Notes on Galois Theory

April 28, 2013

1 First remarks

Definition 1.1. Let E be a field. An *automorphism* of E is a (ring) isomorphism from E to itself. The set of all automorphisms of E forms a group under function composition, which we denote by $\operatorname{Aut} E$. Let E be a finite extension of a field F. Define the *Galois group* $\operatorname{Gal}(E/F)$ to be the subset of $\operatorname{Aut} E$ consisting of all automorphisms $\sigma\colon E \to E$ such that $\sigma(a) = a$ for all $a \in F$. We write this last condition as $\sigma|F = \mathrm{Id}$. It is easy to check that $\operatorname{Gal}(E/F)$ is a subgroup of $\operatorname{Aut} E$ (i.e. that it is closed under composition, $\mathrm{Id} \in \operatorname{Gal}(E/F)$, and, if $\sigma \in \operatorname{Gal}(E/F)$, then $\sigma^{-1} \in \operatorname{Gal}(E/F)$). Note that, if F_0 is the prime subfield of E ($F_0 = \mathbb{Q}$ or $F_0 = \mathbb{F}_p$ depending on whether the characteristic is 0 or a prime p), then $\operatorname{Aut} E = \operatorname{Gal}(E/F_0)$. In other words, every $\sigma \in \operatorname{Aut} E$ satisfies $\sigma(1) = 1$ and hence $\sigma(a) = a$ for all $a \in F_0$. If we have a sequence of fields $F \leq K_1 \leq K_2 \leq E$, then $\operatorname{Gal}(E/K_2) \operatorname{Gal}(E/K_1) \leq \operatorname{Gal}(E/F)$ (the order is reversed). As with the symmetric group, we shall usually write the product in $\operatorname{Gal}(E/F)$ as a product, i.e. the product of σ_1 and σ_2 is $\sigma_1\sigma_2$, instead of writing $\sigma_1 \circ \sigma_2$, and shall often write 1 for the identity automorphism Id.

A useful fact, which was a homework problem, is that if E is a **finite** extension of a field F and $\sigma\colon E \to E$ is a ring homomorphism such that $\sigma(a) = a$ for all $a \in F$, then σ is surjective, hence an automorphism, hence is an element of $\operatorname{Gal}(E/F)$.

Example 1.2. (1) If $\sigma\colon \mathbb{C} \to \mathbb{C}$ is complex conjugation, then $\sigma \in \operatorname{Gal}(\mathbb{C}/\mathbb{R})$, and in fact we shall soon see that $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \sigma\}$.
(2) The group $\operatorname{Aut} \mathbb{R} = \operatorname{Gal}(\mathbb{R}/\mathbb{Q})$, surprisingly, is trivial: $\operatorname{Gal}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{Id}\}$. The argument roughly goes by showing first that every automorphism of $\mathbb{R}$ is continuous and then that a continuous automorphism of $\mathbb{R}$ is the identity. In the case of $\mathbb{C}$, however, the only **continuous** automorphisms of $\mathbb{C}$ are the identity and complex conjugation. Nonetheless, $\operatorname{Aut} \mathbb{C}$ and $\operatorname{Aut} \mathbb{Q}^{\mathrm{alg}}$ turn

out to be very large groups! Most elements of $\operatorname{Aut}\mathbb{C}$ are therefore (very badly) discontinuous.

(3) We have seen in the homework that $\operatorname{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{Id}, \tau\}$, where $\tau(\sqrt{2}) = -\sqrt{2}$ and hence $\tau(a+b\sqrt{2}) = a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$.

(4) We have seen in the homework that $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}\}$.

Let $\sigma \in \operatorname{Aut} E$. We define the *fixed field*

$$E^\sigma = \{\alpha \in E : \sigma(\alpha) = \alpha\}.$$

It is straightforward to check that E^σ is a subfield of E (since, if $\alpha, \beta \in E^\sigma$, then by definition $\sigma(\alpha \pm \beta) = \sigma(\alpha) \pm \sigma(\beta) = \alpha \pm \beta$, and similarly for multiplication and division (if $\beta \neq 0$), so that E^σ is closed under the field operations. Clearly $E^\sigma \leq E$, and, if F_0 is the prime subfield of E, then $F_0 \leq E^\sigma$. We can extend this definition as follows: if X is any subset of $\operatorname{Aut} E$, we define the *fixed field*

$$E^X = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in X\}.$$

Since $E^X = \bigcap_{\sigma \in X} E^\sigma$, it is easy to see that E^X is again a subfield of E. We are usually interested in the case where $X = H$ is a subgroup of $\operatorname{Aut} E$. It is easy to see that, if H is the subgroup generated by a set X, then $E^H = E^X$. In particular, for a given element $\sigma \in \operatorname{Aut} E$, if $\langle\sigma\rangle$ is the cyclic subgroup generated by σ, then $E^{\langle\sigma\rangle} = E^\sigma$: this is just the statement that $\sigma(\alpha) = \alpha \iff$ for all $n \in \mathbb{Z}$, $\sigma^n(\alpha) = \alpha$. More generally, if $\sigma_1, \sigma_2 \in X$ and $\alpha \in E^X$, then by definition $\sigma_1(\alpha) = \sigma_2(\alpha) = \alpha$, and thus $\sigma_1\sigma_2(\alpha) = \sigma_1(\sigma_2(\alpha)) = \sigma_1(\alpha) = \alpha$. Since $\langle X\rangle$, the subgroup generated by X, is just the set of all products of powers of elements of X, we see that $\alpha \in E^X \implies \alpha \in E^{\langle X\rangle}$, and hence that $E^X \leq E^{\langle X\rangle}$. On the other hand, as $X \subseteq \langle X\rangle$, clearly $E^{\langle X\rangle} \leq E^X$, and hence $E^X = E^{\langle X\rangle}$.

We shall usual apply this in the following situation: given a subgroup H of $\operatorname{Gal}(E/F)$, we have defined the *fixed field*

$$E^H = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Then E^H is a subfield of E and by definition $F \leq E^H$ for every H. Thus $F \leq E^H \leq E$. Finally, this construction is order reversing in the sense that, if $H_1 \leq H_2 \leq \operatorname{Gal}(E/F)$, then

$$F \leq E^{H_2} \leq E^{H_1} \leq E.$$

Thus, given a field K with $F \leq K \leq E$, we have a subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/F)$, and given a subgroup $H \leq \mathrm{Gal}(E/F)$ we get a field E^H with $F \leq E^H \leq E$. In general, there is not much one can say about the relationship between these two constructions beyond the straightforward fact that

$$\begin{aligned} &H \leq \mathrm{Gal}(E/E^H); \\ &K \leq E^{\mathrm{Gal}(E/K)}. \end{aligned}$$

Here, to see the first inclusion, note that

$$E^H = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\ \}.$$

Thus, for $\sigma \in H$, $\sigma \in \mathrm{Gal}(E/E^H)$ by definition, hence $H \leq \mathrm{Gal}(E/E^H)$. The inclusion $K \leq E^{\mathrm{Gal}(E/K)}$ is similar.

Our first goal in these notes is to study finite extensions E of a field F, and to find conditions which enable us to conclude that $\mathrm{Gal}(E/F)$ is as large as possible (we will see that the maximum size is $[E : F]$). This study has two parts: First, we describe how to find homomorphisms $\sigma\colon E \to L$, where L is **some** extension of F, with the property that $\sigma(a) = a$ for all $a \in F$. Then we give a condition where, in case E is a subfield of L, the image of σ is automatically contained in E, and thus σ is an automorphism of E. We will discuss the motivation for Galois theory shortly, once we have established a few more basic properties of the Galois group.

Recall the following basic fact about complex roots of polynomials with real coefficients, which says that complex roots of a real polynomial occur in conjugate pairs:

Lemma 1.3. *Let $f(x) \in \mathbb{R}[x]$ is a polynomial with real coefficients and let α be a complex root of $f(x)$. Then $f(\bar{\alpha}) = 0$ as well.*

Proof. Suppose that $f(x) = \sum_{i=0}^n a_i x^i$ with $a_i \in \mathbb{R}$. Then, for all $\alpha \in \mathbb{C}$,

$$0 = \bar{0} = \overline{f(\alpha)} = \overline{\sum_{i=0}^n a_i \alpha^i} = \sum_{i=0}^n \bar{a}_i (\bar{\alpha})^i = \sum_{i=0}^n a_i (\bar{\alpha})^i = f(\bar{\alpha}).$$

Hence $f(\bar{\alpha})) = 0$. $\square$

As a result, assuming the Fundamental Theorem of Algebra, we can describe the irreducible elements of $\mathbb{R}[x]$:

Corollary 1.4. *The irreducible polynomials $f(x) \in \mathbb{R}[x]$ are either linear polynomials or quadratic polynomials with no real roots.*

Proof. Let $f(x) \in \mathbb{R}[x]$ be a non constant polynomial which is an irreducible element of $\mathbb{R}[x]$. By the Fundamental Theorem of Algebra, there exists a complex root α of $f(x)$. If $\alpha \in \mathbb{R}$, then $x - \alpha$ is a factor of $f(x)$ in $\mathbb{R}[x]$ and hence $f(x) = c(x - \alpha)$ for some $c \in \mathbb{R}^*$. Thus $f(x)$ is linear. Otherwise, $\alpha \notin \mathbb{R}$, and hence $\bar{\alpha} \neq \alpha$. Then $(x - \alpha)(x - \bar{\alpha})$ divides $f(x)$ in $\mathbb{C}[x]$. But

