

# Abstract Algebra II

TRISCT

## Contents

<b>1</b>	<b>Some Weird Stuff</b>	<b>2</b>
1.1	Minimal Polynomials over Different Fields . . . . .	2
1.2	Characters . . . . .	2
1.3	Norm and Trace . . . . .	3
1.4	The Sylow Theorems . . . . .	4
<b>2</b>	<b>Basic Types of Field Extensions</b>	<b>5</b>
2.1	Fields . . . . .	5
2.2	Extensions . . . . .	5
2.3	Algebraic Extensions . . . . .	6
2.4	Finite Extensions . . . . .	7
2.5	Transcendental Extensions . . . . .	8
2.6	Algebraic Closure and Embeddings . . . . .	9
2.6.1	Two Very Important Lemmas . . . . .	11
2.7	The Embeddings $\text{Hom}_F(E, \overline{F})$ : An Introduction . . . . .	12
2.8	Normal Extensions and Splitting Fields . . . . .	12
2.9	Separability and Separable Extensions . . . . .	14
2.9.1	Separability of Polynomials . . . . .	14
2.9.2	Separability of Elements and the Separable Degree . . . . .	16
2.9.3	Separable Extensions and Separable Closures . . . . .	20
<b>3</b>	<b>The Primitive Element Theorem</b>	<b>22</b>
<b>4</b>	<b>Galois Theory</b>	<b>24</b>
4.1	Introduction: What Are We Trying to Achieve? . . . . .	24
4.2	Galois Extensions and Galois Groups . . . . .	25
4.3	The Galois Correspondence . . . . .	26
4.4	More on Galois Extensions . . . . .	28

<b>5</b>	<b>More Interesting Extensions</b>	<b>30</b>
5.1	Cyclotomic Extensions . . . . .	30
5.1.1	Over $\mathbb{Q}$ , and the Cyclotomic Polynomials . . . . .	30
5.2	Cyclic Extensions and Abelian Extensions . . . . .	32
5.3	Kummer Extensions . . . . .	32

# 1 Some Weird Stuff

## 1.1 Minimal Polynomials over Different Fields

**Theorem 1.1.** *For algebraic extensions,  $F \subseteq E \subseteq L$ , if  $u \in L$  has minimal polynomials  $P_u^E, P_u^F$  over  $E$  and  $F$  respectively, then*

$$P_u^E \mid P_u^F$$

(Larger fields have smaller polynomials)

**Note 1.1.** Useful for separability.

## 1.2 Characters

Let  $G$  be a monoid and  $E$  a field. A **character of  $G$  (with values) in  $E$**  is a map  $\chi : G \rightarrow E$  that preserves the multiplication and the identity. We say a finite set of characters  $\chi_1, \dots, \chi_k : G \rightarrow E$  is **linearly independent**, if for  $a_i \in E$ ,  $\sum_{i=1}^k a_i \chi_i = 0 \implies a_i = 0$  for all  $i$ . For an infinite collection of characters, we say it is **linearly independent** if every finite subset is linearly independent.

**Note 1.2.** We shall remark for future use that each field is a monoid under multiplication. Each field embedding  $E \hookrightarrow F$  is then a character of  $E$  in  $F$ .

**Theorem 1.2** (Artin, linear independence of characters). *Any set of distinct characters are linearly independent.*

*Proof.* We only have to prove the case with finitely many characters. We prove by induction. Suppose we have  $k$  distinct characters.  $k = 1$  is trivially true. Suppose this  $k \geq 2$  and this holds for  $1, \dots, k-1$ . Let  $\sum_{i=1}^k a_i \chi_i = 0$  with distinct  $\chi_i$ . We may consider only the case  $a_i \neq 0$  for all  $i$ , because if any  $a_i = 0$  then the sum reduces to  $k-1$  terms and we are finished by the induction hypothesis. Then we find some  $h \in G$  such that  $\chi_1(h) \neq \chi_2(h)$  (assuming  $\chi_1(h) \neq 0$ , for at least one of them is) and consider the two sums:

$$\sum_{i=1}^k a_i \chi_1(h) \chi_i = \chi_1(h) \sum_{i=1}^k a_i \chi_i = 0$$

$$\sum_{i=1}^k a_i \chi_i(h) \chi_i = \sum_{i=1}^k a_i \chi_i(h(\cdot)) = 0$$

A subtraction yields

$$\begin{aligned} 0 &= \sum_{i=1}^k a_i \chi_1(h) \chi_i - \sum_{i=1}^k a_i \chi_i(h) \chi_i \\ &= \sum_{i=1}^k a_i (\chi_1(h) - \chi_i(h)) \chi_i \end{aligned}$$

Let  $b_i = a_i(\chi_1(h) - \chi_i(h))$ . Then  $b_1 = 0$ . By the induction hypothesis all  $b_i = 0$ . But  $b_2 = a_2(\chi_1(h) - \chi_2(h)) = 0$  with  $\chi_1(h) \neq \chi_2(h)$ . Hence  $a_2 = 0$ . The case where all  $a_i \neq 0$  is then impossible.  $\square$

### 1.3 Norm and Trace

Let  $E/F$  be a finite extension. We can define the norm and the trace associated with this extension as follows. First we view  $E$  as a finite dimensional over  $F$ . Then we define an  $F$ -linear transformation  $L_u$  on  $E$ , parametrized by elements  $u$  in  $E$ :

$$\begin{aligned} L_u : E &\rightarrow F \\ x &\mapsto ux \end{aligned}$$

The **norm**  $N_{E/F}$  is the map

$$\begin{aligned} N_{E/F} : E &\rightarrow F \\ u &\mapsto \det(L_u) \end{aligned}$$

The **trace**  $T_{E/F}$  is the map

$$\begin{aligned} T_{E/F} : E &\rightarrow F \\ u &\mapsto \text{tr}(L_u) \end{aligned}$$

Without further study, the following are some easy properties.

**Theorem 1.3** (Basic properties). *The following are true for a finite extension  $E/F$ .*

- (i)  $T_{E/F}$  is  $F$ -linear.
- (ii)  $N_{E/F}$  is multiplicative.

- (iii)  $T_{E/F}$  and  $N_{E/F}$  have easy representations for  $u \in F$ , namely,  $u \in F \implies T_{E/F}(u) = nu$ ,  $N_{E/F}(u) = u^n$ , where  $n = [E : F]$ .

