $E$ is clearly generated over $F$ by the roots of $f$.

2. The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. However, $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field of $x^3 - 2$ over $\mathbb{Q}$, since $x^3 - 2$ is not a product of linear factors in $\mathbb{Q}(\sqrt[3]{2})[x]$.

3. The splitting field of $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\pm \sqrt[4]{2}, \pm i \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.

4. The splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note in particular that, in the definition of a splitting field, we do not assume that $f$ is irreducible. Also, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is not a splitting field of $x^2 - 2$ over $\mathbb{Q}$, since $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \neq \mathbb{Q}(\pm \sqrt{2})$.

5. The splitting field of $x^4 - 10x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, because all of the roots $\pm \sqrt{2} \pm \sqrt{3}$ lie in $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is generated by the roots of $x^4 - 10x^2 + 1$. 

17
6. The splitting field of \( x^5 - 1 \) over \( \mathbb{Q} \) is the same as the splitting field of \( x^4 + x^3 + x^2 + x + 1 = \Phi_5 \) over \( \mathbb{Q} \), namely \( \mathbb{Q}(\zeta) \), where \( \zeta = e^{2\pi i/5} \). This follows since every root of \( x^5 - 1 \) is a 5\(^{th}\) root of unity and hence equal to \( \zeta^i \) for some \( i \). Note that, as \( \Phi_5 \) is irreducible in \( \mathbb{Q}[x] \), \( [\mathbb{Q}(\zeta) : \mathbb{Q}] = 4 \). More generally, if \( \zeta \) is any generator of \( \mu_n \), the group of \( n \)\(^{th}\) roots of unity, for example if \( \zeta = e^{2\pi i/n} \), then \( \mu_n = \langle \zeta \rangle \) and

\[
x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta^i).
\]

Hence \( \mathbb{Q}(\zeta) \) is a splitting field for \( x^n - 1 \) over \( \mathbb{Q} \).

7. With \( F = \mathbb{F}_p \) and \( q = p^n \) (\( p \) a prime number), the splitting field of the polynomial \( x^q - x \) over \( \mathbb{F}_p \) is \( \mathbb{F}_q \).

**Remark 4.4.** In a sense, examples 3, 5 and 6 are misleading, because for a "random" irreducible polynomial \( f \in \mathbb{Q}[x] \) of degree \( n \), the expectation is that the degree of a splitting field of \( f \) will be \( n! \). In other words, if \( f \in \mathbb{Q}[x] \) is a "random" irreducible polynomial and \( \alpha_1 \) is some root of \( f \) in an extension field of \( \mathbb{Q} \), then we know that, in \( \mathbb{Q}(\alpha_1)[x] \), \( f = (x - \alpha_1)f_1 \) with \( \deg f_1 = n - 1 \). But there is no reason in general to expect that \( \mathbb{Q}(\alpha_1) \) contains any other root of \( f \), or equivalently a root of \( f_1 \), or even to expect that \( f_1 \) is reducible in \( \mathbb{Q}(\alpha_1) \). Thus we would expect in general that, if \( \alpha_2 \) is a root of \( f_1 \) in some extension field of \( \mathbb{Q}(\alpha_1) \), then \( [\mathbb{Q}(\alpha_1)(\alpha_2) : \mathbb{Q}(\alpha_1)] = n - 1 \) and hence \( [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] = n(n - 1) \). Then \( f = (x - \alpha_1)(x - \alpha_2)f_2 \in \mathbb{Q}(\alpha_1, \alpha_2) \). Continuing in this way, our expectation is that a splitting field for \( f \) over \( \mathbb{Q} \) is of the form \( \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \) with \( [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}] = n(n - 1) \cdots 2 \cdot 1 = n! \).

The following relates the concept of a splitting field to the problem of constructing automorphisms:

**Theorem 4.5.** Let \( E \) be a finite extension of a field \( F \). Then the following are equivalent:

(i) There exists a polynomial \( f \in F[x] \) of degree at least one such that \( E \) is a splitting field of \( f \).

(ii) For every extension field \( L \) of \( E \), if \( \varphi : E \to L \) is a homomorphism such that \( \varphi(a) = a \) for all \( a \in F \), then \( \varphi(E) = E \), and hence \( \varphi \) is an automorphism of \( E \).
(iii) For every irreducible polynomial \( p \in F[x] \), if there is a root of \( p \) in \( E \), then \( p \) factors into a product of linear factors in \( E[x] \).