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} = x^2 - (2 \operatorname{Re} \alpha)x + |\alpha|^2 \in \mathbb{R}[x],$$

hence $(x - \alpha)(x - \bar{\alpha})$ divides $f(x)$ in $\mathbb{R}[x]$. Thus $f(x) = c(x - \alpha)(x - \bar{\alpha})$ for some $c \in \mathbb{R}^*$ and $f(x)$ is an irreducible quadratic polynomial. $\square$

We can generalize Lemma 1.3 as follows:

Lemma 1.5. *Let E be an extension field of a field F, and let $f(x) \in F[x]$. Suppose that $\alpha \in E$ and that $f(\alpha) = 0$. Then, for every $\sigma \in \mathrm{Gal}(E/F)$, $f(\sigma(\alpha)) = 0$ as well.*

Proof. If $f(x) = \sum_{i=0}^{n} a_i x^i$ with $a_i \in F$ for all i, then

$$0 = \sigma(0) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} a_i (\sigma(\alpha))^i,$$

hence $\sigma(\alpha)$ is a root of $f(x)$ as well. $\square$

In fact, it will be useful to prove a more general version. We suppose that we are given the following situation: E is an extension field of a field F, K is another field, and $\varphi\colon E \to K$ is an injective field homomorphism. Let $F' = \varphi(F)$ and let $\psi\colon F \to F'$ be the corresponding isomorphism. Another way to think of this is as follows:

Definition 1.6. Suppose that E is an extension field of the field F, that K is an extension field of the field F', and that $\psi\colon F \to F'$ is a homomorphism. An *extension* of ψ is a homomorphism $\varphi\colon E \to K$ such that, for all $a \in F$, $\varphi(a) = \psi(a)$. We also say that the *restriction* of φ to F is ψ, and write this as $\varphi | F = \psi$.

The situation is summarized in the following diagram:

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, dash] & K \arrow[d, dash] \\ F \arrow[r, "\psi"] & F' \end{tikzcd}$$

Given $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$, define a new polynomial $\psi(f)(x) \in F'[x]$ by the formula

$$\psi(f)(x) = \sum_{i=0}^{n} \psi(a_i) x^i.$$

In other words, $\psi(f)(x)$ is the polynomial obtained by applying the isomorphism ψ to the coefficients of $f(x)$.

Lemma 1.7. *In the above situation, $\alpha \in E$ is a root of $f(x) \in F[x]$ if and only if $\varphi(\alpha) \in K$ is a root of $\psi(f)(x) \in F'[x]$.*

Proof. In fact, for α an arbitrary element of E, and using the definitions and the fact that φ is a field automorphism, we see that

$$\varphi(f(\alpha)) = \varphi(\sum_{i=0}^{n} a_i \alpha^i) = \sum_{i=0}^{n} \varphi(a_i)\varphi(\alpha)^i = \sum_{i=0}^{n} \psi(a_i)\varphi(\alpha)^i = \psi(f)(\varphi(\alpha)).$$

Thus, as φ is injective, $f(\alpha) = 0 \iff \varphi(f(\alpha)) = 0 \iff \psi(f)(\varphi(\alpha)) = 0$. $\square$

A second basic observation is then the following:

Corollary 1.8. *Let E be an extension field of the field F and let $f(x) \in F[x]$. Suppose that $\alpha_1, \dots, \alpha_n$ are the (distinct) roots of $f(x)$ that lie in E, i.e. $\{\alpha \in E : f(\alpha) = 0\} = \{\alpha_1, \dots, \alpha_n\}$ and, for $i \neq j$, $\alpha_i \neq \alpha_j$. Then $\mathrm{Gal}(E/F)$ acts on the set $\{\alpha_1, \dots, \alpha_n\}$, and hence there is a homomorphism $\rho\colon \mathrm{Gal}(E/F) \to S_n$, where S_n is the symmetric group on n letters. If moreover $E = F(\alpha_1, \dots, \alpha_n)$, then ρ is injective, and hence identifies $\mathrm{Gal}(E/F)$ with a subgroup of S_n. In particular, in this case $\#(\mathrm{Gal}(E/F)) \leq n!$.*

Proof. It follows from Lemma 1.5 that $\mathrm{Gal}(E/F)$ acts on the set $\{\alpha_1, \dots, \alpha_n\}$, and hence that there is a homomorphism $\rho\colon \mathrm{Gal}(E/F) \to S_n$. To see that ρ is injective if $E = F(\alpha_1, \dots, \alpha_n)$, it suffices to show that, if $\sigma \in \mathrm{Gal}(E/F)$ and $\sigma(\alpha_i) = \alpha_i$ for all i, then $\sigma = \mathrm{Id}$. To see this, recall that E^σ is the fixed field of σ. Since $\sigma \in \mathrm{Gal}(E/F)$, $F \leq E^\sigma$. If in addition $\sigma(\alpha_i) = \alpha_i$ for all i, then E^σ is a subfield of E containing F and α_i for all i, and hence $E = F(\alpha_1, \dots, \alpha_n) \leq E^\sigma \leq E$. It follows that $E^\sigma = E$, i.e. that $\sigma(\alpha) = \alpha$ for all $\alpha \in E$. This says that $\sigma = \mathrm{Id}$. $\square$

It is not hard to check that every finite extension E of a field F is of the form $E = F(\alpha_1, \dots, \alpha_n)$, where the α_i are the roots in E of some polynomial $f(x) \in F[x]$. Thus

Corollary 1.9. *Let E be a finite extension of the field F. Then* $\mathrm{Gal}(E/F)$ *is finite.*

We shall give an explicit bound for the order of $\mathrm{Gal}(E/F)$ later.

Remark 1.10. The homomorphism $\rho\colon \mathrm{Gal}(E/F) \to S_n$ given in Corollary 1.8 depends on a choice of labeling of the roots of $f(x)$ as $\alpha_1, \dots, \alpha_n$. A different choice of labeling the roots corresponds to an element $\tau \in S_n$, and it is easy to check that listing the roots as $\alpha_{\tau(1)}, \dots, \alpha_{\tau(n)}$ replaces ρ by $\tau \cdot \rho \cdot \tau^{-1}$, i.e. by $i_\tau \circ \rho$, where $i_g\colon S_n \to S_n$ is the inner automorphism given by conjugation by τ. In particular, the image of ρ is well-defined up to conjugation.

Important comment: Returning to the motivation for Galois theory, consider the case where the characteristic of F is 0, or more generally F is perfect, E is a finite extension of F, and assume that there exists a polynomial $f(x) \in F[x]$ such that

1. If $\alpha_1, \dots, \alpha_n$ are the roots of $f(x)$ lying in E, then $E = F(\alpha_1, \dots, \alpha_n)$.
2. The polynomial $f(x)$ is a product of linear of linear factors in $E[x]$, i.e. "all" of the roots of $f(x)$ lie in E.

The first condition says that the Galois group $\mathrm{Gal}(E/F)$ can be identified with a subgroup of S_n. The main point of Galois theory is that, if Condition (2) also holds, then the complexity of the polynomial $f(x)$, and in particular the difficulty in describing its roots, is mirrored in the complexity of the Galois group, both as an abstract group and as a subgroup of S_n.

Example 1.11. (1) In case $F = \mathbb{R}$ and $E = \mathbb{C}$, let $f(x) = x^2 + 1$ with roots $\pm i$. Since $\mathbb{C} = \mathbb{R}(i)$, there is an injective homomorphism $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to S_2$, where S_2 is viewed as the set of permutations of the two element set $\{i, -i\}$. Hence $\#(\mathrm{Gal}(\mathbb{C}/\mathbb{R})) \leq 2$. Since complex conjugation σ is an element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ which exchanges i and $-i$, $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ has order two and is equal to $\{1, \sigma\}$.

(2) Similarly, with $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2})$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is isomorphic to a subgroup of S_2, where S_2 is now viewed as the set of permutations of the two element set $\{\sqrt{2}, -\sqrt{2}\}$. Hence $\#(\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})) \leq 2$, and since (as we have seen) $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of $\mathbb{Q}(\sqrt{2})$ which is the identity on $\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ has order two and is equal to $\{1, \sigma\}$.

(3) More generally, let F be any field of characteristic not equal to 2 and suppose that $t \in F$ is not a perfect square in F, i.e. that the polynomial

$x^2 - t$ has no root in F and hence is irreducible in $F[x]$. Let $E = F(\sqrt{t})$ be the degree two extension of F obtained by adding a root of $x^2 - t$, which we naturally write as $\sqrt{t}$. Then as in (1) and (2) above, $\mathrm{Gal}(F(\sqrt{t})/F)$ is isomorphic to a subgroup of S_2, and in fact $\mathrm{Gal}(F(\sqrt{t})/F)$ has two elements. As in (2), it suffices to show that there is an element σ of $\mathrm{Gal}(F(\sqrt{t})/F)$such that $\sigma(\sqrt{t}) = -\sqrt{t}$; since the characteristic of F is not 2, $\sqrt{a} \neq -\sqrt{a}$, so $\sigma \neq \mathrm{Id}$. To see this, it suffices to show that, since every element of $F(\sqrt{t})$ can be uniquely written as $a + b\sqrt{t}$ with $a, b \in F$, and we define $\sigma(a+b\sqrt{t}) = a - b\sqrt{t}$, then σ is an automorphism of $F(\sqrt{t})$ fixing F. Clearly σ is a bijection, in fact $\sigma^{-1} = \sigma$, and $\sigma(a) = a$ for all $a \in F$. To see that $\sigma \in \mathrm{Gal}(F(\sqrt{t})/F)$, it suffices to check that σ is a ring homomorphism, i.e. that σ preserves addition and multiplication. The first of these is easy, and, as for the second,

$$\begin{aligned}
\sigma((a_1 + b_1\sqrt{t})(a_2 + b_2\sqrt{t})) &= \sigma((a_1a_2 + tb_1b_2) + (a_1b_2 + a_2b_1)\sqrt{t}) \\
&= (a_1a_2 + tb_1b_2) - (a_1b_2 + a_2b_1)\sqrt{t} \\
&= (a_1 - b_1\sqrt{t})(a_2 - b_2\sqrt{t}) \\
&= \sigma(a_1 + b_1\sqrt{t})\sigma(a_2 + b_2\sqrt{t}).
\end{aligned}$$

Hence $\sigma \in \mathrm{Gal}(F(\sqrt{t})/F)$ with $\sigma(\sqrt{t}) = -\sqrt{t}$.