**Theorem 1.4** (Break down into steps). *Let  $E/F$  be finite. Then for  $u \in E$ ,*

$$T_{E/F} = T_{F(u)/F} \circ T_{E/F(u)}$$

$$N_{E/F} = N_{F(u)/F} \circ N_{E/F(u)}$$

**Note 1.3.** N.b. the upper step is computed first.

**Theorem 1.5** (Computations). *Let  $E/F$  be finite and  $u \in E$ . We can compute  $T_{E/F}(u)$  and  $N_{E/F}(u)$  using the minimal polynomial of  $u$  and embeddings of  $E$  into  $\overline{F}$ , namely, if*

$$P_u(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

*is the minimal polynomial of  $u$  over  $F$ , then*

- (i)  $T_{E/F}(u) = [E : F(u)](-a_{n-1})$ ;
- (ii)  $N_{F(u)/F}(u) = ((-1)^n a_0)^{[E:F(u)]}$ ;
- (iii)  $T_{E/F}(u) = [E : F]_i \sum_{\sigma \in \text{Hom}_F(E, \overline{F})} \sigma(u)$ ;
- (iii)  $N_{E/F}(u) = \left( \prod_{\sigma \in \text{Hom}_F(E, \overline{F})} \sigma(u) \right)^{[E:F]_i}$ .

## 1.4 The Sylow Theorems

**Theorem 1.6** (Sylow). *Let  $G$  be a finite group of order  $n$ . Suppose  $n = p^k n'$  where  $p$  is prime,  $k \geq 1$  and  $p^{k+1} \nmid n$ . Then the following are true.*

- (i) *There exists a subgroups of order  $p^k$ , called a **Sylow  $p$ -subgroup**.*
- (ii) *Any  $p$ -subgroup of  $G$  is contained in some Sylow  $p$ -subgroup.*
- (iii) *All Sylow  $p$ -subgroups are conjugate.*
- (iv) *The number  $n_p$  of Sylow  $p$ -subgroups satisfies*

$$n_p \equiv 1 \pmod{p}, \quad n_p | n'$$

## 2 Basic Types of Field Extensions

### 2.1 Fields

A **field** is a commutative ring with identity such that  $1 \neq 0$  and any nonzero element is invertible. For any field  $F$ , there is a unique ring homomorphism

$$\begin{aligned}\mathbb{Z} &\rightarrow F \\ n &\mapsto \underbrace{1 + \cdots + 1}_n\end{aligned}$$

The isomorphism theorem tells us that the image of this mapping is isomorphic to  $\mathbb{Z}/p\mathbb{Z}$  for some  $p \in \mathbb{Z}_{\geq 0}$ . Also  $p$  must be either 0 or a prime number since  $\mathbb{Z}/p\mathbb{Z}$ , as a subring of the field  $F$ , should not have any zero-divisors. Hence each field  $F$  corresponds to a unique integer  $p$  that is either 0 or prime. This integer is called the **characteristic** of the field  $F$ . The smallest subfield of  $F$  is called the **prime field** of  $F$ .

A **field homomorphism** is a ring homomorphism between fields. A field homomorphism is necessarily injective, i.e. an embedding.

### 2.2 Extensions

Let  $F \subseteq E$  be fields. Then  $E$  is called an **extension** of  $F$ .<sup>1</sup> The extensions  $E, E'$  of  $F$  are  **$F$ -isomorphic** if there is an  $F$ -isomorphism  $E \rightarrow E'$ . An extension  $E$  of  $F$  is a vector space over  $F$ , the dimension is called the **degree** of the extension, denoted by

$$[E : F] = \dim_F E$$

**Theorem 2.1.** *The degree satisfies the tower property. Let  $F \subseteq E \subseteq L$  be a tower of field extensions. Then*

$$[L : F] = [F : E][E : F]$$

We can define the intersection and compositum of extensions. Let  $F \subseteq L$  be an extension. Suppose  $F \subseteq E \subseteq L$  and  $F \subseteq K \subseteq L$  are subextensions. Then the **intersection** of  $E/F$  and  $K/F$  is simply the intersection of the sets  $E \cap K$ . One can verify this is also a field extension of  $F$ . The **compositum**  $EK$  of  $E/F$  and  $K/F$  is the smallest field extension containing both  $E$  and  $K$ . The following equality is obvious.

---

<sup>1</sup>When talking about extension, there is a tacit understanding that the smaller field is naturally included in the larger one. But when talking about embeddings no such assumption is made.

**Lemma 2.1.** *Suppose  $F \subseteq L$  is an extension and  $S \subseteq L$  is a subset. Let  $F(S)$  be the extension of  $F$  by adjoining all elements in  $S$ , i.e. the smallest subextension of  $L/F$  containing all elements of  $S$ . Then for any  $K/F$  as a subextension of  $L/F$ ,*

$$K(F(S)) = K(S)$$

*Proof.*  $K \subseteq K(S)$ ,  $F(S) \subseteq K(S) \implies K(F(S)) \subseteq K(S)$ . Conversely,  $S \subseteq K(F(S))$ ,  $K \subseteq K(F(S)) \implies K(S) \subseteq K(F(S))$ .  $\square$

## 2.3 Algebraic Extensions

Given an extension  $E/F$ , an element  $u \in E$  is called **algebraic** over  $F$  if  $Q(u) = 0$  for some nonzero polynomial<sup>2</sup>  $Q \in F[x]$ ; otherwise it is called **transcendental**.

**Theorem 2.2.** *An algebraic element  $u \in E$  over  $F$  has a **minimal polynomial** over  $F$ , in the sense that it divides any other polynomial over  $F$  that annihilates  $u$ . This minimal polynomial can be normalized to be monic. It is also the generator of the annihilator of  $u$  (which is an ideal in  $F[x]$ ).*

*Proof.* Either one can do this by selecting the polynomial of the smallest degree, or by considering the kernel of  $F[x] \rightarrow F[u]$ ,  $x \mapsto u$ .  $\square$

We can now talk about what an extension obtained by adjoining a single element looks like. Suppose  $E/F$  is an extension, with  $u \in E$  algebraic over  $F$ . Let  $P_u \in F[x]$  be its minimal polynomial over  $F$ .

**Theorem 2.3.**  $F[u] \cong F[x]/(P_u(x))$ ,  $F[u] = F(u)$  and  $[F(u) : F] = \deg P_u$ .

*First proof.* The first isomorphism comes from the mapping

$$\begin{aligned} F[x] &\rightarrow F[u] \\ P(x) &\mapsto P(u) \end{aligned}$$

and then second equality comes from the fact that

$$F[u] \subseteq F(u), \quad F[u] \cong F[x]/(P_u(x)) \text{ is a field because } P_u \text{ is irreducible.}$$

and  $F(u)$  is the smallest field containing  $u$ .  $\square$

*Second proof.* One can prove that every element in  $F[u] \setminus \{0\}$  is invertible.  $\square$

---

<sup>2</sup>If  $u \in F$ , then this polynomial has degree 1; otherwise it has at least degree 2.

