Chapter 7

Galois Theory

7.1 Extension Automorphism Group

03/25/19

Lemma 7.1.1 *Let E/F be a field extension. The set of automorphisms of the extension E/F, i.e. automorphisms of E that fix the elements of F,*

$$\{\varphi \in \mathrm{Aut}(E) \mid \varphi(a) = a \text{ for all } a \in F\}$$

is a group, a subgroup of $\mathrm{Aut}(E)$.

Definition 7.1.1. Let E/F be a field extension. The group of automorphisms of this extension, is denoted by $\mathrm{Aut}_F(E)$ or by $\mathrm{Gal}(E : F)$, and is sometimes called the *Galois group* of the extension E/F.[1]

Note that any automorphism of E fixes 1 and therefore it fixes the prime subfield of E. If $\mathrm{char}(E) = 0$ then $\mathrm{Aut}(E) = \mathrm{Aut}_{\mathbb{Q}}(E)$. If $\mathrm{char}(E) = p$, then $\mathrm{Aut}(E) = \mathrm{Aut}_{\mathbb{Z}_p}(E)$.

Examples 7.1.1. 1. $\mathrm{Aut}_F(F) = \{1_F\}$.

2. Denote by τ the complex conjugation map

$$\begin{array}{rccc} \tau: & \mathbb{C} & \to & \mathbb{C} \\ & a+bi & \mapsto & a-bi \end{array}$$

[1] Some authors reserve the name "*Galois group*" for extensions which are Galois extensions. See Definition 7.4.3.

It is straight forward to check that τ is an autormorphism of $\mathbb{C}$ and it fixes the elements of $\mathbb{R}$. Therefore, $\tau \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. It follows from Proposition 7.1.6 below that $1_{\mathbb{C}}$ and τ are the only automorphisms of the extension $\mathbb{C}/\mathbb{R}$. Thus $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1_{\mathbb{C}}, \tau\}$.

We will often need to consider homomorphisms from a field of the form $F(\alpha_1, \ldots, \alpha_n)$, where F is a field and $\alpha_1, \ldots, \alpha_n$ come from an extension of F, to another field or ring. The next lemma tells us that such homomorphism is completely determined by where it maps the elements of F, as well as, where it maps $\alpha_1, \ldots, \alpha_n$. 03/26/19

Lemma 7.1.2 *Let F be a field, $\alpha_1, \ldots, \alpha_n$ elements from some extension E of F, and R a commutative ring with unity. If $\varphi_1, \varphi_2 : F(\alpha_1, \ldots, \alpha_n) \to R$ are homomorphisms such that $\varphi_1(a) = \varphi_2(a)$ for all $a \in F$ and $\varphi_1(\alpha_i) = \varphi_1(\alpha_i)$ for $i = 1, \ldots, n$, then $\varphi_1 = \varphi_2$.*

Exercise 7.1.1. Prove Lemma 7.1.2.

Corollary 7.1.3 *Let $E = F(\alpha_1, \ldots, \alpha_n)$ be an extension of F, and K another extension of F. Any F-homomorphism $\varphi : E \to K$ is completely determined by the values $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ in K.*

In order to work out examples of automorphism groups of extensions, we will use a converse of Lemma 6.4.13, as well as a special cases of that lemma and its converse.

Lemma 7.1.4 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Let $p(x) \in F[x]$ be an irreducible polynomial, and denote by $\hat{p}(x)$ its image $\varphi(p(x)) \in \hat{F}[x]$. If α is a root of $p(x)$ in some extension K of F, $\hat{K}$ an extension of $\hat{F}$, and $\tilde{\varphi} : K \to \hat{K}$ a homomorphism that extends φ, then $\tilde{\varphi}(\alpha)$ is a root of $\hat{p}(x)$.*

$$\begin{array}{ccc} K & \xrightarrow{\tilde{\varphi}} & \hat{K} \\ | & & | \\ F & \xrightarrow{\varphi} & \hat{F} \end{array}$$

Proof. Let $\hat{\alpha} = \tilde{\varphi}(\alpha)$. Then

$$\hat{p}(\hat{\alpha}) = \varphi(p)(\tilde{\varphi}(\alpha)) = \tilde{\varphi}(p)(\tilde{\varphi}(\alpha)) = \tilde{\varphi}(p(\alpha)) = \tilde{\varphi}(0) = 0 \qquad \blacksquare$$

The following propositions are special cases of Lemma 6.4.13, and Lemma 7.1.4, by taking $\hat{F} = F$, $\varphi = I_F$, and $\hat{K} = K$ for the second one.

Proposition 7.1.5 *Let K and E be extensions of F. Let $\alpha \in K$ be algebraic over F, and $\beta \in E$ be a root of $\min_F(\alpha)$. There is a F-homomorphism (i.e. it fixes every $a \in F$) $\varphi : F(\alpha) \to E$, such that $\varphi(\alpha) = \beta$.*

Proposition 7.1.6 *Let K/F be an extension and $\alpha \in K$ algebraic over F. For each $\varphi \in \mathrm{Aut}_F(K)$, $\varphi(\alpha)$ is a root of $\min_F(\alpha)$ in K.*

Now, we are ready to complete Example 7.1.1.2, and consider other examples.

Example 7.1.2.

1. Since $\mathbb{C} = \mathbb{R}(i)$, any automorphism of $\mathbb{C}/\mathbb{R}$ is completely determined by where it maps i. From Proposition 7.1.6 we know that i has to be mapped to a root of $\min_{\mathbb{R}}(i) = x^2 + 1$, i.e. to $\pm i$, confirming the statement that $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1_{\mathbb{C}}, \tau\}$.

2. We know that $\min_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2$. A similar argument to that of the previous example shows that there are only two automorphisms of the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, namely the identity map $1_{\mathbb{Q}(\sqrt{2})}$, and the map

$$\begin{array}{rccc} \gamma: & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ & a + b\sqrt{2} & \mapsto & a - b\sqrt{2} \end{array}$$

   Thus $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{1, \gamma\}$.

3. Consider now the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Since $\min_{\mathbb{Q}}(\sqrt[3]{2}) = x^3 - 2$, has roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, but the last two are not in $\mathbb{Q}(\sqrt[3]{2})$ (they are not even real numbers), the only automorphism of $\mathbb{Q}(\sqrt[3]{2})$ is the identity map. Thus, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$.

