Notes on Galois Theory II

2 The isomorphism extension theorem

We begin by proving the converse to Lemma 1.7 in a special case. Suppose that $E = F(\alpha)$ is a **simple** extension of F and let $f = \mathrm{irr}(\alpha, F, x)$. If $\psi\colon F \to K$ is a homomorphism, L is an extension field of K, and $\varphi\colon E \to L$ is an extension of ψ, the $\varphi(\alpha)$ is a root of $\psi(f)$. The following is the 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 $f = \mathrm{irr}(\alpha, F, x)$, let $\psi\colon F \to K$ 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 $\psi(f)$, then there is a unique extension of ψ to a homomorphism $\varphi\colon E \to L$ such that $\varphi(\alpha) = \beta$.*

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

Proof. Let $\beta \in L$ be a root of $\psi(f)$. We know by basic field theory that there is an isomorphism $\sigma\colon F(\alpha) \cong F[x]/(f)$ with the property that $\sigma(a) = a + (f)$ for $a \in F$ and $\sigma(\alpha) = x + (f)$. Let $\mathrm{ev}_\beta \circ \psi$ be the homomorphism $F[x] \to L$ defined as follows: given a polynomial $g \in F[x]$, let (as above) $\psi(g)$ be the polynomial obtained by applying ψ to the coefficients of g, and let $\mathrm{ev}_\beta \circ \psi(g) = \psi(g)(\beta) = \mathrm{ev}_\beta(\psi(g)$ be the evaluation of $\psi(g)$ at β. Then $\mathrm{ev}_\beta \circ \psi$ is a homomorphism from $F[x]$ to K. For $a \in F$, $\mathrm{ev}_\beta \circ \psi(a) = \psi(a)$, and $\mathrm{ev}_\beta \circ \psi(x) = \beta$. Moreover $f \in \mathrm{Ker}\, \mathrm{ev}_\beta \circ \psi$, since $\psi(f)(\beta) = 0$ by hypothesis. Thus $(f) \subseteq \mathrm{Ker}\, \mathrm{ev}_\beta \circ \psi$ and hence $(f) = \mathrm{Ker}\, \mathrm{ev}_\beta \circ \psi$ since (f) is a maximal ideal and $\mathrm{ev}_\beta \circ \psi$ is not the trivial homomorphism. Then there is an induced homomorphism $e\colon F[x]/(f) \to L$. Let φ be the induced homomorphism $e \circ \sigma\colon F(\alpha) \to L$. It is easily checked to satisfy: $\varphi(a) = \psi(a)$ for all $a \in F$ and $\varphi(\alpha) = \beta$.

Next we claim that φ is uniquely specified by the conditions $\varphi(a) = \psi(a)$ 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

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

Thus φ is uniquely specified by the conditions above. In summary, then, every extension φ of ψ satisfies: $\varphi(\alpha)$ is a root of $\psi(f)$, φ is uniquely determined by the value $\varphi(\alpha) \in L$, and all possible roots of $\psi(f)$ in L arise as $\varphi(\alpha)$ for some extension φ of ψ. Thus the function $\varphi \mapsto \varphi(\alpha)$ is a function from the set of extensions φ of ψ to the set of roots of $\psi(f)$ 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 2.2. *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 $\psi\colon F \to K$ be a homomorphism. Then:*

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

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

Proof. Let $n = \deg f = [E : F]$. Then $\deg \psi(f) = n$ as well. Lemma 2.1 implies that the extensions of ψ to a homomorphism $\varphi\colon F(\alpha) \to L$ are in one-to-one correspondence with the $\beta \in K$ such that β is a root of $\psi(f)$, where $f = \mathrm{irr}(\alpha, F, x)$. In this case, since $\psi(f)$ has at most $n = [E : F]$ roots in any extension field L, there are at most n extensions of ψ, proving (i). To see (ii), choose an extension field L of K such that $\psi(f)$ has a root β in L. Thus there will be at least one homomorphism $\varphi\colon F(\alpha) \to L$ extending ψ. To see (iii), choose an extension field L of K such that $\psi(f)$ 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 $\psi(f) \in \psi(F)[x]$, where $\psi(F)$ is the image of F in K, since $\psi(f)$ is also irreducible. Thus there are n distinct roots of $\psi(f)$ in L, and hence n different extensions of ψ to a homomorphism $\varphi\colon F(\alpha) \to L$. $\square$