**Proof.** (i) \( \implies \) (ii): We begin with a lemma:

**Lemma 4.6.** Let \( L \) be an extension field of a field \( F \) and let \( \alpha_1, \ldots, \alpha_n \in L \). If \( \varphi \colon E = F(\alpha_1, \ldots, \alpha_n) \to L \) is a homomorphism, then \( \varphi(E) = \varphi(F)(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)) \).

**Proof.** The proof is by induction on \( n \). If \( n = 1 \) and \( \alpha = \alpha_1 \), then every element of \( F(\alpha) \) is of the form \( \sum_i a_i \alpha^i \). Then \( \varphi(\sum_i a_i \alpha^i) = \sum_i \varphi(a_i)(\varphi(\alpha))^i \) and hence
\[
\varphi(F(\alpha)) = \left\{ \sum_i \varphi(a_i)(\varphi(\alpha))^i : a_i \in F \right\} = \varphi(F)(\varphi(\alpha)).
\]
For the inductive step, applying the case \( n = 1 \) to the field \( F(\alpha_1, \ldots, \alpha_{n-1}) \), we see that
\[
\varphi(F(\alpha_1, \ldots, \alpha_n)) = \varphi(F(\alpha_1, \ldots, \alpha_{n-1}))(\alpha_n) = \varphi(F(\alpha_1, \ldots, \alpha_{n-1}))(\varphi(\alpha_n))
\]
\[
= \varphi(F(\varphi(\alpha_1), \ldots, \varphi(\alpha_{n-1}))(\varphi(\alpha_n)) = \varphi(F)(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)),
\]
completing the proof of the inductive step. \( \square \)

Returning to the proof of the theorem, by assumption, \( E = F(\alpha_1, \ldots, \alpha_n) \), where \( f = c \prod_{i=1}^n (x - \alpha_i) \). In particular, every root of \( f \) in \( L \) already lies in \( E \). If \( \varphi \colon E \to L \) is a homomorphism such that \( \varphi(a) = a \) for all \( a \in F \), then \( \varphi(\alpha_i) = \alpha_j \) for some \( j \), hence \( \varphi(\{\alpha_1, \ldots, \alpha_n\}) \subseteq \{\alpha_1, \ldots, \alpha_n\} \). Since \( \{\alpha_1, \ldots, \alpha_n\} \) is finite set and \( \varphi \) is injective, it induces a surjective map from \( \{\alpha_1, \ldots, \alpha_n\} \) to itself, i.e. \( \varphi \) permutes the roots of \( f \) in \( E \leq L \). By Lemma 4.6, \( \varphi(E) = \varphi(F)(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)) = F(\alpha_1, \ldots, \alpha_n) = E \). Thus \( \varphi \) is an automorphism of \( E \).

(ii) \( \implies \) (iii): Let \( p \in F[x] \) be irreducible, and suppose that there exists a \( \beta \in E \) such that \( p(\beta) = 0 \). There exists an extension field \( K \) of \( E \) such that \( p \) is a product \( c \prod_j (x - \beta_j) \) of linear factors in \( K[x] \), where \( \beta = \beta_1 \), say. For any \( j \), since \( \beta = \beta_1 \) and \( \beta_j \) are both roots of the irreducible polynomial \( p \), there exists an isomorphism \( \sigma : F(\beta_1) \to F(\beta_j) \leq K \). Applying (ii) of the Isomorphism Extension Theorem to the homomorphism \( \sigma : F(\beta_1) \to K \) and the extension field \( E \) of \( F(\beta_1) \), there exists an extension field \( L \) of \( K \) (hence \( L \) is an extension of \( E \) and of \( F \), since \( E \) and \( F \) are subfields of \( K \)), and a homomorphism \( \varphi : E \to L \) such that \( \varphi(a) = \sigma(a) \) for all \( a \in F(\beta_1) \). In particular, \( \varphi(a) = a \) for all \( a \in F \). By the hypothesis of (ii), it follows that
\( \varphi(E) = E \). But by construction \( \varphi(\beta_j) = \sigma(\beta_j) = \beta_j \), so \( \beta_j \in E \) for every root \( \beta_j \) of \( p \). It follows that \( p \) is a product \( c \prod_j (x - \beta_j) \) of linear factors in \( E[x] \).