4. Let's consider now the extension $E := \mathbb{Q}(\sqrt[3]{2}, \omega)$ of $\mathbb{Q}$. Note first that since $\mathbb{Q}$ is the prime field, any automorphism of E will fix $\mathbb{Q}$. The minimal polynomial $\min_{\mathbb{Q}}(\sqrt[3]{2}) = x^3 - 2$ has roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, and the minimal polynomial $\min_{\mathbb{Q}}(\omega) = x^2 + x + 1$ has roots ω, ω^2. By Proposition 7.1.6, there are only six potential automorphisms of the

extension $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, namely:

$$I: \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \\ \omega & \mapsto & \omega \end{array} \qquad \sigma_1: \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \\ \omega & \mapsto & \omega^2 \end{array}$$

$$\rho: \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} \\ \omega & \mapsto & \omega \end{array} \qquad \sigma_2: \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} \\ \omega & \mapsto & \omega^2 \end{array}$$

$$\rho^2: \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \omega^2\sqrt[3]{2} \\ \omega & \mapsto & \omega \end{array} \qquad \sigma_3: \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \omega^2\sqrt[3]{2} \\ \omega & \mapsto & \omega^2 \end{array}$$

Proposition 7.1.5, guarantees the existence of automorphisms doing what each of the above does. Therefore

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega)) = \{I, \rho, \rho^2, \sigma_1, \sigma_2, \sigma_3\}$$

Straightforward calculation of the table for this group, shows that it is isomorphic to D_3.

The following Corollary to Lemmas 7.1.4 and 6.4.13, gives us both an upper bound, and an exact count, on the number of homomorphisms from a simple algebraic extension, extending a given homomorphism from the ground field.

Corollary 7.1.7 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Let K be an extension of F, and $\alpha \in K$ algebraic over F, and $\hat{K}$ an extension of $\hat{F}$. The number of homomorphism $\tilde{\varphi} : F(\alpha) \to \hat{K}$ which extend φ is at most $\deg_F(\alpha)$. Moreover, let $p(x) = \min_F(\alpha)$, and $\hat{p}(x) = \varphi(p(x))$. The number of homomorphism $\tilde{\varphi} : F(\alpha) \to \hat{K}$ which extend φ is the number of distinct roots of $\hat{p}(x)$ in $\hat{K}$.*

Proof. Any homomorphism $\tilde{\varphi} : F(\alpha) \to \hat{K}$ that extends φ is completely determined by the value fo $\tilde{\varphi}(\alpha)$. Take $p(x) = \min_F(\alpha)$ in the lemma. Since $\deg_{\hat{F}}(\hat{p}(x)) = \deg_F(p(x)) = \deg_F(u)$, the polynomial $\hat{p}(x)$ has at most this many distinct roots, so there are at most $\deg_F(\alpha)$ choices for $\tilde{\varphi}(\alpha)$. ∎

Scholium 7.1.8 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Let E be an extension of F, and $u \in E$ algebraic over F, and $\hat{K}$ an extension of $\hat{F}$. Let $f = \min_F(u)$, and $\hat{f} = \varphi(F)$. The number of homomorphism $\tilde{\varphi} : F(u) \to \hat{K}$ which extend φ is the number of distinct roots of $\hat{f}$ in $\hat{K}$.*

As a particular case of Corollary **??** we get:

enough automorphisms

Proposition 7.1.9 *Let $E = F(\alpha)$ be a simple finite extension of F. Then*

$$|\mathrm{Aut}_F(E)| \leq [E : F]. \tag{7.1}$$

Proof. Let $f(x) = \min_F(\alpha)$, and let $\alpha_1, \ldots, \alpha_k$ be the distinct roots of $f(x)$ in E. Let $n = \deg(f(x))$, so $k \leq n$. By Corollary 6.2.8, we know that $[E : F] = n$, and by Corollary 7.1.7, $|\mathrm{Aut}_F(E)| = k$. ∎

03/27/19 Note that in order to get equality in Proposition 7.4.1 it is necessary and sufficient that $f(x)$ has all its roots in E, and that it has no multiple roots.

Corollary 7.1.10 *Let $E = F(\alpha)$ be a finite simple extension. $|\mathrm{Aut}_F(E)| = [E : F]$ iff $f(x) = \min_F(\alpha)$ has no multiple roots, and E is the splitting field of $f(x)$.*

In Examples 7.1.1 we have

$$\begin{array}{lcll} |\mathrm{Aut}_F(F)| & = & 1 & = [F : F], \\ |\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})| & = & 2 & = [\mathbb{C} : \mathbb{R}], \\ |\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))| & = & 1 < 3 & = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}], \text{ and} \\ |\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega))| & = & 6 & = [\mathbb{Q}(\sqrt[3]{2}, \omega)) : \mathbb{Q}]. \end{array}$$

When equality holds in (7.1), we say that the extension E/F has *enough automorphisms*. When an extension has enough automorphisms, the automorphism group carries information about the extension. See, for example, Theorem 7.4.10, The Fundamental Theorem of Galois Theory.

The two conditions needed for a (simple) extension to have enough automorphims, are:

- The minimal polynomial $\min_F(\alpha)$ has no multiple roots,
- the field E is the splitting field of that minimal polynomial.

We are now going to study these two properties separately, and then jointly.

separable
separable
separable
inseparable

7.2 Separable Extensions

Definition 7.2.1. An irreducible polynomial $p(x) \in F[x]$ is said to be *separable* over F, if it has no multiple roots. A non-constant, polynomial $f(x) \in F[x]$ is *separable* over F it each of its irreducible factors is separable over F. For an extension E/F and $\alpha \in E$, we say that α is *separable* over F if its minimal polynomial $\min_F(\alpha)$ is separable over F, and we say that E is separable over F if every element of E is separable over F. When a polynomial, an extension, or an element is not separable over F, we say that it is *inseparable* over F.

Proposition 7.2.1 *An irreducible polynomial $p(x) \in F[x]$ is separable iff $p'(x) \neq 0$.*

Proof. Assume $p'(x) \neq 0$. Since $p(x)$ is irreducible and $\deg(p'(x)) < \deg(p(x))$, no root of $p(x)$ can be a root of $p'(x)$. By Proposition 6.6.2, $p(x)$ has no multiple roots, hence it is separable.
Conversely, assume $p(x)$ has no multiple roots, then for any root α of $p(x)$ we must have $p'(u) \neq 0$, and therefore $p'(x) \neq 0$. ■

Corollary 7.2.2 *In characteristic 0, all irreducible polynomials, all non-constant polynomials, all algebraic elements, and all algebraic extensions are separable.*

Corollary 7.2.3 *Let $\mathrm{char}(F) = p$, and $p(x) \in F[x]$ be irreducible. Then $p(x)$ is inseparable iff $p(x)$ is of the form $g(x^p)$ for some $g(x) \in F[x]$.*

Proof. ■

Proposition 7.2.4 *For any $n \in \mathbb{N}$, the finite field $\mathbb{F}_{p^n}$ is separable over $\mathbb{Z}_p$.*

Proof. Note that the polynomial $f(x) = x^{p^n} - x$ is separable since $f'(x) = -1$, and $f(x)$ has no multiple roots. Any element of $\alpha \in \mathbb{F}_{p^n}$ is a root of $f(x)$, so $\min_{\mathbb{Z}_p}(\alpha)$ is a factor of $f(x)$, has no multiple roots, hence it is separable. ■

Proposition 7.2.5 *Let $K/E/F$ be an extension tower. If K is separable over F then K is separable over E and E is separable over F.*

Proof. ■

rational functions
field of rational functions

The converse of Proposition 7.2.5, is true, but we will not prove it.