(4) Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Every element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ permutes the roots of $(x^2 - 2)(x^2 - 3)$, i.e. the set $\{\pm\sqrt{2}, \pm\sqrt{3}\}$. Since $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3})$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is isomorphic to a subgroup of S_4. Explicitly, let us label $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, and $\alpha_4 = -\sqrt{3}$. Since $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ actually permutes the set $\{\pm\sqrt{2}\}$ and $\{\pm\sqrt{3}\}$ individually, we see that the image of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is contained in the subgroup $\{1, (12), (34), (12)(34)\} \cong S_2 \times S_2$ of S_4. In fact, we claim that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is isomorphic to the full subgroup $\{1, (12), (34), (12)(34)\}$. To see this, apply (3) above to the case $F = \mathbb{Q}(\sqrt{3})$ and $t = 2$. We have seen in the homework that $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$, i.e. that the polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}(\sqrt{3})[x]$. Then by (3) there is an element $\sigma_1 \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{3})) \leq \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ such that $\sigma_1(\sqrt{2}) = -\sqrt{2}$, and $\sigma_1(\sqrt{3}) = \sqrt{3}$ by construction. Thus σ_1 corresponds to the permutation $(12) \in S_4$. Exchanging the roles of 2 and 3, we see that there is a $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})) \leq \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ such that $\sigma_2(\sqrt{2}) = \sqrt{2}$, and $\sigma_2(\sqrt{3}) = -\sqrt{3}$. Thus σ_2 corresponds to the permutation (34). Finally, the product $\sigma_3 = \sigma_1\sigma_2$ satisfies: $\sigma_3(\sqrt{2}) = -\sqrt{2}$, $\sigma_3(\sqrt{3}) = -\sqrt{3}$, and thus corresponds to the permutation $(12)(34)$.

(5) For a very closely related example, let $\alpha = \sqrt{2} + \sqrt{3}$ with $\mathrm{irr}(\alpha, \mathbb{Q}, x) =$

$x^4 - 10x^2 + 1$. Then we have seen that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. By (4) above, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$, where

$$\begin{aligned} \sigma_1(\sqrt{2}) &= -\sqrt{2}; & \sigma_1(\sqrt{3}) &= \sqrt{3}; \\ \sigma_2(\sqrt{2}) &= \sqrt{2}; & \sigma_2(\sqrt{3}) &= -\sqrt{3}; \\ \sigma_3(\sqrt{2}) &= -\sqrt{2}; & \sigma_3(\sqrt{3}) &= -\sqrt{3}. \end{aligned}$$

Applying σ_i to α and using Lemma 1.5, we see that all of the elements $\pm\sqrt{2} \pm \sqrt{3}$ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are roots of $\mathrm{irr}(\alpha, \mathbb{Q}, x) = x^4 - 10x^2 + 1$. Since there are four such elements and $x^4 - 10x^2 + 1$ has degree four, the roots of $\mathrm{irr}(\alpha, \mathbb{Q}, x) = x^4 - 10x^2 + 1$ are exactly $\alpha = \beta_1 = \sqrt{2} + \sqrt{3}$, $\beta_2 = -\sqrt{2} + \sqrt{3}$, $\beta_3 = \sqrt{2} - \sqrt{3}$, and $\beta_4 = -\sqrt{2} - \sqrt{3}$. The action of the Galois group on the set $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ then identifies the group

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$$

with the subgroup

$$\{1, (12)(34), (13)(24), (14)(23)\}$$

of S_4. We can thus identify the **same** Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ with two **different** (but of course isomorphic) subgroups of S_4.

(6) Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2})$. There is just one root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$, namely $\sqrt[3]{2}$, and hence (as we have already seen) $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$. On the other hand, if $\omega = \frac{1}{2}(-1 + \sqrt{-3})$, then $\omega^3 = 1$, hence $\omega^2 = \omega^{-1} = \bar{\omega}$, and we have seen that the roots of $x^3 - 2$ in $\mathbb{C}$ are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, and $\alpha_3 = \omega^2\sqrt[3]{2}$. Moreover $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. By Corollary 1.8, there is an injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ to S_3. As we shall see, this homomorphism is in fact an isomorphism. Here we just note that complex conjugation defines a nontrivial element σ of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ of order 2. In fact as $\sqrt[3]{2}$ is real, $\sigma(\alpha_1) = \alpha_1$, and $\sigma(\alpha_2) = \bar{\omega}\sqrt[3]{2} = \omega^2\sqrt[3]{2} = \alpha_3$. Thus σ corresponds to $(23) \in S_3$.

(7) Again let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[4]{2})$. There are two roots of $x^4 - 2$ in $\mathbb{Q}(\sqrt[4]{2})$, namely $\pm\sqrt[4]{2}$. Thus $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ has order at most 2 and in fact has order 2 by applying (4) to the case $F = \mathbb{Q}(\sqrt{2})$ and $t = \sqrt{2}$ with $\sqrt{t} = \sqrt[4]{2}$. To improve this situation, consider the field $\mathbb{Q}(\sqrt[4]{2}, i)$, which contains all four roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of the polynomial $x^4 - 2$, namely $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. Since clearly $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\sqrt[4]{2}, i)$, $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is isomorphic to a subgroup of S_4. However, it cannot be all of S_4. In fact, if

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$, then there are at most 4 possibilities for $\sigma(\sqrt[4]{2})$, since $\sigma(\sqrt[4]{2})$ has to be a root of $x^4 - 2$ and hence can only be α_i for $1 \leq i \leq 4$. But there are also at most 2 possibilities for $\sigma(i)$, which must be a root of $x^2 + 1$ and hence can only be $\pm i$. Since σ is specified by its values on $\sqrt[4]{2}$ and on i, there are at most 8 possibilities for σ and hence $\#(\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})) \leq 8$. We will see that in fact $\#(\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})) = 8$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4$, the dihedral group of order 8.

2 The isomorphism extension theorem

We begin by interpreting Lemma 1.5 as follows: suppose that $E = F(\alpha)$ is a **simple** extension of F and let $f(x) = \mathrm{irr}(\alpha, F, x)$. Then, given an element $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(\alpha)$ is a root of $f(x)$ in E. The following is a converse to this statement.

Lemma 2.1. *Let F be a field, let $E = F(\alpha)$ be a simple extension of F, where α is algebraic over F, and let K be an extension field of $E = F(\alpha)$. Let $f(x) = \mathrm{irr}(\alpha, F, x)$. Then there is a bijection from the set of homomorphisms $\sigma\colon E \to K$ such that $\sigma(a) = a$ for all $a \in F$ to the set of roots of the polynomial $f(x)$ in K.*

Proof. Let $\sigma\colon E \to K$ be a homomorphism such that $\sigma(a) = a$ for all $a \in F$. We have seen that $\sigma(\alpha)$ is a root of $f(x)$ in E. Since every element of $E = F(\alpha)$ is of the form $\beta = \sum_i a_i\alpha^i$ with $a_i \in F$, $\sigma(\beta) = \sum_i \sigma(a_i\alpha^i) = \sum_i \sigma(a_i)\sigma(\alpha^i) = \sum_i a_i(\sigma(\alpha))^i$. Hence σ is determined by its value $\sigma(\alpha)$ on α. The above says that here is a well-defined, injective function from the set of homomorphisms $\sigma\colon E \to K$ such that $\sigma(a) = a$ for all $a \in F$ to the set of roots of the polynomial $f(x)$ in K, defined by mapping σ to its value $\sigma(\alpha)$ on α. We must show that this function is surjective, in other words that, given a root $\beta \in K$ of $f(x)$, there exists a homomorphism $\sigma\colon E \to K$ such that $\sigma(a) = a$ for all $a \in F$ and such that $\sigma(\alpha) = \beta$.

Thus, let β be a root of $f(x)$ in K. We know that $F(\alpha) \cong F[x]/(f(x))$, and in fact $\mathrm{ev}_\alpha\colon F[x] \to F(\alpha)$ defines an isomorphism from $F[x]/(f(x))$ to $F(\alpha)$, which we denote by $\widehat{\mathrm{ev}}_\alpha$, with the property that $\widehat{\mathrm{ev}}_\alpha(x + (f(x))) = \alpha$ and $\widehat{\mathrm{ev}}_\alpha(a) = a$ for all $a \in F$ (where we identify $a \in F$ with the coset $a + (f(x)) \in F[x]/(f(x))$). On the other hand, $f(\beta) = 0$ by hypothesis, so that $\mathrm{irr}(\beta, F, x)$ divides $f(x)$. Since both $\mathrm{irr}(\beta, F, x)$ and $f(x)$ are monic irreducible polynomials, $\mathrm{irr}(\beta, F, x) = f(x)$. Thus the subfield $F(\beta)$ of K is also isomorphic to $F[x]/(f(x))$, and in fact the evaluation homomorphism $\mathrm{ev}_\beta\colon F[x] \to F(\beta)$ defines an isomorphism from $F[x]/(f(x))$ to $F(\beta)$, which we denote by $\widehat{\mathrm{ev}}_\beta$, with the property that $\widehat{\mathrm{ev}}_\beta(x+(f(x))) = \beta$ and $\widehat{\mathrm{ev}}_\beta(a) = a$ for all $a \in F$. Taking the composition $\sigma = \widehat{\mathrm{ev}}_\beta \circ \widehat{\mathrm{ev}}_\alpha^{-1}$, σ is an isomorphism from $F(\alpha)$ to $F(\beta) \leq K$, with the property that $\sigma(\alpha) = \beta$ and $\sigma(a) = a$ for all $a \in F$. Viewing the range of σ as K (instead of the subfield $F(\beta)$) gives a homomorphism as desired. □

It will be useful (for example in certain induction arguments) to prove the following generalization of the previous lemma.