(iii) \( \implies \) (i): Since \( E \) is in any case a finite extension of \( F \), there exist \( \alpha_1, \ldots, \alpha_n \in E \) such that \( E = F(\alpha_1, \ldots, \alpha_n) \). For each \( i \), let \( p_i = \text{irr}(\alpha_i, F) \). Then \( p_i \) is an irreducible polynomial with a root in \( E \). By the hypothesis of (iii), \( p_i \) is a product of linear factors in \( E[x] \). Let \( f \) be the product \( p_1 \cdots p_n \). Then \( f \) is a product of linear factors in \( E[x] \), since each of its factors \( p_i \) is a product of linear factors, and \( E \) is generated over \( F \) by some subset of the roots of \( f \) and hence by all of the roots (see the comment after the definition of a splitting field). Thus \( E \) is a splitting field of \( f \).

**Definition 4.7.** Let \( E \) be a finite extension of \( F \). If any one of the equivalent conditions of the preceding theorem is fulfilled, we say that \( E \) is a normal extension of \( F \).

**Corollary 4.8.** Let \( E \) be a finite extension of a field \( F \). Then the following are equivalent:

(i) \( E \) is a separable extension of \( F \) (this is automatic if the characteristic of \( F \) is 0 or \( F \) is finite or perfect) and \( E \) is a normal extension of \( F \).

(ii) \( \#(\operatorname{Gal}(E/F)) = [E: F] \).

**Proof.** We shall just prove that (i) \( \implies \) (ii). Applying the definition that \( E \) is a separable extension of \( F \) to the case where \( K = E \), we see that there exists an extension field \( L \) of \( E \) and \( [E: F] \) homomorphisms \( \varphi: E \to L \) such that \( \varphi(a) = a \) for all \( a \in F \). By the (easy) implication (i) \( \implies \) (ii) of Theorem 4.5, \( \varphi(E) = E \), i.e. \( \varphi \) is an automorphism of \( E \) and hence \( \varphi \in \operatorname{Gal}(E/F) \). Conversely, every element of \( \operatorname{Gal}(E/F) \) is a homomorphism from \( E \) to \( L \) which is the identity on \( F \). Hence \( \#(\operatorname{Gal}(E/F)) = [E: F] \).

**Definition 4.9.** A finite extension \( E \) of a field \( F \) is a Galois extension of \( F \) if and only if \( \#(\operatorname{Gal}(E/F)) = [E: F] \). Thus, the preceding corollary can be rephrased as saying that \( E \) is a Galois extension of \( F \) if and only if \( E \) is a normal and separable extension of \( F \).

**Example 4.10.** We can now redo the determination of the Galois groups \( \operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \) and \( \operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q}) \) much more efficiently. For example, since \( [\mathbb{Q}(\sqrt[3]{2}, \omega): \mathbb{Q}] = 6 \) and \( \mathbb{Q}(\sqrt[3]{2}, \omega) \) is a splitting field for the polynomial \( x^3 - 2 \), we know that the order of \( \operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \) is 6. Since there is an injective homomorphism from \( \operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \) to \( S_3 \), this implies that
Gal(Q(\sqrt[4]{2}, \omega)/Q) \cong S_3 and that every permutation of the roots \{\alpha_1, \alpha_2, \alpha_3\} (notation as in Example 3.3(2)) arises via an element of the Galois group.

In addition, for every \( i, 1 \leq i \leq 3 \), there exists a unique element \( \sigma_1 \) of Gal(Q(\sqrt[4]{2}, \omega)/Q) such that \( \sigma_1(\alpha_1) = \alpha_i \) and \( \sigma_1(\omega) = \omega \), and a unique element \( \sigma_2 \) of Gal(Q(\sqrt[4]{2}, \omega)/Q) such that \( \sigma_2(\alpha_1) = \alpha_i \) and \( \sigma_2(\omega) = \bar{\omega} \).