Now some properties of algebraic extensions follow.

**Theorem 2.4** (Closed under a tower). *If a tower  $F \subseteq E \subseteq L$  is algebraic in each step, then the whole tower is algebraic.*

*Proof.* See le devoir W1. □

**Theorem 2.5** (Closed under a base field lift). *If in a tower  $F \subseteq E \subseteq L$ ,  $L/F$  is algebraic, then upper step is algebraic.*

*Proof.* Let  $u \in L$  be algebraic. Then  $u$  is algebraic over  $F$ . A nonzero polynomial over  $F$  that annihilates  $u$  exists. It is also over  $E$ , hence  $u$  is algebraic over  $E$ . □

**Theorem 2.6** (Closed under a compositum). *Algebraic elements after field operations are still algebraic. Consequently, a compositum of algebraic extensions is algebraic. Moreover, given an extension  $E/F$ , all algebraic elements over  $F$  in  $E$  form a subextension.*

*Proof.* Suppose  $\alpha, \beta \in E$  are algebraic over  $F$ . Consider the tower

$$F \subseteq F(\alpha) \subseteq F(\alpha, \beta)$$

which is finite, hence algebraic. □

**Theorem 2.7** (Closed under a lifting). *If  $E/F$  is algebraic and  $K/F$  is arbitrary, then  $EK/K$  is algebraic.*

*Proof.* Every  $u \in E$  is algebraic over  $F$  and hence over  $K$ . Then  $EK/K$  is algebraic. □

## 2.4 Finite Extensions

Finite extensions satisfy the following properties.

**Theorem 2.8** (Closed under a tower). *If  $F \subseteq E \subseteq L$  consists of finite steps, then  $L/F$  is also finite.*

*Proof.* By the tower property of the degree. □

**Theorem 2.9** (Closed under a base field lift). *If in the tower  $F \subseteq E \subseteq L$ ,  $L/F$  is finite, then so is the upper step.*

*Proof.* Clear from the tower property. □

**Theorem 2.10** (Closed under a lifting). *If  $E/F$  is finite and  $K/F$  is arbitrary, then a (finite) basis  $\mathcal{B}$  for  $E/F$  is a linear spanning set for  $EK/K$ . In particular,  $EK/K$  is finite and  $[EK : K] \leq [E : F] < \infty$ .*

$$\begin{array}{ccc} EK & \xrightarrow{\mathcal{B}} & K \\ \downarrow & & \downarrow \\ E & \xrightarrow{\mathcal{B}} & F \end{array}$$

*Proof.* By Lemma 2.1,  $E = F(\mathcal{B}) \implies EK = K(\mathcal{B})$ . By definition  $\mathcal{B}$  is finite. Let  $\mathcal{B} = \{u_1, \dots, u_n\}$ . Then  $EK = K(u_1, \dots, u_n)$ . Each  $u_i$  is algebraic over  $F$  and hence also over  $K$ . Then by breaking down

$$K \subseteq K(u_1, \dots, u_n)$$

into simple steps, with each step finite, we see  $K \subseteq EK = K(u_1, \dots, u_n)$  is also finite.  $\square$

**Theorem 2.11** (Closed under a compositum). *If  $E/F$  and  $K/F$  are finite, then  $EK/F$  is finite. (See also HW-W1-1)*

*Proof.* Consider  $F \subseteq E \subseteq EK$ . We have  $K/F$  finite  $\implies EK/E$  finite. Then use the tower property.  $\square$

## 2.5 Transcendental Extensions

Let  $E/F$  be an extension. Recall that if  $u$  is not annihilated by any nonzero polynomial over  $F$ , then  $u$  is called **transcendental** over  $F$ . In this case we have

**Theorem 2.12.**  $F(u) \cong F[x]$ .

*First proof.* Let

$$\begin{array}{ccc} F[x] & \rightarrow & F[u] \\ x & \mapsto & u \end{array}$$

extend to

$$\begin{array}{ccc} F(x) & \rightarrow & F(u) \\ x & \mapsto & u \end{array}$$

$\square$

*Second proof.* Consider this mapping

$$\begin{array}{ccc} F(x) & \rightarrow & F(u) \\ \frac{Q(x)}{R(x)} & \mapsto & \frac{Q(u)}{R(u)} \end{array}$$

One can prove this is well-defined by showing  $R = 0 \iff R(u) = 0$ . And this is clearly an isomorphism.  $\square$

**Theorem 2.13.** *Full transcendental implies upper step algebraic. Let  $E/F$  be an extension and  $x \in E$  transcendental over  $F$ . Then for any nontrivial subextension  $K : F \subsetneq K \subseteq F(x)$ ,  $x$  is algebraic over  $K$ .*

*Proof.*  $K$  contains at least one nonconstant rational function over  $F$ . One may use this rational function to construct a nontrivial polynomial over  $K$  that  $x$  satisfies.  $\square$

**Theorem 2.14.** *Let  $y = f(x)/g(x)$  be a rational function with relatively prime polynomials  $f, g \in F[x]$ . Let  $n = \max(\deg f, \deg g)$ . Suppose  $n \geq 1$ . Prove that  $[F(x) : F(y)] = n$ .*

*Proof.* See MSEQ-3353809 or my homework answer.  $\square$

## 2.6 Algebraic Closure and Embeddings

The reason why we want an algebraic closure is that we want to have a large enough extensions such that any algebraic extension can be “contained” in it. However, since isomorphic extensions may not be identical as sets, we talk about embeddings rather than inclusions.

A field is called **algebraically closed** if it has no algebraic extension other than itself. The algebraically closed property can be characterized in a few different ways.

**Theorem 2.15** (Equivalent conditions for an algebraically closed field). *The following are equivalent for a field  $E$ .*

- (i)  $E$  is algebraically closed, i.e. has no nontrivial algebraic extensions;
- (ii) Every irreducible polynomial over  $E$  has degree 1;
- (iii) Any nonconstant polynomial over  $E$  factors into linear terms;
- (iv) Any nonconstant polynomial has a root in  $E$ .