Lemma 2.2. *Let F be a field, let $E = F(\alpha)$ be a simple extension of F, where α is algebraic over F, and let $\psi\colon F \to K$ be a homomorphism from F to a field K. Let $f(x) = \mathrm{irr}(\alpha, F, x)$. Then there is a bijection from the set of homomorphisms $\sigma\colon E \to K$ such that $\sigma(a) = \psi(a)$ for all $a \in F$ to the set of roots of the polynomial $\psi(f)(x)$ in K, where $\psi(f)(x) \in K[x]$ is the polynomial obtained by applying the homomorphism ψ to coefficients of $f(x)$.*

Proof. Let $\sigma\colon E \to K$ be a homomorphism such that $\sigma(a) = \psi(a)$ for all $a \in F$. By Lemma 1.7, $\sigma(\alpha) \in K$ is a root of $\psi(f)(x)$. Thus σ determines a root $\sigma(\alpha)$ of $\psi(f)(x)$. Since $E = F(\alpha)$, every element ξ of E is of the form $\xi = \sum_{i=0}^{n-1} c_i\alpha^i$, where $c_i \in F$. Thus

$$\sigma(\xi) = \sigma(\sum_{i=0}^{n-1} c_i\alpha^i) = \sum_{i=0}^{n-1} \sigma(c_i)\sigma(\alpha)^i = \sum_{i=0}^{n-1} \psi(c_i)\sigma(\alpha)^i.$$

It follows that that σ is uniquely determined by $\sigma(\alpha)$ and the condition that $\sigma(a) = \psi(a)$ for all $a \in F$,

Conversely, suppose that we are given a root $\beta \in K$ of $\psi(f)(x)$. Then $F(\alpha) \cong F[x]/(f(x))$. Let $\mathrm{ev}_{\psi,\beta}$ be the homomorphism $F[x] \to K$ defined as follows: given a polynomial $p(x) \in F[x]$, let (as above) $\psi(p)(x)$ be the polynomial obtained by applying ψ to the coefficients of $p(x)$, and let $\mathrm{ev}_{\psi,\beta}(p(x)) = \psi(p)(x)(\beta)$ be the evaluation of $\psi(p)(x)$ at β. Then $\mathrm{ev}_{\psi,\beta}$ is a homomorphism from $F[x]$ to K, and $f(x) \in \mathrm{Ker}\,\mathrm{ev}_{\psi,\beta}$, since $\psi(f)(\beta) = 0$. Thus $(f(x)) \subseteq \mathrm{Ker}\,\mathrm{ev}_{\psi,\beta}$ and hence $(f(x)) = \mathrm{Ker}\,\mathrm{ev}_{\psi,\beta}$ since $(f(x))$ is a maximal ideal. The rest of the proof is identical to the proof of Lemma 2.1. □

Corollary 2.3. *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 $\psi\colon F \to K$ be a homomorphism. Then:*

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

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

(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 $\sigma\colon E \to L$ extending ψ.*

Proof. If $E = F(\alpha)$ is a simple extension of F, then Lemma 2.2 implies that the extensions of ψ to a homomorphism $\sigma\colon F(\alpha) \to K$ are in one-to-one correspondence with the $\beta \in K$ such that β is a root of $\psi(f)(x)$, where $f(x) = \mathrm{irr}(\alpha, F, x)$. In this case, since $\psi(f)(x)$ has at most $n = [F(\alpha) : F]$ roots, there are at most n extensions of ψ, proving (i). To see (ii), choose an extension field L of K such that $\psi(f)(x)$ has a root β in L. Thus there will be at least one homomorphism $\sigma\colon F(\alpha) \to L$ extending ψ. To see (iii), choose an extension field L of K such that $\psi(f)(x)$ 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 $f(x) \in F[x]$ has no multiple roots in any extension field, and the same will be true of the polynomial $\psi(f)(x) \in \psi(F)[x]$, where $\psi(F)$ is the image of F in K, since $\psi(f)(x)$ is also irreducible. Thus there are n distinct roots of $\psi(f)(x)$ in L, and hence n different extensions of ψ to a homomorphism $\sigma\colon F(\alpha) \to L$. $\square$

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

$$\begin{tikzcd}
 & L \arrow[d, dash] \\
E \arrow[ur, dashed, "\sigma"] \arrow[d, dash] & K \arrow[d, dash] \\
F \arrow[r, "\psi"] & F'
\end{tikzcd}$$

Let us give some examples to show how one can use Lemma 2.2, especially in case the homomorphism ψ is not the identity:

Example 2.4. (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 $\mathbb{Q}(\sqrt{2})$, Id and σ, where $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. We have seen that $f(x) = x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$. Since in fact $f(x) \in \mathbb{Q}[x]$, $\sigma(f)(x) = f(x)$, and clearly $\mathrm{Id}(f)(x) = f(x)$. In particular, the roots of

$\sigma(f)(x) = f(x)$ are $\pm\sqrt{3}$. Applying Lemma 2.2 to the case $F = \mathbb{Q}(\sqrt{2})$, $E = F(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = K$, and $\psi = \mathrm{Id}$ or $\psi = \sigma$, we see that there are two extensions of Id to a homomorphism (necessarily an automorphism) $\varphi\colon E \to E$. One of these satisfies: $\varphi(\sqrt{3}) = \sqrt{3})$, hence $\varphi = \mathrm{Id}$, and the other satisfies $\varphi(\sqrt{3}) = -\sqrt{3})$, hence $\varphi = \sigma_2$ in the notation of 4) of Example 1.11. Likewise, there are two extensions of σ to an automorphism) $\varphi\colon E \to E$. 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 4) of Example 1.11. In particular, we see that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ has order 4, giving another argument for (4) of Example 1.11.

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

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

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 $\mathrm{Gal}(K/\mathbb{Q}(\omega)$, correspond to the roots of $x^3 - 2$ in K. Thus for example, there is an automorphism $\rho\colon \mathbb{Q}(\sqrt[3]{2}, \omega) \to \mathbb{Q}(\sqrt[3]{2}, \omega)$ such that $\rho(\omega) = \omega$ and $\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. This completely specifies ρ. 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 ρ corresponds to the permutation (123). Then $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 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 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$, with $\beta_1 = \sqrt[4]{2}$, $\beta_2 = i\sqrt[4]{2}$, $\beta_3 = -\sqrt[4]{2}$, and $\beta_4 = -i\sqrt[4]{2}$. Then if $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$, it follows that $\varphi(\beta_1) = \beta_k$ for some k, $1 \leq k \leq 4$ and $\varphi(i) = \pm i$. In particular $\#(\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})) \leq 8$. As in (3), complex conjugation σ is an element of $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ 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 $\mathbb{Q}(i)$ by inspection (the β_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 ± 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 $i \notin \mathbb{Q}(\sqrt[4]{2})$ since i is not real but $\mathbb{Q}(\sqrt[4]{2}) \leq \mathbb{R}$, hence

$$\begin{aligned}[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8 \\ &= [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}],\end{aligned}$$

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

As $\mathbb{Q}(\sqrt[4]{2}, i)$ 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 $\mathbb{Q}(\sqrt[4]{2}, i)$ to $\mathbb{Q}(\sqrt[4]{2}, i)$ which is the identity on $\mathbb{Q}(i)$ corresponds to the choice of a root of $x^4 - 2$ in $\mathbb{Q}(\sqrt[4]{2}, i)$. In particular, there exists $\rho \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(i)) \leq \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ such that $\rho(i) = i$ and $\rho(\beta_1) = \beta_2$. Then $\rho(\beta_2) = \rho(i\beta_1) = i\beta_2 = \beta_3$ and likewise $\rho(\beta_3) = \rho(-\beta_1) = -\rho(\beta_1) = -\beta_2 = \beta_4$ and $\rho(\beta_4) = \beta_1$. It follows that ρ 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 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$, 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 2.5 (Isomorphism Extension Theorem)**.** *Let E be a finite extension of a field F. Let K be a field and let $\psi \colon F \to K$ be a homomorphism. Then:*

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

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

(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 $\sigma\colon E \to L$ extending ψ.*

Proof. Since E is a finite extension of F, $E = F(\alpha_1, \dots, \alpha_n)$ 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 2.3.