A very similar argument handles the case of Gal(Q(\sqrt[2]{2}, i)/Q): Setting

\[
\beta_1 = \sqrt[2]{2}; \quad \beta_2 = i \sqrt[2]{2}; \quad \beta_3 = -\sqrt[2]{2}; \quad \beta_4 = -i \sqrt[2]{2},
\]

every \( \sigma \in \text{Gal}(Q(\sqrt[2]{2}, i)/Q) \) takes \( \beta_1 = \sqrt[2]{2} \) to some \( \beta_i \) and takes \( i \) to \( \pm i \), and every possibility has to occur since the order of \( \text{Gal}(Q(\sqrt[2]{2}, i)/Q) \) is 8. Thus for example there exists a \( \rho \in \text{Gal}(Q(\sqrt[2]{2}, i)/Q) \) such that \( \rho(\sqrt[2]{2}) = i \sqrt[2]{2} \) and \( \rho(i) = i \). It follows that

\[
\rho(\beta_2) = \rho(i \sqrt[2]{2}) = \rho(i)\rho(\sqrt[2]{2}) = i^2 \sqrt[2]{2} = -\sqrt[2]{2} = \rho(\beta_3),
\]

and similarly that \( \rho(\beta_3) = \beta_4 \) and that \( \rho(\beta_4) = \beta_1 \). Hence \( \rho \) corresponds to the permutation (1234), and as before it is easy to check from this that \( \text{Gal}(Q(\sqrt[2]{2}, i)/Q) \cong D_4 \).

**Example 4.11.** If \( p \) is a prime number and \( q = p^n \), then \( F_q \) is a separable extension of \( F_p \) since \( F_p \) is perfect and it is normal since it is a splitting field of \( x^q - x \) over \( F_p \). Thus \( F_q \) is a Galois extension of \( F_p \). The order of the Galois group \( \text{Gal}(F_q/F_p) \) is thus \( [F_q : F_p] = n \). On the other hand, we claim that, if \( \sigma_p \) is the Frobenius automorphism, then the order of \( \sigma_p \) in \( \text{Gal}(F_q/F_p) \) is exactly \( n \): clearly, \( \sigma_p^k = \text{Id} \iff \sigma_p^k(\alpha) = \alpha \) for all \( \alpha \in F_q \). Moreover, by our computations on finite fields, \( (\sigma_p)^k = \sigma_{p^k} \), and \( \sigma_{p^k}(\alpha) = \alpha \iff \alpha \) is a root of the polynomial \( x^{p^k} - x \), which has at most \( p^k \) roots. But, if \( k < n \), then \( p^k < p^n = q \), so that \( \sigma_p^k \neq \text{Id} \) for \( k < n \). Finally, as we have seen, \( (\sigma_p)^n = \sigma_{p^n} = \sigma_q = \text{Id} \), so that the order of \( \sigma_p \) in \( \text{Gal}(F_q/F_p) \) is \( n \).

Hence \( \text{Gal}(F_q/F_p) \) is cyclic and \( \sigma_p \) is a generator, i.e. \( \text{Gal}(F_q/F_p) \cong \langle \sigma_p \rangle \). More generally, if \( F_q' \) is a subfield of \( F_q \), so that \( q = (q')^d \) and \( [F_q : F_q'] = d \), similar arguments show that \( \text{Gal}(F_q/F_q') \) is cyclic and \( \sigma_{q'} \) is a generator, i.e. \( \text{Gal}(F_q/F_q') \cong \langle \sigma_{q'} \rangle \).

**Remark 4.12.** One important point about normal extensions is the following: unlike the case of finite or algebraic extensions, there exist sequences of extensions \( F \leq K \leq E \) where \( K \) is a normal extension of \( F \) and \( E \) is a normal extension of \( K \), but \( E \) is not a normal extension of \( F \). For example, consider the sequence \( \mathbb{Q} \leq \mathbb{Q}(\sqrt[2]{2}) \leq \mathbb{Q}(\sqrt[4]{2}) \). Then we have seen that \( \mathbb{Q}(\sqrt[2]{2}) \) is a normal extension of \( \mathbb{Q} \), and likewise \( \mathbb{Q}(\sqrt[4]{2}) \) is a normal extension
of \( \mathbb{Q}(\sqrt{2}) \) (it is the splitting field of \( x^2 - \sqrt{2} \) over \( \mathbb{Q}(\sqrt{2}) \)). But \( \mathbb{Q}(\sqrt{2}) \) is not a normal extension of \( \mathbb{Q} \), since it does not satisfy the condition (iii) of the theorem: \( x^4 - 2 \) is an irreducible polynomial with coefficients in \( \mathbb{Q} \), there is one root of \( x^4 - 2 \) in \( \mathbb{Q}(\sqrt{2}) \), but \( \mathbb{Q}(\sqrt{2}) \) does not contain the root \( i\sqrt{2} \) of \( x^4 - 2 \).