**Note 2.1.** It is important to remember that algebraic elements correspond to irreducible polynomials.

*Proof.* (i)  $\implies$  (ii): If not, then we can use this polynomial to get a nontrivial finite extension of  $E$ . Then it is also a nontrivial algebraic extension.  
(ii)  $\implies$  (iii): Any polynomial with degree  $\geq 1$  is reducible. Repeat this argument.  
(iii)  $\implies$  (iv): Every linear term has a root.  
(iv)  $\implies$  (iii): Any polynomial of degree  $\geq 1$  has a linear term. Factor it out.  
(iii)  $\implies$  (ii): Any polynomial of degree  $\geq 2$  is reducible.  
(ii)  $\implies$  (i): For any algebraic element  $u$  over  $E$ , its minimal polynomial is of degree 1, hence  $u \in E$ .  $\square$

An **algebraic closure** of a field  $F$  is an algebraic extension of  $F$  which is algebraically closed. There may be more than one algebraic closure (and in fact, they are  $F$ -isomorphic). We usually fix an algebraic closure and denote it by  $\overline{F}$ . We know the following basic facts about algebraic closures (the lemmas needed are presented in Section 2.6.1 as they are too important).

**Theorem 2.16.** *For any field  $F$  the following are true.*

- (i)  $F$  has an algebraic closure;
- (ii) Fixing an algebraic closure  $\overline{F}$  of  $F$ , any algebraic extension  $E/F$  has an  $F$ -embedding into  $\overline{F}$ .
- (iii) Fixing an algebraic closure  $\overline{F}$  of  $F$ , if  $K/F$  is algebraic and we have an  $F$ -embedding

$$\sigma : K \hookrightarrow \overline{F}$$

then for any further algebraic extension  $E/K$ , there is an extension of  $\sigma$  into  $\overline{F}$ :

$$\tau : E \hookrightarrow \overline{F}$$

- (iv) Any two algebraic closures of  $F$  are  $F$ -isomorphic.

*Proof.* (i): Use Zorn's lemma on the set

$$\{E : E/F \text{ is algebraic}\}, \text{ ordered by set inclusion}$$

and prove that a maximal element leads to an algebraic closure.

(ii): Use Zorn's lemma on the set of pairs

$$\{(K, \sigma) : F \subseteq K \subseteq E, \sigma : K \hookrightarrow \overline{F} \text{ is an } F\text{-embedding}\}$$

ordered by set inclusion and mapping restriction (i.e.  $(K, \sigma) \leq (K', \sigma')$  if  $K \subseteq K'$ ,  $\sigma = \sigma'|_K$ ). And prove that a maximal element is an embedding of  $E$  using Lemma 2.2.

(iii): Use Zorn's lemma similar to above, on the set of all possible extensions of  $\sigma$  and claim that a maximal element leads to an  $F$ -embedding of  $E$ .

(iv): One can embed two different algebraic closures into each other and prove that the composite of the two embeddings is an isomorphism. Lemma 2.3 ensures the second part of the argument.  $\square$

### 2.6.1 Two Very Important Lemmas

**Lemma 2.2.** *Fixing an algebraic closure  $\overline{F}$  of  $F$ , if  $K/F$  is algebraic and has an  $F$ -embedding into  $\overline{F}$ :*

$$\sigma : K \hookrightarrow \overline{F}$$

*then for any  $u$  algebraic over  $K$ , there is an  $F$ -embedding*

$$\tau : K(u) \hookrightarrow \overline{F}$$

*that extends  $\sigma$ .*

*Proof.* For notational simplicity let  $\sigma(P_u) = P_u^\sigma$  and  $\sigma(K) = K^\sigma$ . Let  $P_u$  be the minimal polynomial of  $u$  over  $K$ . Then  $P_u^\sigma \in K^\sigma[x] \subseteq \overline{F}[x]$ . Let  $v$  be any root of  $P_u^\sigma$  in  $\overline{F}$ . Note that

$$P_u \text{ is irreducible in } K[x] \iff P_u^\sigma \text{ is irreducible in } K^\sigma[x]$$

Hence  $P_u^\sigma$  is the minimal polynomial of  $v$  over  $K^\sigma$ . We then have this isomorphism

$$\begin{array}{ccccccc} K(u) & \xrightarrow{\cong} & \frac{K[x]}{P_u(x)} & \xrightarrow{\cong} & \frac{K^\sigma[x]}{P_u^\sigma(x)} & \xrightarrow{\cong} & K^\sigma(v) \subseteq \overline{F} \\ u & \mapsto & \overline{x} & & \overline{x} & \mapsto & v \\ & & \overline{P(x)} & \mapsto & \overline{P^\sigma(x)} & & \end{array}$$

which is also an  $F$ -embedding and extends  $\sigma$ .  $\square$

**Lemma 2.3.** *If  $E/F$  is algebraic, then*

$$\text{Hom}_F(E, E) = \text{Aut}_F(E)$$

*Proof.* “ $\supseteq$ ”: Obvious. “ $\subseteq$ ”: For any  $u \in E$ , let  $P_u$  be its minimal polynomial, and let  $r_u$  be the set of the roots of  $P_u$  in  $E$ . Then

$$\sigma|_{r_u} : r_u \rightarrow r_u$$

is an injection from a finite set to itself. It follows that  $\sigma|_{r_u}$  is surjective as well. Then there is some  $v \in r_u$  for which  $\sigma v = u$ . Since  $u \in E$  is arbitrary,  $\sigma : E \rightarrow E$  is surjective, and thus an  $F$ -automorphism of  $E$ .  $\square$

## 2.7 The Embeddings $\text{Hom}_F(E, \overline{F})$ : An Introduction

After fixing a base field  $F$  and its algebraic closure  $\overline{F}$ , we wish to study the structure of an algebraic extension  $E/F$  by considering the set of its embeddings into  $\overline{F}$ , i.e. we wish to study the set  $\text{Hom}_F(E, \overline{F})$ . There are two questions we can ask:

1. Are they embedded into the same “area” in  $\overline{F}$ ? Are  $\sigma(E)$  the same for all  $\sigma \in \text{Hom}_F(E, \overline{F})$ ?
2. How many elements are there in  $\text{Hom}_F(E, \overline{F})$ ? How many ways can the extension  $E$  be embedded?

The first question leads to the concept of **normal extensions** and **splitting fields**, while the second introduces us to **separability**.