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

By assumption, $E = F_1(\alpha)$ and the inductive hypothesis applies to the extension F_1 of F. Given a homomorphism $\psi\colon F \to K$, where K is a field, by induction, there exist at most $[F_1 : F]$ extensions of ψ to a homomorphism $F_1 \to K$. Suppose that the set of all such homomorphisms is $\{\sigma_1, \dots, \sigma_d\}$, with $d \le [F_1 : F]$. Fix one such homomorphism σ_i. Applying Corollary 2.3 to the simple extension $F_1(\alpha) = E$ and the homomorphism $\sigma_i\colon F_1 \to K$, there are at most e extensions of σ_i to a homomorphism $\tau\colon F_1(\alpha) \to K$, where $e = [F_1(\alpha) : F_1] = [E : F_1]$. In all, since each of the d extensions σ_i has at most e extensions to a homomorphism from E to K, there are at most de extensions of ψ to a homomorphism $E \to K$. As $d \le [F_1 : F]$ and $e = [E : F_1]$, we see that there are at most $[F_1 : F][E : F_1] = [E : F]$ extensions of ψ 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 L_1 containing K and an extension of ψ to a homomorphism $\psi_1\colon F_1 \to L_1$. Let $f_1(x) = \mathrm{irr}(\alpha, F_1, x)$. Adjoining a root of $\psi_1(f_1)(x)$ to L_1 if necessary, to obtain an extension field L of L_1 containing a root of $\psi_1(f_1)(x)$, it follows from Corollary 2.3 that there exists a homomorphism $\sigma\colon F_1(\alpha) = E \to L$ extending ψ_1, and hence extending ψ. 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 $\psi\colon F \to K$, where K is a field, by the inductive hypothesis, after enlarging the field K to some extension field L_1 if need be, there exist exactly $[F_1 : F]$ extensions of ψ to a homomorphism $F_1 \to L_1$. Suppose that the set of all such homomorphisms is $\{\sigma_1, \dots, \sigma_d\}$, with $d = [F_1 : F]$. As before, we let $f_1(x) = \mathrm{irr}(\alpha, F_1, x)$. There exists a finite extension L of the field L_1 such that every one of the (not necessarily distinct) irreducible polynomials $\sigma_i(f_1)(x) \in \sigma_i(F_1)[x]$ splits into linear factors in L, and hence has e distinct roots in L, where $e = \deg f_1(x) = [F_1(\alpha) : F_1] = [E : F_1]$. Fix one such homomorphism σ_i. Again applying Corollary 2.3 to the simple extension $F_1(\alpha) = E$ and the homomorphism $\sigma_i\colon F_1 \to L$, there are exactly e extensions of σ_i to a homomorphism $\tau_{ij}\colon F_1(\alpha) \to L$. In all, since each of the d extensions σ_i has e extensions to a homomorphism from E to L, there are exactly de extensions of ψ 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 ψ to a homomorphism $E \to L$. This completes the inductive step for the proof of (iii), and hence the proof of the theorem. $\square$

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

Corollary 2.6. *Let E be a finite extension of F. Then*

$$\#(\mathrm{Gal}(E/F)) \leq [E : F]. \quad \square$$

Definition 2.7. 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 $\sigma\colon E \to L$ with $\sigma(a) = a$ 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 $\iff$ for all $\alpha \in E$, the polynomial $\mathrm{irr}(\alpha, F, x)$ does not have multiple roots.

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

Theorem 2.8 (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 2.6, we might have strict inequality, i.e. $\#(\mathrm{Gal}(E/F)) < [E : F]$. 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 $\sigma \colon E \to L$, where L is **some** extension field of E, without being able to guarantee that $\sigma(E) = E$. 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 $\sigma \colon E \to L$, but only one of these has image equal to E. We will fix this problem in the next section.

3 Splitting fields

Definition 3.1. Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree at least 1. Then an extension field E of F is a *splitting field* for $f(x)$ over F if the following two conditions hold:

(i) In $E[x]$, there is a factorization $f(x) = c\prod_{i=1}^{n}(x-\alpha_i)$. In other words, $f(x)$ factors in $E[x]$ into a product of linear factors.

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

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

Remark 3.2. (i) Clearly, E is a splitting field of $f(x)$ over F if (i) holds ($f(x)$ factors in $E[x]$ into a product of linear factors) and there exist some subset $\{\alpha_1, \dots, \alpha_k\}$ of the roots of $f(x)$ such that $E = F(\alpha_1, \dots, \alpha_k)$ (because, if $\alpha_{k+1}, \dots, \alpha_n$ are the remaining roots, then they are in E by (i) and thus $E = E(\alpha_{k+1}, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_k)(\alpha_{k+1}, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n)$).

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

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

Example 3.3.

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, $f(x) \in F[x]$ is an irreducible polynomial of degree 2, and $E = F(\alpha)$, where α is a root of $f(x)$, then E is a splitting field of $f(x)$, since in $E[x]$, $f(x) = (x - \alpha)g(x)$, where $g(x)$ has degree one, hence is linear, and E is clearly generated over F by the roots of $f(x)$.

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 $f(x)$ 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 $x^4 - 10x^2 + 1$.

6. The splitting field of $x^5 - 1$ over $\mathbb{Q}$ is the same as the splitting field of $x^4 + x^3 + x^2 + x + 1 = \Phi_5(x)$ 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 ζ^i for some i. Note that, as $\Phi_5(x)$ is irreducible in $\mathbb{Q}[x]$, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. More generally, if ζ is any generator of μ_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 3.4. In a sense, examples 3, 5 and 6 are misleading, in the sense that for a "random" irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree n, the expectation is that the degree of a splitting field of $f(x)$ will be $n!$. In other words, if $f(x) \in \mathbb{Q}[x]$ is a "random" irreducible polynomial and α_1 is some root of $f(x)$ in an extension field of $\mathbb{Q}$, then we know that, in $\mathbb{Q}(\alpha_1)[x]$, $f(x) = (x-\alpha_1)f_1(x)$ with $\deg f_1(x) = n-1$. But there is no reason in general to expect that $\mathbb{Q}(\alpha_1)$ contains any other root of $f(x)$, or equivalently a root of $f_1(x)$, or even to expect that $f_1(x)$ is reducible in $\mathbb{Q}(\alpha_1)$. Thus we would expect in general that, if α_2 is a root of $f_1(x)$ in some extension field of $\mathbb{Q}(\alpha_1)$, then $[\mathbb{Q}(\alpha_1)(\alpha_2) : \mathbb{Q}(\alpha_1)] = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] = n-1$ and hence $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] = n(n-1)$. Then $f(x) = (x-\alpha_1)(x-\alpha_2)f_2(x) \in \mathbb{Q}(\alpha_1, \alpha_2)$. Continuing in this way, our expectation is that a splitting field for $f(x)$ over $\mathbb{Q}$ is of the form $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ with $[\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}] = n(n-1)\cdots 2 \cdot 1 = n!$.

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

Theorem 3.5. *Let E be a finite extension of a field F. Then the following are equivalent:*

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

(ii) *For every extension field L of E, if $\sigma \colon E \to L$ is a homomorphism such that $\sigma(a) = a$ for all $a \in F$, then $\sigma(E) = E$, and hence σ is an automorphism of E.*

(iii) *For every **irreducible** polynomial $p(x) \in F[x]$, if there is a root of $p(x)$ in E, then $p(x)$ factors into a product of linear factors in $E[x]$.*

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

Lemma 3.6. *Let L be an extension field of a field F and let $\alpha_1, \dots, \alpha_n \in L$. If $\sigma \colon E = F(\alpha_1, \dots, \alpha_n) \to L$ is a homomorphism, then $\sigma(E) = \sigma(F)(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$.*

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 $\sigma(\sum_i a_i\alpha^i) = \sum_i \sigma(a_i)(\sigma(\alpha))^i$ and hence

$$\sigma(F(\alpha)) = \{\sum_i \sigma(a_i)(\sigma(\alpha))^i : a_i \in F\} = \sigma(F)(\sigma(\alpha)).$$

For the inductive step, applying the case $n = 1$ to the field $F(\alpha_1, \dots, \alpha_{n-1})$, we see that

$$\begin{aligned}\sigma(F(\alpha_1, \dots, \alpha_n)) &= \sigma(F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)) = \sigma(F(\alpha_1, \dots, \alpha_{n-1}))(\sigma(\alpha_n)) \\ &= \sigma(F)(\sigma(\alpha_1), \dots, \sigma(\alpha_{n-1}))(\sigma(\alpha_n)) = \sigma(F)(\sigma(\alpha_1), \dots, \sigma(\alpha_n)),\end{aligned}$$

completing the proof of the inductive step. $\square$

Returning to the proof of the theorem, by assumption, $E = F(\alpha_1, \dots, \alpha_n)$, where $f(x) = c\prod_{i=1}^n (x - \alpha_i)$. In particular, every root of $f(x)$ in L already lies in E. If $\sigma\colon E \to L$ is a homomorphism such that $\sigma(a) = a$ for all $a \in F$, then $\sigma(\alpha_i) = \alpha_j$ for some j, hence $\sigma(\{\alpha_1, \dots, \alpha_n\}) \subseteq \{\alpha_1, \dots, \alpha_n\}$. Since $\{\alpha_1, \dots, \alpha_n\}$ is finite set and σ is injective, it induces a surjective map from $\{\alpha_1, \dots, \alpha_n\}$ to itself, i.e. σ permutes the roots of $f(x)$ in $E \leq L$. By Lemma 3.6, $\sigma(E)) = \sigma(F)(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = F(\alpha_1, \dots, \alpha_n) = E$. Thus σ is an automorphism of E.

(ii) $\implies$ (iii): Let $p(x) \in F[x]$ 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 $p(x)$ 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 β_j are both roots of the irreducible polynomial $p(x)$, there exists an isomorphism $\psi\colon F(\beta_1) \to F(\beta_j) \leq K$. Applying (ii) of the Isomorphism Extension Theorem to the homomorphism $\psi\colon F(\beta_1) \to K$ 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 $\sigma\colon E \to L$ such that $\sigma(a) = \psi(a)$ for all $a \in F(\beta_1)$. In particular, $\sigma(a) = a$ for all $a \in F$. By the hypothesis of (ii), it follows that $\sigma(E) = E$. But by construction $\sigma(\beta_1) = \psi(\beta_1) = \beta_j$, so $\beta_j \in E$ for every root β_j of $p(x)$. It follows that $p(x)$ 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 $\alpha_1, \dots, \alpha_n \in E$ such that $E = F(\alpha_1, \dots, \alpha_n)$. For each i, let $p_i(x) = \mathrm{irr}(\alpha_i, F, x)$. Then $p_i(x)$ is an irreducible polynomial with a root in E. By the hypothesis of (iii), $p_i(x)$ is a product of linear factors in $E[x]$. Let $f(x)$ be the product $p_1(x) \cdots p_n(x)$. Then $f(x)$ is a product of linear factors in $E[x]$, since each of its factors $p_i(x)$ is a product of linear factors, and E is generated over F by some subset of the roots of $f(x)$ and hence by all of the roots (see the comment after the definition of a splitting field). Thus E is a splitting field of $f(x)$. $\square$

Definition 3.7. 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 3.8. *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) $\#(\mathrm{Gal}(E/F)) = [E : F]$.