03/29/19 **Proposition 7.2.6** *Every algebraic extension of a finite field is separable.*

Proof. Let F be a finite field of characteristic p, and E an algebraic extension of F. Let $\alpha \in E$. Since α is algebraic over F, the field $F(\alpha)$ is a finite extension of F, hence a finite field. From Proposition 7.2.4 we know that $\min_{\mathbb{Z}_p}(\alpha)$ is separable. But $\min_F(\alpha)$ is a factor of $\min_{\mathbb{Z}_p}(\alpha)$, and therefore it is also separable. ■

From Proposition 7.2.6, and Corollary 7.2.2, we see that the only way to find an inseparable extension, is by looking at infinite fields of prime characteristic. We now define one such field.

Definition 7.2.2. Let F be a field, and $F[x]$ the ring of polynomials with coefficients in F. Since $F[x]$ is an integral domain, it has a field of quotients. We denote by $F(x)$ the field of quotients of $F[x]$. Each element in $F(x)$ is of the from $\dfrac{f(x)}{g(x)}$ with $f(x), g(x) \in F[x]$, and $g(x) \neq 0$. The elements of $F(x)$ are called *rational functions* over F, and we call $F(x)$ the *field of rational functions* over F.

Every polynomial is a rational function, and every rational function is a quotient of two polynomials. Sometimes we will use a variable other than x for the rational functions, so that we can consider polynomials on x over a field of rational functions.

Lemma 7.2.7 *Let $0 \neq h(x) \in F(x)$ be a rational function over F. The integer $\deg(f(x)) - \deg(g(x))$ where $h(x) = \dfrac{f(x)}{g(x)}$, with $0 \neq f(x), g(x) \in F[x]$ is well-defined.*

Proof. Use the fact that for non-zero polynomials, the degree of a product is the sum of the degrees. ■

Definition 7.2.3. For $0 \neq h(x) \in F(x)$ a rational function over F, we denote by $\deg(h(x))$ the integer $\deg(f(x)) - \deg(g(x))$ where $h(x) = \frac{f(x)}{g(x)}$, with $0 \neq f(x), g(x) \in F[x]$.

Example 7.2.1. Let $F = \mathbb{Z}_2(t)$ be the field of rational functions over $\mathbb{Z}_2$, on the variable t. Consider the polynomial $p(x) = x^2 - t \in F[x]$. Note that for any $0 \neq h(t) = \dfrac{f(t)}{g(t)} \in F$, we have

$$\begin{aligned} \deg(h^2(t)) &= \deg\left(\frac{f^2(t)}{g^2(t)}\right) \\ &= \deg(f^2(t)) - \deg(g^2(t)) \\ &= 2\deg(f(t)) - 2\deg(g(t)) \\ &= 2(\deg(f(t)) - \deg(g(t))) \\ &= 2\deg(h(t)) \end{aligned}$$

is an even integer. In order to have $h(t)$ as a root of $x^2 - t$ we would need $h^2(t) - t = 0$, i.e. $h^2(t) = t$, but this is impossible since the left hand side, as a rational function on t, has even degree, and the right hand side has degree 1. Being quadratic, with no roots in F, the polynomial $p(x) = x^2 - t$ is irreducible over F. Let α be a root of this polynomial in some extension E of F. We have $\alpha^2 = t$, and therefore $(x - \alpha)^2 = x^2 - \alpha^2 = x^2 - t$. The irreducible polynomial $p(x) = x^2 - t$ has α as a root of multiplicity 2, hence it is inseparable. The element α is inseparable over F, and the extension E is inseparable over F.

The condition on the extension E/F to be simple, in Corollary 7.1.10, is somewhat restrictive, and it will be relaxed (See Proposition 7.4.1 below). However, the next theorem gives us weak conditions sufficient for an extension to be simple.

Theorem 7.2.8 [Primitive Element Theorem] *If E/F is a finite, separable extension, then it is a simple extension, that is, there is $u \in E$ such that $E = F(u)$.*

As immediate consequence of this Theorem together with Chorollary 7.2.2 and Proposition 7.2.6, we get the following corollaries.

Corollary 7.2.9 *Every finite extension in characteristic 0 is simple.*

Corollary 7.2.10 *Every finite extension of a finite field is simple.*

The statement in Corollary 7.2.10 is something we have already proved in Corollary 6.6.10.

04/01/19 Before we prove the Primitive Element Theorem, we prove the following lemma.

Lemma 7.2.11 *Let F be an infinite field, E and extension of F and $\beta, \gamma \in E$, both algebraic over F, and γ separable over F. There is δ such that $F(\beta, \gamma) = F(\delta)$.*

Proof. Let $p(x) = \min_F(\beta)$, and $q(x) = \min_F(\gamma)$. Let K be a spliting field of $p(x) \cdot q(x)$ that contains $F(\beta, \gamma)$. Let $\beta = \beta_1, \ldots, \beta_m$ be the distinct roots of $p(x)$ in K, and $\gamma = \gamma_1, \ldots, \gamma_n$ the distinct roots of $q(x)$ in K. Since γ is separable over F $q(x)$ has no multiple roots, i.e. $q(x) = (x - \gamma_1) \cdots (x - \gamma_n)$. There are finitely many elements $\dfrac{\beta - \beta_i}{\gamma - \gamma_j}$ with $i = 1, \ldots, m$ and $j = 2, \ldots, n$. Since F is infinite, we may choose $a \in F$ different from all those quotients.