## 2.8 Normal Extensions and Splitting Fields

An extension  $E/F$  is called **normal** if it is algebraic<sup>3</sup> and is such that

$$\sigma_1(E) = \sigma_2(E) \text{ for any } \sigma_1, \sigma_2 \in \text{Hom}_F(E, \overline{F})$$

A polynomial  $P \in F[x]$  is said to **split** over  $F$  if it can be factored into linear terms in  $F$ . A **splitting field**  $E$  for a polynomial  $P \in F[x]$  is an algebraic extension  $E/F$  such that  $P$  splits over  $E$  and  $E$  is precisely generated by the roots of  $P$  in  $E$ . Similarly, a **splitting field for a family of polynomials**  $\{P_i \in F[x]\}$  is an algebraic extension  $E/F$  such that each  $P_i$  splits over  $E$  and  $E$  is precisely generated by all the roots of  $P_i$  in  $E$ .

The following lemma will be useful.

**Lemma 2.4 (Existence of certain embeddings).** *Let  $E/F$  be algebraic. Fix an algebraic closure  $\overline{F}$ . If  $u \in E$  has the minimal polynomial  $P_u \in F[x]$ . Then for any  $v$  that is a root of  $P_u$  in  $\overline{F}$ , there is an  $F$ -embedding  $\sigma : E \hookrightarrow \overline{F}$  with  $\sigma(u) = v$ .*

---

<sup>3</sup>Since we are embedding it into the algebraic closure, it does not make sense to talk about “normal transcendental extensions”.

*Proof.*  $u \mapsto v$  has a unique extension  $F[u] \hookrightarrow \overline{F}$ . Use Theorem 2.16-(iii) to extend it to an  $F$ -embedding  $E \hookrightarrow \overline{F}$ .  $\square$

An normal extension has a few different characterizations.

**Theorem 2.17.** *For  $E/F$  algebraic, the following are equivalent.*

- (i)  $E/F$  is normal, i.e.  $\sigma(E)$  is the same for all  $\sigma \in \text{Hom}_F(E, \overline{F})$ ;
- (ii) If  $P \in F[x]$  is irreducible and has a root in  $E$ , then  $P$  splits over  $E$ ;
- (iii)  $E$  is a the splitting field of some family  $\{P_i \in F[x]\}$ .

**Note 2.2.** Some intuition behind (ii): Note that  $P$  splits over  $E$  if and only if  $P$  splits over  $\sigma(E)$ . If  $P$  does not split over  $\sigma(E)$ , then  $\sigma(E)$  does not contain some roots of  $P$  in  $\overline{F}$ . And by Lemma 2.4, we have an embedding  $\tau$  that maps the root of  $P$  in  $E$  (existence is assured by assumption) to the root of  $P$  in  $\overline{F} \setminus \sigma(E)$ , in which case  $\tau(E) \neq \sigma(E)$ . Conversely, for any  $u \in E$ , its minimal polynomial splits. And we can restrict an embedding to the set of its roots to observe its behavior.

*Proof.* (i)  $\iff$  (ii): See Note 2.2.

(ii)  $\implies$  (iii): One can simply prove the claim that  $E$  is the splitting field for  $\{P_u : u \in E\}$ . Note that each  $P_u$  ( $u \in E$ ) splits in  $E$  by (ii), and  $E$  is generated by the roots of all  $P_u$ . Hence  $E$  is the splitting field for  $\{P_u\}$ .

(iii)  $\implies$  (i): Let  $S_E$  be the set of all the roots of the polynomials  $\{P_i\}$  in  $E$ , and let  $S_{\overline{F}}$  be the set of all the roots of the polynomials  $\{P_i\}$  in  $\overline{F}$ . Then  $E = F(S_E)$ . For any  $\sigma \in \text{Hom}_F(E, \overline{F})$ , we have

$$\sigma(E) = \sigma(F(S_E)) = F(\sigma(S_E))$$

Note that  $\sigma(S_E) \subseteq S_{\overline{F}}$ . Conversely, since every  $P_i$  splits over  $E$ , we can prove  $\sigma(S_E) = S_{\overline{F}}$ . It follows that

$$\sigma(E) = F(\sigma(S_E)) = F(S_{\overline{F}})$$

where the right hand side does not depend on  $\sigma$ .  $\square$

**Corollary 2.1.** *Any two splitting fields for the same family are  $F$ -isomorphic.*

*Proof.* Notice that  $E \cong \sigma(E) = F(S_{\overline{F}})$  in the above proof, whereas  $(S_{\overline{F}})$  depends only on the family  $\{P_i\}$ .  $\square$

Now we explore some properties of normal extensions.

**Theorem 2.18** (Closed under a base field lift). *If  $F \subseteq E \subseteq L$  is such that  $L/F$  is normal, then  $L/E$  is normal.*

*Proof.* Let  $L$  be the splitting field of  $\{P_u \in F[x] : u \in L\}$ . Note that  $P_u \in F[x] \subseteq E[x]$ . Then  $L/E$  is a splitting field and hence normal.  $\square$

**Theorem 2.19** (Closed under a lifting). *If  $E/F$  is normal and  $K/F$  is arbitrary, then  $EK/K$  is normal.*

*Proof.* Let  $E$  be the splitting field for a family of polynomials  $\mathcal{F}$  over  $F$ . Let  $R$  be all the roots of the polynomials in  $\mathcal{F}$ . Then  $E = F(R)$  and  $EK = K(F(R)) = K(R)$ , which is a splitting field for  $\mathcal{F}$  (viewing  $\mathcal{F}$  as a family of polynomials over  $K$ ).  $\square$

**Theorem 2.20** (Closed under an arbitrary compositum or intersection).

*Proof.* **Omitted. See Roman.**  $\square$

## 2.9 Separability and Separable Extensions

Let  $E/F$  be an extension and fix an algebraic closure  $\overline{F}$ . We want to study now how many embeddings there are from  $E$  into  $\overline{F}$ , i.e. the cardinality of  $\text{Hom}_F(E, \overline{F})$ . In the special case where  $E = F(u)$  for some  $u$  algebraic over  $F$ , each embedding corresponds to a root of  $P_u$  in  $\overline{F}$ . And different roots determines different embeddings. Hence the **separable degree** of  $E/F$  is defined as the number of distinct embedding of  $E$  into  $\overline{F}$ , i.e.  $|\text{Hom}_F(E, \overline{F})|$ , or the number of distinct roots of  $P_u$ . In general, the **separable degree** of  $E/F$  is defined as

$$[E : F]_s = |\text{Hom}_F(E, \overline{F})|$$

This does not depend on the choice of  $\overline{F}$  because algebraical closures of the same field are  $F$ -isomorphic.