Likewise, there exist sequences of extensions \( F \leq K \leq E \) where \( E \) is a normal extension of \( F \), but \( K \) is not a normal extension of \( F \). (It is automatic that \( E \) is a normal extension of \( K \), since if \( E \) is a splitting field of \( f \in K[x] \), then it is still a splitting field of \( f \) when we view \( f \) as an element of \( K[x] \).) For example, consider the sequence \( \mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \omega) \), where as usual \( \omega = \frac{1}{2}(-1 + \sqrt{-3}) \). Then we have seen that \( \mathbb{Q}(\sqrt{2}, \omega) \) is a normal extension of \( \mathbb{Q} \) (it is the splitting field of \( x^3 - 2 \)), but \( \mathbb{Q}(\sqrt{2}) \) is not a normal extension of \( \mathbb{Q} \) (the irreducible polynomial \( x^3 - 2 \) has one root in \( \mathbb{Q}(\sqrt{2}) \), but it does not factor into linear factors in \( \mathbb{Q}(\sqrt{2})[x] \)).

A useful consequence of the characterization of splitting fields and the isomorphism extension theorem is the following:

**Proposition 4.13.** Suppose that \( E \) is a splitting field of the polynomial \( f \in F[x] \), where \( f \) is irreducible in \( F[x] \). Then \( \text{Gal}(E/F) \) acts transitively on the roots of \( f \).

**Proof.** Suppose that the roots of \( f \) in \( E \) are \( \alpha_1, \ldots, \alpha_n \). Fixing one root \( \alpha = \alpha_1 \) of \( f \), it suffices to prove that, for all \( j \), there exists a \( \varphi \in \text{Gal}(E/F) \) such that \( \varphi(\alpha_1) = \alpha_j \). By Lemma 3.1, there exists an isomorphism \( \sigma: F(\alpha_1) \to F(\alpha_j) \) such that \( \sigma(\alpha_1) = \alpha_j \). By the Isomorphism Extension Theorem, there exists an extension field \( L \) of \( E \) and a homomorphism \( \varphi: E \to L \) of \( \sigma \); in particular, \( \varphi(\alpha_1) = \alpha_j \). Finally, by the implication \( (i) \implies (ii) \) of Theorem 4.5, the image of \( \varphi \) is \( E \), i.e. in fact an element of \( \text{Gal}(E/F) \). \( \square \)

**Example 4.14.** Considering the example of \( \text{Gal}(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \) again, the proposition says that, since \( x^3 - 2 \) is irreducible in \( \mathbb{Q}[x] \), \( \text{Gal}(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \) is isomorphic to a subgroup of \( S_3 \) which acts transitively on the set \( \{1, 2, 3\} \). There are only two subgroups of \( S_3 \) with this property: \( S_3 \) itself and \( A_3 = \langle (123) \rangle \). Since every nontrivial element of \( A_3 \) has order 3 and complex conjugation is an element of \( \text{Gal}(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \) of order 2, \( \text{Gal}(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \cong S_3 \).

**Corollary 4.15.** Suppose that \( E \) is a splitting field of the polynomial \( f \in F[x] \), where \( f \) is an irreducible polynomial in \( F[x] \) of degree \( n \) with \( n \) distinct roots (automatic if \( F \) is perfect). Then \( n \) divides the order of \( \text{Gal}(E/F) \) and the order of \( \text{Gal}(E/F) \) divides \( n! \).
Proof. Let $\alpha_1, \ldots, \alpha_n$ be the $n$ distinct roots of $f$ in $E$. We have sent that there is an injective homomorphism from $\text{Gal}(E/F)$ to $S_n$, and hence that $\text{Gal}(E/F)$ is isomorphic to a subgroup of $S_n$. By Lagrange’s theorem, the order of $\text{Gal}(E/F)$ divides the order of $S_n$, which is $n!$. To get the other divisibility, note that $\{\alpha_1, \ldots, \alpha_n\}$ is a single orbit for the action of $\text{Gal}(E/F)$ on the set $\{\alpha_1, \ldots, \alpha_n\}$. By our work on group actions from last semester, the order of an orbit of a finite group acting on a set divides the order of the group (this is another application of Lagrange’s theorem). Hence $n$ divides the order of $\text{Gal}(E/F)$. \qed