$F(\beta,\gamma)$ / $F(\delta)$ / F

Let $\delta = \beta - a\gamma$. Clearly $F(\delta) \leq F(\beta, \gamma)$. We want to show the other inclusion. Consider the tower $F(\beta, \gamma)/F(\delta)/F$. Let $r(x) = \min_{F(\delta)}(\gamma)$. We have $r(x)$ is a factor of $q(x)$, since $q(\gamma) = 0$, so the roots of $r(x)$ are among $\gamma_1, \ldots, \gamma_n$, and include γ_1. Consider now $f(x) = p(\delta + ax) \in F(\delta)[x]$. We have $f(\gamma) = p(\delta + a\gamma) = p(\beta) = 0$, so $r(x)$ is a factor of $f(x)$, and every root of $r(x)$ is a root of $f(x)$. For any $i = 1, \ldots, m$, and $j = 2, \ldots, n$, we have $a(\gamma - \gamma_j) \neq (\beta - \beta_i)$, so $\delta + a\gamma_j = (\beta - a\gamma) + a\gamma_j = \beta - a(\gamma - \gamma_j) \neq \beta - (\beta - \beta_i) = \beta_i$, and therefore, for $j = 2, \ldots, n$, $f(\gamma_j) = p(\delta + a\gamma_j) \neq 0$. So, among all γ_j, the only root of $f(x)$ is $\gamma_1 = \gamma$. and therefore $r(x) = x - \gamma$, which yields $\deg_{F(\delta)}(\gamma) = 1$, and $\gamma \in F(\delta)$. Since $\beta = \delta + a\gamma$, we also get $\beta \in F(\delta)$, completing the proof that $F(\beta, \gamma) \leq F(\delta)$. ∎

E / F / $\mathbb{Z}_p$

Proof of Primitive Element Theorem. We consider two cases, depending on whether F is finite or not.

If F is finite of characteristic p, then E is also finite of characteristic p. By Corollary 6.6.10, E is a simple extension of $\mathbb{Z}_p$, i.e. $E = \mathbb{Z}_p(u)$ for some $u \in E$. It follows that $E = F(u)$.

Now, consider the case when F is infinite. By Proposition 6.4.9, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$, algebraic over F. Use induction on n and Lemma 7.2.11. ∎

7.3 Cyclotomic and Finite Field Extensions

We now explore some additional examples of the automorphism group of an extension.

Example 7.3.1. For $\omega = \text{cis}(2\pi/3)$ we have $\min_{\mathbb{Q}}(\omega) = x^2 + x + 1$, since $\omega^3 = 1$ and $x^3 - 1 = (x-1)(x^2+x+1)$. The roots of $x^2 + x + 1$ are ω and ω^2, both of which are in $\mathbb{Q}(\omega)$, so we have two automorphisms of $\mathbb{Q}(\omega)$, which depend on where they map ω to. There is the identity $I : \omega \mapsto \omega$ and $\tau : \omega \mapsto \omega^2$. Clearly, $\tau^2 : \omega \mapsto \omega^4 = \omega$ is the identity, and $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) = \{I, \tau\}$ is the cyclic group of order 2.

We generalize this example in the following proposition. 04/02/19 Problem Set

Proposition 7.3.1 *Let p be a prime number, and let $\xi_p = \text{cis}(2\pi/p)$. Then $\min_{\mathbb{Q}}(\xi_p) = x^{p-1} + x^{p-2} + \cdots + x + 1$, and $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi_p)) \approx U_p$.*

Proof. ξ_p satisfies $\xi_p^p = 1$, so it is a root of $x^p - 1$. This polynomial factors as

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1), \tag{7.2}$$

and since $\xi_p \neq 1$, it is a root of $\varphi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1$. We want to show that $\varphi_p(x)$ is irreducible over $\mathbb{Q}$. Note that $(x+1)^p - 1 = x \cdot \varphi(x+1)$, and we have

$$\begin{aligned} x \cdot \varphi(x+1) &= (x+1)^p - 1 \\ &= \left(\sum_{i=0}^{p} \binom{p}{i} x^i \right) - 1 \\ &= \sum_{i=1}^{p} \binom{p}{i} x^i \\ &= x \cdot \sum_{i=1}^{p} \binom{p}{i} x^{i-1}, \end{aligned}$$

so, cancelling the common factor x, we get

cyclotimic polynomial

$$\begin{aligned}\varphi_p(x+1) &= \sum_{i=1}^{p}\binom{p}{i}x^{i-1}\\ &= \tbinom{p}{1}+\tbinom{p}{2}x+\cdots+\tbinom{p}{p-1}x^{p-2}+\tbinom{p}{p}x^{p-1}\end{aligned}$$

The leading coefficient is $\binom{p}{p}=1$, and for $i=1,\ldots,p-1$ the binomial coefficient $\binom{p}{i}$ is divisible by p. The constant term, $\binom{p}{1}=p$ is divisible by p, but not by p^2. By Proposition 4.6.2 [Eisenstein Criterion], we get that $\varphi(x+1)$ is irreducible over $\mathbb{Q}$. Since any factorization of $\varphi(x)$ yields a factorization of $\varphi(x+1)$, and viceversa, it follows that $\varphi(x)$ is also irreducible over $\mathbb{Q}$.

04/03/19 Let's consider now the automorphisms of the extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$. The roots of x^p-1 are ξ_p^k for $k=0,\ldots,p-1$. From Equation 7.2 we see that the roots of $\varphi_p(x)$ are ξ_p^k for $k=1,\ldots,p-1$. Each automorphism of $\mathbb{Q}(\xi_p)$ is completely determine from where it maps ξ_p, and it has to map it to one of the roots of $\varphi_p(x)$, i.e. some ξ_p^k for $k=1,\ldots,p-1$. For each such k, let $\sigma_k(\xi_p)=\xi_p^k$. That means $\mathrm{Aut}_{\mathbb{Q}}((\mathbb{Q}(\xi_p)))=\{\sigma_1,\ldots,\sigma_{p-1}\}$. Note that

$$\sigma_k\sigma_j(\xi_p)=\sigma_k(\xi_p^j)=\sigma_k(\xi_p)^j=(\xi_p^k)^j=\xi_p^{kj}=\sigma_{kj}(\xi_p),$$

so, we have $\sigma_k\sigma_j=\sigma_{kj}$, and the map

$$\begin{array}{rccc}\sigma: & U_p & \to & \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi_p))\\ & k & \mapsto & \sigma_k\end{array}$$

is an isomorphism. ■

Definition 7.3.1. For a prime p, the polynomial

$$\varphi_p(x):=x^{p-1}+x^{p-2}+\cdots+x+1$$

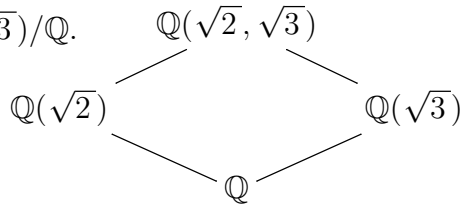
is called the p-th *cyclotimic polynomial*.