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

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

Let us give some examples to show how one can use Lemma 2.1, especially in case the homomorphism ψ is not the identity:

Example 2.3. (1) Consider the sequence of extensions $\mathbb{Q} \le \mathbb{Q}(\sqrt{2}) \le \mathbb{Q}(\sqrt{2}, \sqrt{3})$. 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 $f = x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$. Since in fact $f \in \mathbb{Q}[x]$, $\sigma(f) = f$, and clearly $\mathrm{Id}(f) = f$. In particular, the roots of $\sigma(f) = f$ are $\pm\sqrt{3}$. Applying Lemma 2.1 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 **??**.

(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 $\mathbb{Q} \le \mathbb{Q}(\omega) \le \mathbb{Q}(\sqrt[3]{2}, \omega)$. 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 $f = x^3 - 2$ is irreducible in $\mathbb{Q}(\omega)$. In fact, since $\deg f = 3$, f is reducible in $\mathbb{Q}(\omega) \iff$ there exists a root α 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 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 (2), 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 2.4 (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 $\varphi\colon E \to K$ extending ψ, i.e. such that $\varphi(\alpha) = \psi(\alpha)$ for all $\alpha \in F$.*

(ii) *There exists an extension field L of K and a homomorphism $\varphi\colon E \to L$ 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 $\varphi\colon E \to L$ 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 2.2.

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 $F \leq F_1 \leq E$. Notice that, given an extension of ψ to a homomorphism $\varphi\colon F_1 \to K$ and an extension τ of φ 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 φ of ψ to F_1, by taking $\varphi(\alpha) = \tau(\alpha)$ for $\alpha \in F_1$ (i.e. φ is the restriction of τ to F_1), and clearly τ is an extension of φ 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 $\{\varphi_1, \dots, \varphi_d\}$, with $d \leq [F_1 : F]$. Fix one such homomorphism φ_i. Applying Corollary 2.2 to the simple extension $F_1(\alpha) = E$ and the homomorphism $\varphi_i\colon F_1 \to K$, there are at most e extensions of φ_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 φ_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 $d \leq [F_1 : F]$ 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 $f_1 = \mathrm{irr}(\alpha, F_1, x)$. Adjoining a root of $\psi_1(f_1)$ to L_1 if necessary, to obtain an extension field L of L_1 containing a root of $\psi_1(f_1)$, it follows from Corollary 2.2 that there exists a homomorphism $\varphi\colon F_1(\alpha) = E \to L$ 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 $\{\varphi_1, \dots, \varphi_d\}$, with $d = [F_1 : F]$. As before, we let $f_1 = \mathrm{irr}(\alpha, F_1, x)$. There exists a finite extension L of the field L_1 such that every one of the (not necessarily distinct) irreducible polynomials $\varphi_i(f_1) \in \varphi_i(F_1)[x]$ 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 φ_i. Again applying Corollary 2.2 to the simple extension $F_1(\alpha) = E$ and the homomorphism $\varphi_i\colon F_1 \to L$, there are exactly e extensions of φ_i to a homomorphism $\tau_{ij}\colon F_1(\alpha) \to L$. In all, since each of the d extensions φ_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 2.5. *Let E be a finite extension of F. Then*

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

Definition 2.6. 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 $\varphi \colon E \to L$ 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 $\iff$ 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 2.7 (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 2.5, 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 $\varphi \colon E \to L$, 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 $\varphi \colon E \to L$, 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 $f \in F[x]$ 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), $E = F(\alpha_1, \dots, \alpha_n)$. 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 3.2. (i) Clearly, E is a splitting field of f over F if (i) holds (f 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 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 over F and K is an intermediate field, i.e. $F \le K \le E$, 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 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, $f \in F[x]$ is an irreducible polynomial of degree 2, and $E = F(\alpha)$, where α 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 $x^4 - 10x^2 + 1$.