### 2.9.1 Separability of Polynomials

A polynomial  $P \in F[x]$  is called **separable** if it has no multiple root in  $\overline{F}$ . Otherwise it is called **inseparable**. We may use the **formal derivative** of a polynomial to determine whether the polynomial is separable.

**Theorem 2.21.** *The following are true.*

- (i) *For a polynomial  $P \in F[x]$ ,  $u \in \overline{F}$  is a multiple root of  $P \iff P'(u) = 0$ ;*
- (ii) *For a polynomial  $P \in F[x]$ ,  $P$  is separable  $\iff (P, P') = 1$ ;*
- (iii) *For an irreducible polynomial  $P \in F[x]$ ,  $P$  is separable  $\iff P' \neq 0$ .*

As one can imagine, an inseparable polynomial should have a very special form.

**Theorem 2.22.** *If a monic irreducible polynomial  $P(x) \in F[x]$  is inseparable, then the following are true.*

(i) *(On the field)  $\text{char } F = p > 0$  is a prime number;*

(ii) *(On the form on  $P$ )  $P$  has the form*

$$P(x) = Q(x^{p^r})$$

*for some monic, irreducible and separable  $Q(x) \in F[x]$ . The degree formula is*

$$\deg P = p^r \cdot \deg Q$$

(iii) *(On the factorization) Since  $Q$  is separable, let  $w_i$   $i = 1, \dots, m$  be its distinct roots in  $\overline{F}$ , where  $m = \deg Q = \frac{\deg P}{p^r}$ , and we write*

$$Q(x) = \prod_{i=1}^m (x - w_i)$$

*Then  $P$  has the following factorization over  $F(w_1, \dots, w_m)$ :*

$$P(x) = \prod_{i=1}^m (x^{p^r} - w_i)$$

*and the following factorization in its splitting field*

$$P(x) = \prod_{i=1}^m (x^{p^r} - u_i^{p^r}) = \prod_{i=1}^m (x - u_i)^{p^r}$$

*where  $u_i = w_i$  is the unique  $p^r$ -th root of  $w_i$  in  $\overline{F}$ .*

(iv) *(On the roots of  $P$ ) If  $u$  is a root of  $P$ , then  $u^{p^r} = w_i$  for precisely one  $w_i$ , i.e.  $u$  is a  $p^r$ -th root of  $w_i$ . Conversely, each  $w_i$  has exactly one  $p^r$ -th root  $u_i$ . In particular,  $P$  has  $\deg Q$  distinct roots, each of which has multiplicity  $p^r$ .*

*Proof.* (i) and (ii): Let  $P(x)$  be

$$P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \quad (n \geq 1)$$

Since  $P$  is inseparable, from Theorem 2.21

$$P'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1 = 0$$

Each term must be zero. Particularly,  $n = 0 \in F \implies \text{char } F = p > 0$  is a prime number and  $p \mid n$ . We write  $n = m_1 p$ . For other terms  $ka_k x^{k-1}$  ( $1 \leq k \leq n-1$ ). If  $p \nmid k$ , then  $a_k = 0$  in the first place, and  $P$  has the form

$$P(x) = x^{m_1 p} + a_{(m_1-1)p} x^{(m_1-1)p} + \cdots + a_p x^p + a_0$$

Write

$$Q_1(x) = x^{m_1} + a_{(m_1-1)p} x^{m_1-1} + \cdots + a_p x + a_0$$

Then

$$P(x) = Q_1(x^p)$$

If  $Q_1$  is not yet separable, we can repeat this procedure on  $Q_1$  and find  $Q_2$  such that

$$Q_1(x) = Q_2(x^p)$$

Keep this up we shall end up with some  $Q_r$  that is separable and  $Q_{r-1}(x) = Q_r(x^p)$  because from  $Q_k$  to  $Q_{k+1}$ , the degree decreases by a factor of  $p$ , and hence the process cannot go on forever.  $P$  can be rewritten as

$$P(x) = Q_1(x^p) = Q_2((x^p)^p) = Q_2(x^{p^2}) = \cdots = Q_r(x^{p^r})$$

$Q_r$  must be irreducible because  $P$  is.

(iii), (iv): These are clear from (ii). □

Through an inseparable polynomial we can study its roots: the inseparable elements. But this discussion is moved to the next paragraph.

## 2.9.2 Separability of Elements and the Separable Degree

In an extension  $E/F$ , an element  $u \in E$  is **separable over**  $F$  if it is algebraic and its minimal polynomial  $P_u$  over  $F$  is separable. The **separable degree**<sup>4</sup> of  $E/F$  is

$$[E : F]_s = |\text{Hom}_F(E, \overline{F})|$$

An extension  $E/F$  is called a **separable extension** if every  $u \in E$  is separable over  $F$ .

Now we want to see what happens if there is an inseparable element. Let  $E/F$  be an extension and  $u \in E$  inseparable over  $F$ . From the last paragraph we know  $\text{char } F = p > 0$  must be a prime number, and that  $P_u$  must have the form  $P_u(x) = Q_u(x^{p^r})$  for some separable  $Q$ . Now we are going to study the inseparable element  $u$  through its minimal polynomial.

---

<sup>4</sup>When talking about the separable degree, we always assume the extension is algebraic because we need to embed it into an algebraic closure.

**Theorem 2.23.** *The following are true when  $u \in E$  is inseparable over  $F$  as above. Let  $p, P_u, Q_u$  be as above.*

- (i)  *$w$  has the minimal polynomial  $Q_u$  over  $F$ , and hence is separable over  $F$ ;*
- (ii)  $[F(u) : F] = \deg P_u$ ,  $[F(w) : F] = \deg Q_u$ ,  $[F(u) : F(w)] = \frac{\deg P_u}{\deg Q_u} = p^r$ ;
- (iii)  *$u$  has the minimal polynomial  $x^{p^r} - w$  over  $F(w)$ , and is the unique root of  $x^{p^r} - w$  having multiplicity  $p^r$ ;*
- (iv)  $[F(u) : F]_s = \deg Q_u = \frac{\deg P_u}{p^r}$ ;
- (v)  $[F(u) : F]_s \mid [F(u) : F]$ . More precisely,  $[F(u) : F]_s \cdot p^r = [F(u) : F]$ .

*Proof.* (i) Note that  $P_u(u) = Q_u(u^{p^r}) = Q_u(w) = 0$  and  $Q_u$  is irreducible, hence  $Q_u$  is the minimal of  $w$  over  $F$ .  $w$  is separable because  $Q_u$  is.

(ii) Obvious.