There is a generalization of cyclotomic polynomials from $\varphi_p(x)$ when p is a prime, to $\varphi_n(x)$ for any natural number n.

Proposition 7.3.2 *Let p be a prime number, $n \geq 1$, and $E = \mathbb{F}_{p^n}$. The automorphism group $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ is cyclic of order n, generated by the Frobenius automorphism Φ_p.*

Proof. Since E is finite and the Frobenius endomorphism $\Phi_p : E \to E$ is injective and fixes the prime subfield, we have $\Phi_p \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$. The elements of E all satisfy $x^{p^n} = x$, i.e $\Phi_p^n(x) = x$, so $\Phi_p^n = I_E$. Since $E/\mathbb{F}_p$ is a simple extension, for a primitive element $u \in E$ of this extension, n is the smallest integer such that $u^{p^n} = u$, so it is also the smallest integer such that $\Phi_p^n = I_E$, and Φ_p has order n. But Proposition 7.1.9 tells us that $|\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})| \leq [E : \mathbb{F}_p] = n$. Therefore $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ is cyclic of orde n, generated by the Frobenius automorphism Φ_p. ∎

Example 7.3.2. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. The minimal polynomials are $x^2 - 2$ and $x^2 - 3$, with roots $\pm\sqrt{2}$ and $\pm\sqrt{3}$, respectively. For $\sqrt{2}$ there are two choices, and for $\sqrt{3}$ there are also two choices, for a total of 4 potential automorphisms. So we get that $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))| \leq 4$. (Note also, that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$) The potential automorphisms are given by



$$I: \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \sigma_1: \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

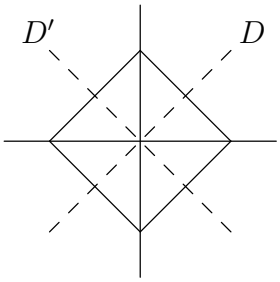
$$\sigma_2: \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \sigma_3: \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

Since $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $x^2 - 3$ over $\mathbb{Q}(\sqrt{2})$. Corollary 6.4.14, tells us that the there are automorphisms doing the above. Moreover, notice that $\sigma_1, \sigma_2, \sigma_3$ have order 2. Therefore, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ is the Klein 4-group.

Example 7.3.3. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ has degree 4, since $\min_{\mathbb{Q}}(\sqrt[4]{2}) = x^4 - 2$ (use Eisenstein' criterion to check irreducibility). However, only two of the four roots, namely $\pm\sqrt[4]{2}$ are in the extension, and therefore $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}))| \leq 2$. Proposition 7.1.5 guarantees the existence of both automorphisms, $(\sqrt[4]{2} \mapsto \sqrt[4]{2})$, and $(\sqrt[4]{2} \mapsto -\sqrt[4]{2})$. Thus, we have $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}))$

is cyclic of order 2.
The splitting field of $x^4 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\sqrt[4]{2}, i)$, which has degree 8 over $\mathbb{Q}$. In this case, there are four choices of where to map $\sqrt[4]{2}$, i.e. $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. There are two choices of where to map i, i.e. $\pm i$, since the minimal polynomial for i over $\mathbb{Q}(\sqrt[4]{2})$ is $x^2 + 1$. Thus, there are a total of 8 potential automorphism of this extension. Therefore, $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))| \leq 8$. As in the previous example, Corollary 6.4.14, guarantees the existence of those 8 automorphisms, so $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))| = 8$. We describe the 8 automorphisms by indicating where they map $\sqrt[4]{2}$ and i.

$\to$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-i\sqrt[4]{2}$
i	i	$-i$	i	$-i$	i	$-i$	i	$-i$
order	1	2	4	2	2	2	4	2



Note that $\sigma_2^2 = \sigma_4$, and $\sigma_2^3 = \sigma_6$. Moreover, $\sigma_2\sigma_3 = \sigma_1$, and $\sigma_3\sigma_2 = \sigma_5$, so the group is not abelian. There are two non-abelian groups of order 8: the dihedral group D_4, and the quaternion group Q_8. Q_8, however, has three elements of order 4, so by elimination we must have $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i)) \approx D_4$. We can do better. The four roots of $x^4 - 2$ form a square on the complex plane, and $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))$ act by symmetries on this square. More precisely, $\sigma_2 = \rho$ is a counterclockwise rotation by $\pi/2$, $\sigma_1 = H$ is a reflection with respect to the real axis, $\sigma_5 = V$ is a reflection with respect to the imaginary axis, $\sigma_3 = D$ is a reflection with respect to one diagonal, and $\sigma_7 = D'$ is a reflection with respect to the other diagonal.

04/05/19
Test 2

7.4 The Fundamental Theorem of Galois Theory

04/08/19 The following proposition generalizes Proposition 7.1.9, by removing the hypothesis of simple extension. The first part is a weaker but useful version.

field of rational functions

Proposition 7.4.1 *1. Let $E = F(\alpha_1, \ldots, \alpha_n)$ be a finite extension of F. Let $r_i = \deg_F(\alpha_i)$.*

$$|\mathrm{Aut}_F(E)| \leq r_1 \cdot r_2 \cdots r_n.$$

2. Let E/F be a finite extension. Then

$$|\mathrm{Aut}_F(E)| \leq [E : F]. \tag{7.3}$$

Proof. (1) By Lemma 7.1.2, any $\sigma \in \mathrm{Aut}_F(E)$ is completely determined by the choice of $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. Let $m_i(x) = \min_F(\alpha_i)$. Proposition 7.1.6 says that $\sigma(\alpha_i)$ is a root of $m_i(x)$, so, there are at most r_i choices for $\sigma(\alpha_i)$.
(2) Choose $\alpha_1, \ldots, \alpha_n \in E$, recursively such that $\alpha_i \notin F(\alpha_1, \ldots, \alpha_{i-1})$. Let $m_i(x) = \min_{F(\alpha_1,\ldots,\alpha_{i-1})}(\alpha_i)$, and $r_i = \deg(m_i)$. We have $[F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})] = \deg_{F(\alpha_1,\ldots,\alpha_{i-1})}(\alpha_i) = r_i$, and the multiplicative property of tower extensions yields

$$[E : F] = r_1 \cdot r_2 \cdots r_n.$$

Let $\sigma \in \mathrm{Aut}_F(E)$, and let σ_i be the restriction of σ to $F(\alpha_1, \ldots, \alpha_i)$. Note that σ_0 is the inclusion mape $\iota_F : F \to E$, and $\sigma_n = \sigma$ Since all $\sigma_i : F(\alpha_1, \ldots, \alpha_i) \to E$ agree with σ, we get that $\sigma_i : F(\alpha_1, \ldots, \alpha_i) \to E$ extends $\sigma_{i-1} : F(\alpha_1, \ldots, \alpha_{i-1}) \to E$. By Corollary 7.1.7 there are at most r_i ways to do this extension. As σ is built from $\sigma_0 = \iota_F$, step by step, we end up with at most $r_1 \cdot r_2 \cdots r_n$ possible $\sigma_n = \sigma \in \mathrm{Aut}_E(F)$. ∎

To see that Proposition 7.4.1.2 is indeed more general than Proposition 7.1.9, we need an example of a finite extension that is not simple. The Primitive Element Theorem (7.2.8) tells us that any finite separable extension is simple, so we need to look at inseparable extensions. Example 7.2.1 gives us an example of a finite inseparable extension. However, that extension is simple. But we can extend the idea of that example, to create the example we need.