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 $\sigma\colon E \to L$ such that $\sigma(a) = a$ for all $a \in F$. By the (easy) implication (i) $\implies$ (ii) of Theorem 3.5, $\sigma(E) = E$, i.e. σ is an automorphism of E and hence $\sigma \in \mathrm{Gal}(E/F)$. Conversely, every element of $\mathrm{Gal}(E/F)$ is a homomorphism from E to L which is the identity on F. Hence $\#(\mathrm{Gal}(E/F)) = [E : F]$. $\square$

Definition 3.9. A finite extension E of a field F is a *Galois extension* of F if and only if $\#(\mathrm{Gal}(E/F)) = [E : F]$. 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 3.10. We can now redo the determination of the Galois groups $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ 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 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ is 6. Since there is an injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ to S_3, this implies that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$ and that every permutation of the roots $\{\alpha_1, \alpha_2, \alpha_3\}$ (notation as in Example 2.4(2)) arises via an element of the Galois group. In addition, for every i, $1 \leq i \leq 3$, there exists a unique element σ_1 of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ such that $\sigma_1(\alpha_1) = \alpha_i$ and $\sigma_1(\omega) = \omega$, and a unique element σ_2 of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ such that $\sigma_2(\alpha_1) = \alpha_i$ and $\sigma_2(\omega) = \bar{\omega}$.

A very similar argument handles the case of $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$: Setting

$$\beta_1 = \sqrt[4]{2}; \qquad \beta_2 = i\sqrt[4]{2}; \qquad \beta_3 = -\sqrt[4]{2}; \qquad \beta_4 = -i\sqrt[4]{2},$$

every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ takes $\beta_1 = \sqrt[4]{2}$ to some β_i and takes i to $\pm i$, and every possibility has to occur since the order of $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is 8. Thus for example there exists a $\rho \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ such that $\rho(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\rho(i) = i$. It follows that

$$\rho(\beta_2) = \rho(i\sqrt[4]{2}) = \rho(i)\rho(\sqrt[4]{2}) = i^2\sqrt[4]{2} = -\sqrt[4]{2} = \rho(\beta_3),$$

and similarly that $\rho(\beta_3) = \beta_4$ and that $\rho(\beta_4) = \beta_1$. Hence ρ corresponds to the permutation (1234), and as before it is easy to check from this that $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong D_4$.

Example 3.11. If p is a prime number and $q = p^n$, then $\mathbb{F}_q$ is a separable extension of $\mathbb{F}_p$ since $\mathbb{F}_p$ is perfect and it is normal since it is a splitting field of $x^q - x$ over $\mathbb{F}_p$. Thus $\mathbb{F}_q$ is a Galois extension of $\mathbb{F}_p$. The order of the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is thus $[\mathbb{F}_q : \mathbb{F}_p] = n$. On the other hand, we claim that, if σ_p is the Frobenius automorphism, then the order of σ_p in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is exactly n: Clearly, $\sigma_p^k = \mathrm{Id} \iff \sigma_{p^k}(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_q$. Moreover, by our computations on finite fields, $(\sigma_p)^k = \sigma_{p^k}$, and $\sigma_{p^k}(\alpha) = \alpha$ $\iff$ α 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 $\sigma_p^k \neq \mathrm{Id}$ for $k < n$. Finally, as we have seen, $(\sigma_p)^n = \sigma_{p^n} = \sigma_q = \mathrm{Id}$, so that the order of σ_p in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is n.

Hence $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic and σ_p is a generator, i.e. $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \langle \sigma_p \rangle$. More generally, if $\mathbb{F}_{q'}$ is a subfield of $\mathbb{F}_q$, so that $q = (q')^d$ and $[\mathbb{F}_q : \mathbb{F}_{q'}] = d$, similar arguments show that $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q'})$ is cyclic and $\sigma_{q'}$ is a generator, i.e. $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q'}) \cong \langle \sigma_{q'} \rangle$.

Remark 3.12. 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 $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt[4]{2})$. Then we have seen that $\mathbb{Q}(\sqrt{2})$ 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 $\mathbb{Q}(\sqrt[4]{2})$ 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 $\mathbb{Q}(\sqrt[4]{2})$, but $\mathbb{Q}(\sqrt[4]{2})$ does not contain the root $i\sqrt[4]{2}$ 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 $f(x) \in K[x]$, then it is still a splitting field of $f(x)$ when we view $f(x)$ as an element of $K[x]$.) For example, consider the sequence $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$, where as usual $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. Then we have seen that

$\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a normal extension of $\mathbb{Q}$ (it is the splitting field of $x^3 - 2$), but $\mathbb{Q}(\sqrt[3]{2})$ is not a normal extension of $\mathbb{Q}$ (the irreducible polynomial $x^3 - 2$ has one root in $\mathbb{Q}(\sqrt[3]{2})$, but it does not factor into linear factors in $\mathbb{Q}(\sqrt[3]{2})[x]$).

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

Proposition 3.13. *Suppose that E is a splitting field of the polynomial $f(x) \in F[x]$, where $f(x)$ is* ***irreducible*** *in $F[x]$. Then $\mathrm{Gal}(E/F)$ acts transitively on the roots of $f(x)$.*

Proof. Suppose that the roots of $f(x)$ in E are $\alpha_1, \ldots, \alpha_n$. Fixing one root $\alpha = \alpha_1$ of $f(x)$, it suffices to prove that, for all j, there exists a $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(\alpha_1) = \alpha_j$. By Lemma 2.1, there exists an isomorphism $\psi \colon F(\alpha_1) \to F(\alpha_j)$ such that $\psi(\alpha_1) = \alpha_j$. By the Isomorphism Extension Theorem, there exists an extension field L of E and a homomorphism $\sigma \colon E \to L$ of ψ; in particular, $\sigma(\alpha_1) = \alpha_j$. Finally, by the implication (i) $\implies$ (ii) of Theorem 3.5, the image of σ is E, i.e. in fact an element of $\mathrm{Gal}(E/F)$. $\square$

Example 3.14. Considering the example of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ again, the proposition says that, since $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 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 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ of order 2, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$.

Corollary 3.15. *Suppose that E is a splitting field of the polynomial $f(x) \in F[x]$, where $f(x)$ 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 $\mathrm{Gal}(E/F)$ and the order of $\mathrm{Gal}(E/F)$ divides $n!$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the n distinct roots of $f(x)$ in E. We have sent that there is an injective homomorphism from $\mathrm{Gal}(E/F)$ to S_n, and hence that $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of S_n. By Lagrange's theorem, the order of $\mathrm{Gal}(E/F)$ 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 $\mathrm{Gal}(E/F)$ 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 $\mathrm{Gal}(E/F)$. $\square$

4 The main theorem of Galois theory

Let E be a finite extension of F. Then we have defined the Galois group $\mathrm{Gal}(E/F)$ (although it could be very small). If H is a subgroup of $\mathrm{Gal}(E/F)$, we have defined the *fixed field*

$$E^H = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Clearly $F \le E^H \le E$.

On the other hand, given an intermediate field K between F and E, i.e. a subfield of E containing F, so that $F \le K \le E$, we can define $\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(E/K)$ is clearly a **subgroup** of $\mathrm{Gal}(E/F)$, since if $\sigma(a) = a$ for all $a \in K$, then $\sigma(a) = a$ for all $a \in F$. Thus we have two constructions: one associates an intermediate field to a subgroup of $\mathrm{Gal}(E/F)$, and the other associates a subgroup of $\mathrm{Gal}(E/F)$ to an intermediate field. In general, there is not much that we can say about these two constructions. But if E is a **Galois** extension of F, they turn out to set up a one-to-one correspondence between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields K between F and E, i.e. fields K with $F \le K \le E$.

Theorem 4.1 (Main Theorem of Galois Theory)**.** *Let E be a **Galois** extension of a field F. Then:*

(i) *There is a one-to-one correspondence between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields K between F and E, given as follows: To a subgroup H of $\mathrm{Gal}(E/F)$, we associate the fixed field E^H, and to an intermediate field K between F and E we associate the subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/F)$. These constructions are inverses, in other words*

$$\begin{aligned} \mathrm{Gal}(E/E^H) &= H; \\ E^{\mathrm{Gal}(E/K)} &= K. \end{aligned}$$

In particular, the fixed field of the full Galois group $\mathrm{Gal}(E/F)$ is F and the fixed field of the identity subgroup is E:

$$E^{\mathrm{Gal}(E/F)} = F \qquad \text{and} \qquad E^{\{\mathrm{Id}\}} = E.$$

Finally, since there are only finitely many subgroups of $\mathrm{Gal}(E/F)$, there are only finitely many intermediate fields K between F and E.

(ii) *The above correspondence is order reversing with respect to inclusion.*

(iii) *For every subgroup* H *of* $\mathrm{Gal}(E/F)$, $[E : E^H] = \#(H)$, *and hence* $[E^H : F] = (\mathrm{Gal}(E/F) : H)$. *Likewise, for every intermediate field* K *between* F *and* E, $\#(\mathrm{Gal}(E/K)) = [E : K]$.