(iii) From (ii)  $u$  over  $F(w)$  has degree  $p^r$ , and  $x^{p^r} - w$  has exactly degree  $p^r$ , hence is the minimal polynomial of  $u$ . Note that  $\text{char } F = p \implies$

$$x^{p^r} - w = x^{p^r} - u^{p^r} = (x - u)^{p^r}$$

(iv)  $[F(u) : F]_s = |\text{Hom}_F(F(u), \overline{F})|$  by definition. The latter equals the number of distinct roots of  $P_u$ , which is  $\deg Q_u = \frac{\deg P_u}{p^r}$ .

(v)  $[F(u) : F]_s = \deg Q_u$ ,  $[F(u) : F] = \deg P_u$ . The dividing relation then comes from  $P_u(x) = Q_u(x^{p^r})$ .

□

The separable degree has a few properties. We can use them to determine how far an extension is from being separable.

**Theorem 2.24.** *The following are true.*

(i) **(Tower property of the separable degree)** *If  $F \subseteq E \subseteq L$  are algebraic extensions of fields, then*

$$[L : F]_s = [L : E]_s [E : F]_s$$

(ii) *If  $E/F$  is finite, then*

$$[E : F]_s \mid [E : F]$$

(iii) If  $E/F$  is finite, then

$$E/F \text{ is separable} \iff [E : F]_s = [E : F]$$

(iv) If  $u$  is separable over  $F$ , then  $F(u)/F$  is separable.

*Proof.* (i) By Theorem 2.16-(iii), for any given  $\sigma \in \text{Hom}_F(E, \overline{F})$ , we can find  $\tau \in \text{Hom}_F(\overline{E}, \overline{F})$  that extends  $\sigma$ , i.e. the following diagram commutes:

$$\begin{array}{ccc} \overline{E} & & \\ \uparrow \iota & \searrow \tau & \\ E & \xrightarrow{\sigma} & \overline{F} \end{array}$$

But note that  $F \subseteq E \subseteq \overline{E} \implies \overline{E}$  is also an algebraic closure of  $F \implies \exists \tau' \in \text{Hom}_F(\overline{F}, \overline{E})$  that is an  $F$ -isomorphism. Since  $\tau\tau' : \overline{F} \rightarrow \overline{F}$  must be an  $F$ -isomorphism,  $\tau = (\tau\tau')(\tau')^{-1}$  must also be an  $F$ -isomorphism. For each given  $\sigma \in \text{Hom}_F(E, \overline{F})$ , we denote by  $\text{Hom}_\sigma(L, \overline{F})$  the embeddings that extend  $\sigma$ . We claim this is a bijection

$$\begin{aligned} \text{Hom}_E(L, \overline{E}) &\rightarrow \text{Hom}_\sigma(L, \overline{F}) \\ \eta &\mapsto \tau \circ \eta \end{aligned}$$

First note that  $\tau \circ \eta$  is indeed in  $\text{Hom}_\sigma(L, \overline{F})$ :

$$(\tau \circ \eta)|_E = \tau \circ \eta|_E = \tau \circ \text{id}_E = \tau|_E = \sigma$$

Then we can prove that this is indeed has an inverse:

$$\begin{aligned} \text{Hom}_\sigma(L, \overline{F}) &\rightarrow \text{Hom}_E(L, \overline{E}) \\ \eta' &\mapsto \tau^{-1} \circ \eta' \end{aligned}$$

Clearly we only need to prove  $\tau^{-1} \circ \eta' \in \text{Hom}_E(L, \overline{E})$ :

$$(\tau^{-1} \circ \eta')|_E = \tau^{-1} \circ \eta'|_E = \tau^{-1} \circ \sigma = \iota$$

where  $\iota : E \hookrightarrow \overline{E}$  is the inclusion map (see the commutative diagram above). Hence for any  $\sigma \in \text{Hom}_F(E, \overline{F})$ ,

$$|\text{Hom}_\sigma(L, \overline{F})| = |\text{Hom}_E(L, \overline{E})|$$

Now we come back to  $\text{Hom}_F(L, \overline{F})$ , note that each  $\xi \in \text{Hom}_F(L, \overline{F})$  restricted to  $E$  is

$$\xi|_E \in \text{Hom}_F(E, \overline{F}) \implies \xi|_E \in \text{Hom}_{\xi|_E}(L, \overline{F})$$

This means we can write

$$\mathrm{Hom}_F(L, \overline{F}) = \bigcup_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \mathrm{Hom}_\sigma(L, \overline{F})$$

Cardinality-wise we obtain from this relation:

$$\begin{aligned} |\mathrm{Hom}_F(L, \overline{F})| &= \left| \bigcup_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \mathrm{Hom}_\sigma(L, \overline{F}) \right| \\ &= \left| \bigcup_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \mathrm{Hom}_E(L, \overline{E}) \right| \\ &= |\mathrm{Hom}_F(E, \overline{F})| |\mathrm{Hom}_E(L, \overline{E})| \end{aligned}$$

which is exactly

$$[L : F]_s = [L : E]_s [E : F]_s$$

(ii) Since  $E/F$  is finite, we write

$$E = F(u_1, \dots, u_n)$$

Applying Theorem 2.23-(v) and the tower property to  $[E : F]$  and  $[E : F]_s$  respectively gives the result.

(iii) If  $E/F$  is separable, then each step in (ii) is separable, and we may use Theorem 2.23-(v) and the tower property. Conversely if  $[E : F]_s = [E : F]$ , then suppose by contradiction there is an inseparable  $u \in E$  over  $F$ . By the tower property

$$[E : F] = [E : F]_s = [E : F(u)]_s [F(u) : F]_s$$

And  $u$  is inseparable  $\implies [F(u) : F]_s < [F(u) : F] \implies$

$$\begin{aligned} [E : F] &= [E : F(u)]_s [F(u) : F]_s \leq [E : F(u)] [F(u) : F]_s \\ &< [E : F(u)] [F(u) : F] = [E : F] \end{aligned}$$

The contradiction finishes the proof.

(iv) This follows from (iii). □

### 2.9.3 Separable Extensions and Separable Closures

Recall that a **separable extension** is an extension in which all elements are separable over the base field. Similar to algebraic closures, we would like to find the "largest" separable extension possible, in the sense that any separable extension can be embedded into it. This leads to the concepts of a separable closure. We shall eventually prove all the separable elements from an algebraic closure form a separable closure. But first, some definitions are in order.

A field  $E$  is called **separably closed** if any separable element over  $E$  must be in  $E$ . An extension  $E/F$  is called **separable closure** of  $F$  if  $E$  is algebraic and separable over  $F$ , and is itself separably closed. A separable closure of  $F$  is often denoted by  $F^{\text{sep}}$ .