Example 7.4.1. Let $R = \mathbb{F}_2[s, t]$ be the ring of polynomials in two variables s and t over $\mathbb{F}_2$. As R is an integral domain (it is, in fact, a UFD) it embeds in its field of quotients, that we denote $\mathbb{F}_2(s, t)$, and call the *field of rational functions* in the two variables s and t. Let $f(x) = x^2 - s, g(x) = x^2 - t \in F[x]$. The same argument used in Example 7.2.1, shows that $f(x)$ and $g(x)$ are

irreducible over F. Let α be a root of $f(x)$ and β a root of $g(x)$. We can write $\alpha = \sqrt{s}$ and $\beta = \sqrt{t}$. $F(\alpha)$ is spanned by $\{1, \alpha\}$ over F, so for any $u \in F(\alpha)$, $u = a + b\alpha$ for some $a, b \in F$. We have $u^2 = a^2 + b^2\alpha^2 = a^2 + b^2 s$, and therefore $\deg_t(u^2)$ is even. Thus, $u^2 \neq t$, and $\beta \notin F(\alpha)$. It follows that $[F(\alpha, \beta) : F(\alpha)] = 2$ and $[F(\alpha, \beta) : F]$=4, with basis $\{1, \alpha, \beta, \alpha\beta\}$. Take $v \in F(\alpha, \beta)$. We can write $v = a + b\alpha + c\beta + d\alpha\beta$, with $a, b, c, d \in F$. It follows that $v^2 = a^2 + b^2\alpha^2 + c^2\beta^2 + d^2\alpha^2\beta^2 = a^2 + b^2 s + c^2 t + d^2 st \in F$. So, we have $\deg_F(v) \leq 2$, and therefore we cannot have $F(\alpha, \beta) = F(v)$. In other words, $F(\alpha, \beta)$ is not a simple extension of F.

04/09/19 **Theorem 7.4.2** *[Dedekind-Artin Theorem] Let E be a field, G a finite subgroup of* $\mathrm{Aut}(E)$*. Let E_G be the subfield of E fixed by G,*

$$E_G = \{u \in E | \sigma(u) = u \text{ for all } \sigma \in G\}.$$

Then E/E_G is a finite extension and $[E : E_G] = |G|$. Moreover, $\mathrm{Aut}_{E_G}(E) = G$.

Proof. Let $F = E_G$. We have $G \leq \mathrm{Aut}_F(E)$, so if E/F is finite, Proposition 7.4.1.2 yields $|G| \leq |\mathrm{Aut}_F(E)| \leq [E : F]$. It remains to show that E/F is indeed finite, and $[E : F] \leq |G|$. Let $n = |G|$. By way of contradiction, assume $[E : F] > n$. There are $u_0, u_1, \ldots, u_n \in E$, distinct, such that $I = \{u_0, u_1, \ldots, u_n\}$ is linearly independent over F. Write $G = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = 1_E$. Consider the $n \times (n+1)$ matrix $M = (\sigma_i(u_j))$, with coefficients in E,

$$M = \begin{bmatrix} u_0 & u_1 & \ldots & u_n \\ \sigma_2(u_0) & \sigma_2(u_1) & \ldots & \sigma_2(u_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(u_0) & \sigma_n(u_1) & \ldots & \sigma_n(u_n) \end{bmatrix}$$

and the system of equations $M \cdot X = 0$.

$$\begin{array}{rcrcccrl} u_0x_0 & + & u_1x_1 & + & \cdots & + & u_nx_n & = 0 \\ \sigma_2(u_0)x_0 & + & \sigma_2(u_1)x_1 & + & \cdots & + & \sigma_2(u_n)x_n & = 0 \\ \vdots & & \vdots & & & & \vdots & \vdots \\ \sigma_n(u_0)x_0 & + & \sigma_n(u_1)x_1 & + & \cdots & + & \sigma_n(u_n)x_n & = 0 \end{array} \tag{7.4}$$

Since there are more variables than equations, the system has a non-trivial solution $\bar{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in E^n$. Pick $\bar{\alpha}$ non-trivial, with the smallest

normal extension

number, $(r+1) > 0$, of non-zero entries. Reorder the elements of I (if needed) so that $\bar{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_r, 0, \ldots, 0)$, and $\alpha_0, \alpha_1, \ldots, \alpha_r \neq 0$. Since the set of solutions of (7.4) is a linear space over E, we may also choose $\bar{\alpha}$, so that $\alpha_0 = 1$. The first of the equations in (7.4) yields

$$u_0\alpha_0 + \cdots + u_r\alpha_r = 0,$$

and by the linear independence of the set I we must have that at least one of $\alpha_0, \ldots, \alpha_r$, say α_k, is not in F. By definition of F, this means that there is $\tau \in G$ such that $\tau(\alpha_k) \neq \alpha_k$. The fact that $\bar{\alpha}$ is a solution of (7.4) means that for each $i = 1 \ldots n$,

$$\sigma_i(u_0)\alpha_0 + \sigma_i(u_1)\alpha_1 + \cdots + \sigma_i(u_r)\alpha_r = 0. \tag{7.5}$$

Let $\beta_j = \tau(\alpha_j)$, and $\gamma_j = \alpha_j - \beta_j$. Note that $\beta_0 = \tau(\alpha_0) = \tau(1) = 1 = \alpha_0$, so $\gamma_0 = 0$. Also, $\gamma_k = \alpha_k - \beta_k = \alpha_k - \tau(\alpha_k) \neq 0$. Let $\sigma_l = \tau\sigma_i$. Applying τ to Equation (7.5) yields

$$\sigma_l(u_0)\beta_0 + \sigma_l(u_1)\beta_1 + \cdots + \sigma_l(u_r)\beta_r = 0, \tag{7.6}$$