(iv) *For every intermediate field* K *between* F *and* E, *the field is a* ***normal*** *extension of* F *if and only if* $\mathrm{Gal}(E/K)$ *is a* ***normal*** *subgroup of* $\mathrm{Gal}(E/F)$. *In this case,* K *is a Galois extension of* F, *and*

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \Big/ \mathrm{Gal}(E/K).$$

Example 4.2. 1) Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We keep the notation of 4) of Example 1.11. If $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, then $G = \{1, \sigma_1, \sigma_2, \sigma_3\}$. The subgroups of G are the trivial subgroups $\{1\}$ and G and the subgroups $\langle \sigma_i \rangle$ of order 2, hence of index 2. As always, $E^{\{1\}} = E$ and $E^G = F = \mathbb{Q}$. Clearly $\sigma_1(\sqrt{3}) = \sqrt{3}$. Thus $\mathbb{Q}(\sqrt{3}) \leq E^{\langle \sigma_1 \rangle}$. But since $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 = (G : \langle \sigma_1 \rangle)$, in fact $\mathbb{Q}(\sqrt{3}) = E^{\langle \sigma_1 \rangle}$. Similarly $\mathbb{Q}(\sqrt{2}) = E^{\langle \sigma_2 \rangle}$. As for $E^{\langle \sigma_3 \rangle}$, since $\sigma_3(\sqrt{2}) = -\sqrt{2}$ and $\sigma_3(\sqrt{3}) = -\sqrt{3}$, it follows that $\sigma_3(\sqrt{6}) = \sqrt{6}$. Thus $\mathbb{Q}(\sqrt{6}) = E^{\langle \sigma_3 \rangle}$.

It is also interesting to look at this example from the viewpoint of $\mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2}+\sqrt{3}$. Using the notation $\alpha = \beta_1 = \sqrt{2}+\sqrt{3}$, $\beta_2 = -\sqrt{2}+\sqrt{3}$, $\beta_3 = \sqrt{2} - \sqrt{3}$, and $\beta_4 = -\sqrt{2} - \sqrt{3}$ identifies σ_1 with $(12)(34)$, σ_2 with $(13)(24)$, and σ_3 with $(14)(23) \in S_4$. It is then clear that $\beta_1 + \beta_2$ is fixed by σ_1. (Of course, so is $\beta_3+\beta_4$, but it is easy to check that $\beta_3+\beta_4 = -(\beta_1+\beta_2)$.) Hence $\mathbb{Q}(\beta_1 + \beta_2) \leq E^{\langle \sigma_1 \rangle}$. On the other hand, $\beta_1 + \beta_2 = 2\sqrt{3}$, and degree arguments as above show that

$$E^{\langle \sigma_1 \rangle} = \mathbb{Q}(\beta_1 + \beta_2) = \mathbb{Q}(2\sqrt{3}) = \mathbb{Q}(\sqrt{3}).$$

Likewise using the element $\beta_1+\beta_3 = 2\sqrt{2}$ which is fixed by σ_2, corresponding to $(13)(24)$ gives $E^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{2})$. If we try to do the same thing with $\sigma_3 = (14)(23)$, however, we find that $\beta_1 + \beta_4 = 0$, since $\sigma_3(\beta_1) = -\beta_4$, and hence we obtain the useless information that $\mathbb{Q}(0) \leq E^{\langle \sigma_3 \rangle}$. To find a nonzero, in fact a nonrational element of E fixed by σ_3, note that as $\sigma_3(\beta_1) = -\beta_1$, $\sigma_3(\beta_1^2) = (-\beta_1)^2 = \beta_1^2$. Now $\beta_1^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, and $\mathbb{Q}(5 + 2\sqrt{6}) = \mathbb{Q}(\sqrt{6})$. Thus as before $\mathbb{Q}(\sqrt{6}) = E^{\langle \sigma_3 \rangle}$.

2) Take $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$. List the roots of $x^3 - 2$ as $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega \sqrt[3]{2}$, $\alpha_3 = \omega^2 \sqrt[3]{2}$. Let $G = \mathrm{Gal}(E/F) \cong S_3$. Now S_3 has the trivial subgroups S_3 and $\{1\}$, as well as $A_3 = \langle (123) \rangle$ and three subgroups of order 2, $\langle (12) \rangle$, $\langle (13) \rangle$, and $\langle (23) \rangle$. Clearly $\alpha_3 \in \mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (12) \rangle}$. Since $[\mathbb{Q}(\alpha_3) : \mathbb{Q}] = 3 = (S_3 : \langle (12) \rangle)$, $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (12) \rangle} = \mathbb{Q}(\alpha_3)$. Similarly $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (13) \rangle} =$

$\mathbb{Q}(\alpha_2)$ and $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle(23)\rangle} = \mathbb{Q}(\alpha_1)$. The remaining fixed field is $\mathbb{Q}(\sqrt[3]{2}, \omega)^{A_3}$, which is a degree 2 extension of $\mathbb{Q}$. Since we already know a subfield of $\mathbb{Q}(\sqrt[3]{2}, \omega)$ which is a degree 2 extension of $\mathbb{Q}$, namely $\mathbb{Q}(\omega)$ it must be equal to $\mathbb{Q}(\sqrt[3]{2}, \omega)^{A_3}$ by the Main Theorem. However, let us check directly that $\omega \in \mathbb{Q}(\sqrt[3]{2}, \omega)^{A_3}$. It suffices to check that the element φ of the Galois group corresponding to (123) satisfies $\varphi(\omega) = \omega$. Note that $\omega = \alpha_2/\alpha_1 = \alpha_3/\alpha_2$. Thus

$$\varphi(\omega) = \varphi(\alpha_2/\alpha_1) = \varphi(\alpha_2)/\varphi(\alpha_1) = \alpha_3/\alpha_2 = \omega,$$

as claimed.

We will describe the more complicated example of $\mathrm{Gal}(\sqrt[4]{2}, i)/\mathbb{Q})$ is a separate handout.

5 Proofs

For simplicity, we shall always assume that F has characteristic zero, or more generally is perfect. In particular, every irreducible polynomial $f(x) \in F[x]$ has only simple zeroes in any extension field of F, and every finite extension of F is automatically separable.

We begin with a proof of the primitive element theorem:

Theorem 5.1. *Let F be a perfect field and let E be a finite extension of F. Then there exists $\alpha \in E$ such that $E = F(\alpha)$.*

Proof. If F is finite we have already proved this. So we may assume that F is infinite. We begin with the following:

Claim 5.2. *Let L be an extension field of the field K, and suppose that $p(x), q(x) \in K[x]$. If the gcd of $p(x)$ and $q(x)$ in $L[x]$ is of the form $x - \xi$, then $\xi \in K$.*

Proof of the claim. We have seen that the gcd of $p(x), q(x)$ in $K[x]$ is a gcd of $p(x), q(x)$ in $L[x]$, and hence they are the same if they are both monic. It follows that $x - \xi$ is the gcd of $p(x), q(x)$ in $K[x]$ and in particular that $\xi \in K$. □

Returning to the proof of the theorem, it is clearly enough by induction to prove that $F(\alpha, \beta) = F(\gamma)$ for some $\gamma \in F(\alpha, \beta)$. Let $f(x) = \mathrm{irr}(\alpha, F, x)$ and let $g(x) = \mathrm{irr}(\beta, F, x)$. There is an extension field L of $F(\alpha, \beta)$ such that $f(x)$ factors into distinct linear factors in L, say $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, with $\alpha = \alpha_1$, and likewise $g(x)$ factors into distinct linear factors in L, say

$g(x) = (x - \beta_1) \cdots (x - \beta_m)$, with $\beta = \beta_1$. Since F is infinite, we can choose a $c \in F$ such that, for all i, j with $j \neq 1$,

$$c \neq \frac{\alpha - \alpha_i}{\beta - \beta_j}.$$

(Notice that we need to take $j \neq 1$ so that the denominator is not zero.) In other words, for all i and j with $j \neq 1$, $\alpha - \alpha_i \neq c(\beta - \beta_j)$. Set $\gamma = \alpha - c\beta$. Then

$$\gamma = \alpha - c\beta \neq \alpha_i - c\beta_j$$

for all i and j with $j \neq 1$. Thus $\gamma + c\beta = \alpha = \alpha_1$, but for all $j \neq 1$, $\gamma + c\beta_j \neq \alpha_i$ for any i.

We are going to construct a polynomial $h(x) \in F(\gamma)[x]$ such that $h(\beta) = 0$ but, for $j \neq 1$, $h(\beta_j) \neq 0$. Once we have done so, consider the gcd of $g(x)$ and $h(x)$ in L (which contains all of the roots $\beta = \beta_1, \ldots, \beta_m$ of $g(x)$). The only irreducible factor of $g(x)$ which divides $h(x)$ is $x - \beta$, which divides $g(x)$ only to the first power. Thus the gcd of $g(x)$ and $h(x)$ in $L[x]$ is $x - \beta$. Since $h(x) \in F(\gamma)[x]$ by construction and $g(x) \in F[x] \leq F(\gamma)[x]$, both $g(x)$ and $h(x)$ are elements of $F(\gamma)[x]$. Then Claim 5.2 implies that $\beta \in F(\gamma)$. But then $\alpha = \gamma + c\beta \in F(\gamma)$ also (recall $c \in F$ by construction). So $\alpha, \beta \in F(\gamma)$, but clearly $\gamma \in F(\alpha, \beta)$. Hence $F(\alpha, \beta) = F(\gamma)$.