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 ζ^i for some i. Note that, as Φ_5 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, 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 α_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 α_2 is a root of f_1 in some extension field of $\mathbb{Q}(\alpha_1)$, then $[\mathbb{Q}(\alpha_1)(\alpha_2) : \mathbb{Q}(\alpha_1)] = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] = n - 1$ 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 $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ 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 $f \in F[x]$ of degree at least one such that E is a splitting field of f.*

(ii) *For every extension field L of E, if $\varphi\colon E \to L$ is a homomorphism such that $\varphi(a) = a$ for all $a \in F$, then $\varphi(E) = E$, and hence φ 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 3.6. *Let L be an extension field of a field F and let $\alpha_1, \dots, \alpha_n \in L$. If $\varphi\colon E = F(\alpha_1, \dots, \alpha_n) \to L$ is a homomorphism, then $\varphi(E) = \varphi(F)(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$.*

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

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

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

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

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 $f = c\prod_{i=1}^n(x - \alpha_i)$. 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 $\varphi(\{\alpha_1, \dots, \alpha_n\}) \subseteq \{\alpha_1, \dots, \alpha_n\}$. Since $\{\alpha_1, \dots, \alpha_n\}$ is finite set and φ is injective, it induces a surjective map from $\{\alpha_1, \dots, \alpha_n\}$ to itself, i.e. φ permutes the roots of f in $E \le L$. By Lemma 3.6, $\varphi(E)) = \varphi(F)(\varphi(\alpha_1), \dots, \varphi(\alpha_n)) = F(\alpha_1, \dots, \alpha_n) = E$. Thus φ 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 β_j are both roots of the irreducible polynomial p, there exists an isomorphism $\psi\colon F(\beta_1) \to F(\beta_j) \le K$. 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 $\varphi\colon E \to L$ such that $\varphi(a) = \psi(a)$ 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 $\varphi(\beta_1) = \psi(\beta_1) = \beta_j$, so $\beta_j \in E$ for every root β_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 $\alpha_1, \dots, \alpha_n \in E$ such that $E = F(\alpha_1, \dots, \alpha_n)$. For each i, let $p_i = \operatorname{irr}(\alpha_i, F, x)$. 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. $\square$

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

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 $\varphi\colon E \to L$ such that $\varphi(a) = a$ for all $a \in F$. By the (easy) implication (i) $\implies$ (ii) of Theorem 3.5, $\varphi(E) = E$, i.e. φ 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 $\#(\operatorname{Gal}(E/F)) = [E : F]$. $\square$

Definition 3.9. 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 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 2.3(2)) arises via an element of the Galois group. In addition, for every i, $1\le i\le 3$, 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 $f \in K[x]$, then it is still a splitting field of f when we view f as an element of $K[x]$.) For example, consider the sequence $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$, 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 $f \in F[x]$, where f is* ***irreducible*** *in $F[x]$. Then $\mathrm{Gal}(E/F)$ acts transitively on the roots of f.*

Proof. Suppose that the roots of f in E are $\alpha_1, \dots, \alpha_n$. Fixing one root $\alpha = \alpha_1$ of f, it suffices to prove that, for all j, there exists a $\varphi \in \mathrm{Gal}(E/F)$ such that $\varphi(\alpha_1) = \alpha_j$. 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 $\varphi\colon E \to L$ of ψ; in particular, $\varphi(\alpha_1) = \alpha_j$. Finally, by the implication (i) $\implies$ (ii) of Theorem 3.5, the image of φ 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 $f \in F[x]$, 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 $\mathrm{Gal}(E/F)$ and the order of $\mathrm{Gal}(E/F)$ divides $n!$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the n distinct roots of f 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 $\mathrm{Gal}(E/F)$. $\square$