As σ_i ranges over G, σ_l also ranges over all of G. So, for each $i = 1, \ldots n$,

$$\sigma_i(u_0)\beta_0 + \sigma_i(u_1)\beta_1 + \cdots + \sigma_i(u_r)\beta_r = 0, \tag{7.7}$$

and subtracting (7.7) from (7.5), we get

$$\sigma_i(u_0)\gamma_0 + \sigma_i(u_1)\gamma_1 + \cdots + \sigma_i(u_r)\gamma_r = 0. \tag{7.8}$$

Since $\gamma_0 = 0$ and $\gamma_k \neq 0$, this is a non-trivial solution to (7.4) with less than $r+1$ non-zero entries, contradicting the choice of $\bar{\alpha}$. ■

7.4.1 Galois Extensions

The property in Theorem 7.4.2 that $[E : E_G] = |G|$ is one several equivalent conditions thatr a finite extension may have. Proposition 7.4.3 below gives us a list of such equivalent properties. Before stating this proposition, we need to define several terms, and introduce some convenient notation.

Definition 7.4.1. A finite extension E/F is said to be a *normal extension*, if E is the splitting field of a polynommial $f(x) \in F[x]$.

fixer subgroup
Galois Connection

Definition 7.4.2. Let E be a field and G a subgroup of $\mathrm{Aut}(E)$. Let

$$F = E_G = \{a \in E | \sigma(a) = a \text{ for all } \sigma \in G\},$$

be the subfield of E fixed by G. We define two maps between $\mathrm{Sub}(G)$, the lattice of subgroups of G, and $\mathrm{Sub}_F(E)$, the lattice of intermediate fields of the extension E/F as follows. The maps go one in each direction, and both maps are denoted by *. The context will tell which is which.

$$\mathrm{Sub}_F(E) \underset{*}{\overset{*}{\rightleftharpoons}} \mathrm{Sub}(G) \tag{7.9}$$

For $L \in \mathrm{Sub}_F(E)$, let

$$L^* = \{\sigma \in G | \sigma(a) = a, \text{ for all } a \in L\}.$$

For $H \in \mathrm{Sub}(G)$, let

$$H^* = E_H = \{a \in E | \sigma(a) = a, \text{ for all } \sigma \in H\}.$$

Note that as defined $F = G^*$. Recall that we showed in Corollary 6.6.4, that E_H, the subfield fixed by H, is indeed a subfield of E. It is obvious that any $\sigma \in H$ fixes the elements of F, so $E_H \in \mathrm{Sub}_F(E)$. Similarly, it is easy to show that L^* is a subgroup of G. It is called the *fixer subgroup* of L. (see Exercise 7.4.1 below)
The pair of posets $(\mathrm{Sub}_F(E), \mathrm{Sub}(G))$, together with the maps just defined, is called a *Galois Connection*, as it satisfies the properties in Lemma 7.4.4 below.

Exercise 7.4.1. Let E be a field, G a subgroup of $\mathrm{Aut}(E)$, $F = E_G$, and $L \in \mathrm{Sub}_F(E)$. Show that $L^* = \mathrm{Aut}_L(E)$, and it is a subgroup of G.

Proposition 7.4.3 *Let E/F be a finite extension, and $G = \mathrm{Aut}_F(E)$. TFAE:*

1. $[E : F] = |G|$
2. *E is the splitting field of a separable polynomial over F.*
3. *E is the splitting field of an irreducible separable polynomial over F.*
4. *The extension E/F is separable and normal.*

Galois extension
Galois group

5. $G^* = F$, *i.e.* $F^{**} = F$

The proof appears below, after some examples, and lemmas.

Definition 7.4.3. Let E/F be a finite extension. We say that E/F is a (finite) *Galois extension* if it satisfies the properties in Proposition 7.4.3. The group $\mathrm{Aut}_F(E)$ is called the *Galois group* of the extension, and is denoted $\mathrm{Gal}_F(E)$.

Examples 7.4.2.

1. In Examples 6.4.2 and 7.1.2.3, we have seen that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$. Hence, it is a Galois extension. It has degree 6, and Galois group isomorphic to D_3. On the other hand, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has degree 3, but $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})$ is trivial, so this extension is not Galois. It follows that $\mathbb{Q}(\sqrt[3]{2})$ cannot be the splitting field of any polynomial over $\mathbb{Q}$.

2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Example 6.4.1 shows that the extension $E/\mathbb{Q}$ is a Galois extension, with Galois group isomorphic to K_4, the Klein 4-group.

3. Let $E = \mathbb{Q}(\sqrt[4]{2})$. Example 7.3.3 shows that $E/\mathbb{Q}$ is **not** a Galois extension, as $[E : \mathbb{Q}] = 4$, but $|\mathrm{Aut}_{\mathbb{Q}}(E)| = 2$.

4. On the other hand, $\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field of $x^4 - 2$ over $\mathbb{Q}$, and this polynomial is separable. Thus, $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is a Galois extension, and therefore $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))$ has order 8, as we have shown in Example 7.3.3.

5. Proposition 7.3.2 shows that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension. Its Galois group is cyclic of order n, generated by the Frobenius automorphism. 04/10/19

6. Proposition 7.3.1 shows that the extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is a Galois extension, with Galois group cyclic of order $p - 1$.

7. The Dedkind-Artin theorem tells us that for G a finite subgroup of $\mathrm{Aut}(E)$, the extension E/E_G is a Galois extension, with Galois group G.

7.4.2 Galois Connection

subgroup lattice
partially ordered set
reflexive
transivite
anti-symmetric
lattice
meet
join
intermediate field lattice
Galois Connection

Recall that given a group G, the *subgroup lattice* of G as the set

$$\mathrm{Sub}(G) := \{H | H \leq G\}$$

of all subgroups of G, ordered by inclusion. This is an example of a *partially ordered set*, poset for short, since the binary relation of inclusion is *reflexive*, *transivite*, and *anti-symmetric*. It is called a *lattice* as it has the following two properties. Given $H_1, H_2 \in \mathrm{Sub}(G)$, there is a greatest lower bound of H_1 and H_2 in $\mathrm{Sub}(G)$, given by $H_1 \cap H_2$, which we call the *meet* of H_1 and H_2. And a least upper bound of H_1 and H_2 in $\mathrm{Sub}(G)$, given by $H_1 \vee H_2$, the *join* of H_1 and H_2, which is the subgroup generated by the union $H_1 \cup H_2$.

$$H_1 \wedge H_2 := H_1 \cap H_2 \qquad H_1 \vee H_2 := \langle H_1 \cup H_2 \rangle.$$

Given a field extension E/F, we define is a similar way, the *intermediate field lattice* of the extension E/F, as the set

$$\mathrm{Sub}_F(E) := \{L | F \leq L \leq E\}$$

of all subfields L of E that contain F. It is ordered by inclusion, and for any $L_1, L_2 \in \mathrm{Sub}_F(E)$, there is a greatest lower bound in $\mathrm{Sub}_F(E)$ given by $L_1 \cap L_2$, and a least upper bound given by $L_1 \vee L_2$, the subfield of E generated by the union $L_1 \cup L_2$.

$$L_1 \wedge L_2 := L_1 \cap L_2 \qquad L_1 \vee L_2 := \langle L_1 \cup L_2 \rangle.$$

The following lemma gives us properties of the maps in (7.9), that justify calling them a *Galois Connection*. In other words, a Galois Connection consists of two posets, and two maps between them, satisfying the following properties.