Finally we construct $h(x) \in F(\gamma)[x]$. Take $h(x) = f(\gamma + cx)$, where $f(x) = \mathrm{irr}(\alpha, F, x)$. Clearly the coefficients of $h(x)$ lie in $F(\gamma)$. Note that $h(\beta) = f(\gamma + c\beta) = f(\alpha) = 0$, but for $j \neq 1$, $h(\beta_j) = f(\gamma + c\beta_j)$. By construction, for $j \neq 1$, $\gamma + c\beta_j \neq \alpha_i$ for any i, hence $\gamma + c\beta_j$ is not a root of $f(x)$ and so $h(\beta_j) \neq 0$. This completes the construction of $h(x)$ and the proof of the theorem. $\square$

Remark 5.3. For fields F which are not perfect, there can exist simple extensions of F which are not separable as well as finite extensions which are not simple. One can show that a finite extension E of a field F is a simple extension $\iff$ there are only finitely many fields K with $F \leq K \leq E$.

Next we turn to a proof of the Main Theorem of Galois Theory. Let E be a Galois extension of F. Recall that the correspondence given in the Main Theorem between intermediate fields K (i.e. $F \leq K \leq E$ and subgroups H of $\mathrm{Gal}(E/F)$ is as follows: given K, we associate to it the subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/F)$, and given $H \leq \mathrm{Gal}(E/F)$, we associate to it the fixed field $E^H \leq E$. Both of these constructions are clearly order-reversing with respect to inclusion, in other words

$$H_1 \leq H_2 \implies E^{H_2} \leq E^{H_1}$$

and

$$F \leq K_1 \leq K_2 \leq E \implies \mathrm{Gal}(E/K_2) \leq \mathrm{Gal}(E/K_1).$$

This is (ii) of the Main Theorem.

Next we prove (i) and (iii). First, suppose that K is an intermediate field. We will show that $E^{\mathrm{Gal}(E/K)} = K$. Clearly, $K \leq E^{\mathrm{Gal}(E/K)}$. It thus suffices to show that, if $\alpha \in E$ but $\alpha \notin K$, then there exists a $\sigma \in \mathrm{Gal}(E/K)$ such that $\sigma(\alpha) \neq \alpha$, i.e. $\alpha \notin E^{\mathrm{Gal}(E/K)}$. (This says that $E^{\mathrm{Gal}(E/K)} \leq K$ and hence $E^{\mathrm{Gal}(E/K)} = K$.) If $\alpha \notin K$, then $f(x) = \mathrm{irr}(\alpha, K, x)$ is an irreducible polynomial in $K[x]$ of degree $k > 1$. Since E is a normal extension of F and hence of K and the root α of the irreducible polynomial $f(x) \in K[x]$ lies in E, all roots $\alpha = \alpha_1, \dots, \alpha_k$ of $f(x)$ lie in E. Choose some $i > 1$. Then there is an injective homomorphism $\psi\colon K(\alpha) \to E$ such that $\psi|K = \mathrm{Id}$ but $\psi(\alpha) = \alpha_i \neq \alpha$. By the isomorphism extension theorem, there exists an extension L of E such that the homomorphism ψ extends to a homomorphism $\sigma\colon E \to L$. Since E is a normal extension of F and $\sigma|F = \mathrm{Id}$, $\sigma(E) = E$ and thus $\sigma \in \mathrm{Gal}(E/F)$. Since $\sigma|K = \psi|K = \mathrm{Id}$, in fact $\sigma \in \mathrm{Gal}(E/K)$. We have thus found the desired σ. Note further that, as E is a Galois extension of K, we must have $\#(\mathrm{Gal}(E/K)) = [E : K]$.

Now suppose that H is a subgroup of $\mathrm{Gal}(E/F)$. We claim that

$$\mathrm{Gal}(E/E^H) = H.$$

Clearly, $H \leq \mathrm{Gal}(E/E^H)$ by definition. Thus, $\#(H) \leq \#(\mathrm{Gal}(E/E^H))$. To prove that $\mathrm{Gal}(E/E^H) = H$, it thus suffices to show that $\#(\mathrm{Gal}(E/E^H)) \leq \#(H)$. This will follow from:

Claim 5.4. *For all $\alpha \in E$, $\deg_{E^H} \alpha \leq \#(H)$.*

First let us see that Claim 5.4 implies that $\#(\mathrm{Gal}(E/E^H)) \leq \#(H)$. By the Primitive Element Theorem, there exists an $\alpha \in E$ such that $E = E^H(\alpha)$, and hence $\deg_{E^H} \alpha = [E : E^H]$. For this α, Claim 5.4 implies that

$$\#(\mathrm{Gal}(E/E^H)) = [E : E^H] = \deg_{E^H} \alpha \leq \#(H).$$

Thus $\#(H) \geq \#(\mathrm{Gal}(E/E^H))$. But $H \leq \mathrm{Gal}(E/E^H)$ and hence $\#(H) \leq \#(\mathrm{Gal}(E/E^H))$. Clearly we must have $\mathrm{Gal}(E/E^H) = H$ and $\#(H) = \#(\mathrm{Gal}(E/E^H))$, proving the rest of (i) and (iii).

To prove Claim 5.4, given $\alpha \in E$ consider the polynomial

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)).$$

The number of linear factors of $f(x)$ is $\#(H)$, so that $f(x) \in E[x]$ is a polynomial of degree $\#(H)$. We claim that in fact $f(x) \in E^H[x]$, in other words that all coefficients of $f(x)$ lie in the fixed field E^H. It suffices to show that, for all $\psi \in H$, $\psi(f)(x) = f(x)$. Now, using the fact that ψ is an automorphism, it is easy to see that

$$\psi(f)(x) = \prod_{\sigma \in H} (x - \psi\sigma(\alpha)).$$

As $\psi \in H$, the function $\sigma \in H \mapsto \psi\sigma$ is a permutation of the group H (cf. the proof of Cayley's theorem!) and so the product $\prod_{\sigma \in H}(x - \psi\sigma(\alpha))$ is the same as the product $\prod_{\sigma \in H}(x - \sigma(\alpha))$ (but with the order of the factors changed, if $\psi \neq \mathrm{Id}$). Hence $\psi(f)(x) = f(x)$ for all $\psi \in H$, so that $f(x) \in E^H[x]$. It follows that $\mathrm{irr}(\alpha, E^H, x)$ divides $f(x)$, and hence that $\deg_{E^H} \alpha \leq \deg f(x) = \#(H)$.

Finally we must prove (iv) of the Main Theorem. Let $F \leq K \leq E$. The first statement of (iv) is the statement that K is a normal (hence Galois) extension of $F \iff \mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$. A slight variation of the proof of Theorem 3.5 shows that K is a normal extension of $F \iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(K) = K$. More generally, for K an arbitrary intermediate field, given $\sigma \in \mathrm{Gal}(E/F)$, we can ask for a description of the image subfield $\sigma(K)$ of E. By Part (i) of the Main Theorem (already proved), it is equivalent to describe the corresponding subgroup $\mathrm{Gal}(E/\sigma(K))$ of $\mathrm{Gal}(E/F)$.

Claim 5.5. *In the above notation,* $\mathrm{Gal}(E/\sigma(K)) = \sigma \cdot \mathrm{Gal}(E/K) \cdot \sigma^{-1} = i_\sigma(\mathrm{Gal}(E/K))$*, where* i_σ *is the inner automorphism of* $\mathrm{Gal}(E/F)$ *given by conjugation by the element* σ.

Proof. If $\varphi \in \mathrm{Gal}(E/F)$, then $\varphi \in \mathrm{Gal}(E/\sigma(K)) \iff$ for all $\alpha \in K$, $\varphi(\sigma(\alpha)) = \sigma(\alpha) \iff$ for all $\alpha \in K$, $\sigma^{-1}\varphi\sigma(\alpha) = \alpha \iff \sigma^{-1}\varphi\sigma \in \mathrm{Gal}(E/K) \iff \varphi \in \sigma \cdot \mathrm{Gal}(E/K) \cdot \sigma^{-1}$. □

Now apply the remarks above: K is a normal extension of $F \iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(K) = K \iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\mathrm{Gal}(E/\sigma(K)) = \mathrm{Gal}(E/K)$ (by (i) of the Main Theorem) $\iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\mathrm{Gal}(E/K) = \sigma \cdot \mathrm{Gal}(E/K) \cdot \sigma^{-1} \iff \mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$. This proves the first statement of (iv). We must then show that $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \big/ \mathrm{Gal}(E/K)$. To see this, given $\sigma \in \mathrm{Gal}(E/F)$, we have seen that $\sigma(K) = K$, and hence that $\sigma \mapsto \sigma|K$ defines a function from $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(K/F)$. Clearly, this is a homomorphism, and by definition its kernel is just the subgroup of $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma|K = \mathrm{Id}$, which by definition is $\mathrm{Gal}(E/K)$. To see that $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \big/ \mathrm{Gal}(E/K)$, by the fundamental homomorphism theorem, it suffices to show that the homomorphism $\sigma \mapsto \sigma|K$ is a surjective homomorphism from $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(K/F)$. This says that, given a $\psi\colon K \to K$ such that $\psi|F = \mathrm{Id}$, there exists an extension of ψ to a $\sigma \in \mathrm{Gal}(E/F)$. But it follows from the Isomorphism Extension Theorem that, given ψ, there exists an extension field L of E and an extension of ψ to a homomorphism $\sigma\colon E \to L$. Since E is a normal extension of F, $\sigma(E) = E$, and hence $\sigma \in \mathrm{Gal}(E/F)$ is such that $\sigma \mapsto \psi \in \mathrm{Gal}(K/F)$. It follows that restriction defines a surjective homomorphism $\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ with kernel $\mathrm{Gal}(E/K)$, so that $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \big/ \mathrm{Gal}(E/K)$. This concludes the proof of the Main Theorem. $\square$