Lemma 7.4.4 *Let E be a field, G a subgroup of $\mathrm{Aut}(E)$, and $F = E_G$. For any $H, H_1, H_2 \in \mathrm{Sub}(G)$, and any $L, L_1, L_2 \in \mathrm{Sub}_F(E)$*

1. *If $H_1 \leq H_2$, then $H_2^* \leq H_1^*$.* (* is order reversing)
2. *If $L_1 \leq L_2$, then $L_2^* \leq L_1^*$.* (* is order reversing)

3. $H \leq H^{**}$ $(1 \leq {}^{**})$

4. $L \leq L^{**}$ $(1 \leq {}^{**})$

Exercise 7.4.2. Prove Lemma 7.4.4.

Corollary 7.4.5 *Let E be a field, G a subgroup of $\mathrm{Aut}(E)$, and $F = E_G$. For any $H \in \mathrm{Sub}(G)$, and any $L \in \mathrm{Sub}_F(E)$*

1. $H^{***} = H^*$

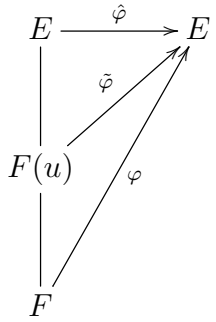
2. $L^{***} = L^*$

Proof. Let $H \in \mathrm{Sub}(G)$. By part 3 of the lemma, we have $H \leq H^{**}$, and applying part 1, we get $H^{***} \leq H^*$. Since $H^* \in \mathrm{Sub}_F(E)$, by part 4 we have $H^* \leq H^{***}$.
A similar argument works for $L \in \mathrm{Sub}_F(E)$. ∎

We often refer to the properties in Corollary 7.4.5 as the "3 = 1" property.

Lemma 7.4.6 *Let E be the splitting field of a separable polynomial $f(x) \in F[x]$. Given $\varphi : F \to E$, such that φ fixes the coefficients of $f(x)$, there are $[E : F]$ different extensions of the homomorphism φ to $\hat{\varphi} : E \to E$.* 04/12/19

Proof. By induction on $n = [E : F]$. The statement is clear when $n = 1$. Let $n > 1$. Let $u \in E - F$ be a root of $f(x)$ and $m(x) = \min_F(u)$. Since $m(x)$ is an irreducible factor of $f(x)$, it is separable, and it splits in E. By Scholium 7.1.8, there are $r = \deg(m(x))$ different extensions of φ to $\tilde{\varphi} : F(u) \to E$ that extend φ. The extension $E/F(u)$ has degree $[E : F(u)] = n/r < n$, and E is the splitting field of the separable polynomial $f(x) \in F(u)[x]$. Moreover, $\tilde{\varphi}$ being an extension of φ, fixes the coefficients of $f(x)$. By induction, there are n/r different extensions of $\tilde{\varphi}$ to $\hat{\varphi} : E \to E$. Therefore, there are $r \cdot (n/r) = n$ different extensions of φ to $\hat{\varphi} : E \to E$. ∎



Proof of Proposition 7.4.3.
Recall that we have E/F a finite extension, and $G = \mathrm{Aut}_F(E) = F^*$.

(1)⇒(5) Assume $[E : F] = |G|$. Note that $F^{**} = G^* = E_G$. Since $F \leq F^{**}$, we may consider the tower $E/E_G/F$, and have

$$[E : F] = [E : E_G][E_G : F].$$

By assumption, $[E : F] = |G|$, and, using the Dedekind–Artin Theorem, $[E : E_G] = |G|$. Therefore $[E_G : F] = 1$, and $E_G = F$, as desired.

(5)⇒(4 and 3) Assume $E_G = F$. We first prove that E/F is separable.
Write $G = \{1, \sigma_2, \ldots, \sigma_n\}$. Let $u \in E$, and consider the elements

$$u, \sigma_2(u), \ldots, \sigma_n(u) \tag{7.10}$$

in E. This list may contain repetitions. Let $u, u_2, \ldots, u_r$ be the distinct elements in (7.10). Consider the polynomial

$$f(x) = (x - u)(x - u_2) \cdots (x - u_r).$$

Each $\tau \in G$ permutes the list (7.10), and therefore it also permutes the elements $u, u_2, \ldots, u_r$, and the factors of $f(x)$. It follows that when we apply τ to $f(x)$, its coefficients are unchanged. In other words, the coefficients of $f(x)$ are in $E_G = F$, and $f(x) \in F[x]$. Since $f(x)$ has no multiple roots, it follows that $\min_F(u)$, which is a factor of $f(x)$, is separable, hence u is separable over F. Moreover, $\min_F(x)$ splits in E. Since $u \in E$ was arbitrary, we have E/F is separable.
Now, by the Primitive Element Theorem, there is $u \in E$ such that $E = F(u)$. Since $\min_F(u)$ splits in E, E is the splitting field of $\min_F(u)$, an irreducible separable polynomial in $F[x]$, hence (3), and E/F is a normal extension, hence (4).

(4)⇒(2) Assume E/F is normal and separable. By normality, let $f(x) \in F[x]$ be such that E is the splitting field of $f(x)$. To see that $f(x)$ is a separable polynomial, let $q(x) \in F[x]$ be any monic irreducible factor of $f(x)$, and let $u \in E$ be a root of $q(x)$. Then $q(x) = \min_F(u)$, and by separability of E/F, u is separable over F, i.e. $q(x)$ is separable over F.

(3)⇒(2) is clear.

(2)⇒(1) Assume E is the splitting field of a separable polynomial $f(x) \in F[x]$, and let $n = [E : F]$. Apply Lemma 7.4.6 to the inclusion map i :