There is an equivalent condition for separable closedness .

**Theorem 2.25.** *The following are equivalent.*

- (i)  $E$  is separably closed;
- (ii) Any irreducible separable polynomial over  $E$  has degree 1.

*Proof.* (i)  $\implies$  (ii): Otherwise there is a separable extension.

(ii)  $\implies$  (i): Obvious. □

The following lemma makes sense of a maximal separable subextension and will be useful in proving the existence of a separable closure.

**Lemma 2.5.** *Separable elements are closed under field arithmetics. More precisely, let  $E/F$  be an algebraic extension and denote by  $E_s$  all the elements in  $E$  that are separable over  $F$ . Then  $E_s$  is a field.*

*Proof.* Given  $u, v$  separable over  $F$ , the tower  $F \subseteq F(u) \subseteq F(u, v)$  has separable steps. Hence  $F(u, v)/F$  is separable. □

Now we exhibit some properties of separable closures.

**Theorem 2.26.** *The following are true about separable closures. Let  $F$  be a field.*

- (i) *There exists a separable closure for any  $F$ . Specifically,  $(\overline{F})_s$  (all the separable elements in  $\overline{F}$ ) is a separable closure;*
- (ii) *Separable closures of  $F$  are all  $F$ -isomorphic;*
- (iii) *If we fix a separable closure  $F^{\text{sep}}$ , then any separable extension of  $F$  can be embedded into  $F^{\text{sep}}$ ;*
- (iv)  *$F^{\text{sep}}/F$  is normal;*

*Proof.* (i) Use Lemma 2.5.

(ii) Q.

(iii) Q.

(iv) If  $\text{char } F = 0$ , then  $F^{\text{sep}} = \overline{F}$ . Hence  $F^{\text{sep}}/F = \overline{F}/F$  is normal because every polynomial splits. If  $\text{char } F = p > 0$ , then we take any irreducible polynomial  $P$  over  $F$ . If  $P$  has a root in  $\overline{F}$  that is inseparable, say  $u$ , then  $P$  is the minimal polynomial of  $u$  over  $F$ . And  $P$  is therefore inseparable. It follows that any other root of  $P$  is inseparable over  $F$ , hence  $P$  has no root in  $F^{\text{sep}}$ . This is equivalent to if  $P$  has a root in  $F^{\text{sep}}$  then all roots of  $P$  are in  $F^{\text{sep}}$ , whence  $F^{\text{sep}}/F$  is normal.  $\square$

We finish our topic on separable extensions by presenting some properties.

**Theorem 2.27** (Closed under a compositum). *If  $E/F$  and  $K/F$  are separable extensions, then  $EK/F$  is separable.*

*Proof.* By Lemma 2.5.  $\square$

**Theorem 2.28** (Closed under a base field lift). *If in the tower  $F \subseteq E \subseteq L$ ,  $L/F$  is separable, then so is the upper step.*

*Proof.* Let  $u \in L$ , and  $P_u^E$  (resp.  $P_u^F$ ) the minimal polynomial of  $u$  over  $E$  (resp.  $F$ ). Then  $P_u^F \in E[x]$  as well. Hence  $P_u^E \mid P_u^F$ . Note that  $P_u^F$  is separable, hence  $P_u^E$  is also separable.  $\square$

**Theorem 2.29** (Closed under a tower). *If  $L/E$  and  $E/F$  are separable extensions, then  $L/F$  is separable.*

*Proof.* Let  $u \in L$ , and  $P_u$  the minimal polynomial of  $u$  over  $E$ . Suppose  $a_1, \dots, a_n \in E$  are the coefficients of  $P_u^E$ . We see that  $P_u \in F(a_1, \dots, a_n)[x]$  and is also irreducible and separable. Hence  $u$  is separable over  $F(a_1, \dots, a_n)$ . Now we restrict our attention to the tower

$$F \subseteq F(a_1) \subseteq \dots \subseteq F(a_1, \dots, a_n) \subseteq F(a_1, \dots, a_n, u)$$

Each step is finite (because  $a_i, u$  are algebraic over  $F$ ) and separable. Hence for  $i = 1, \dots, n+1$  ( $a_{n+1} = u$ ),

$$\begin{aligned} [F(a_1, \dots, a_{i-1}, a_i) : F(a_1, \dots, a_{i-1})]_s &= [F(a_1, \dots, a_{i-1}, a_i) : F(a_1, \dots, a_{i-1})] \\ \implies [F(a_1, \dots, a_n, u) : F]_s &= [F(a_1, \dots, a_n, u) : F] \end{aligned}$$

Hence  $F(a_1, \dots, a_n, u)/F$  is separable and in particular  $u$  is separable.  $\square$

**Theorem 2.30** (Closed under a lifting). *If  $E/F$  is separable and  $K/F$  is arbitrary, then  $EK/K$  is separable.*

*Proof.* Each  $u \in E$  is separable over  $F$  by assumption. Note that the minimal polynomial over  $K$  is a factor of the minimal polynomial over  $F$ , and is hence also separable. Therefore  $u$  is separable over  $K$ . And apparently all elements in  $K$  are separable over  $K$ . By Lemma 2.5, the field  $EK$  obtained by field operations is also separable over  $K$ .  $\square$

### 3 The Primitive Element Theorem

Our goal is to find for a finite<sup>5</sup> extension  $E/F$  an element  $u \in E$  such that  $E = F(u)$ . The following factors may determine whether a primitive element exists.

- Number of intermediate fields between  $F \subseteq E$ .
- Separability of  $E/F$ .
- Whether  $F$  is infinite.

We first give a necessary condition for a primitive element.

**Lemma 3.1** (Necessary condition for a primitive element). *If an algebraic extension  $E/F$  has a primitive element  $u$ , then it has finitely many intermediate fields.*

*Proof.* We shall prove this by mapping the intermediate fields (injectively) into a set of polynomials and claim that the latter is a finite set. Let  $P_u^K \in K[x]$  be the minimal polynomial of  $u$  over  $K$  for some  $K : F \subseteq K \subseteq L$ . Then we have a map

$$\begin{aligned} \{K : F \subseteq K \subseteq L\} &\rightarrow E[x] \\ K &\mapsto P_u^K \end{aligned}$$

In particular we have

$$P_u^K \mid P_u^F$$

for all intermediate fields  $K$ . Then we can rewrite the map as

$$\begin{aligned} \{K : F \subseteq K \subseteq L\} &\rightarrow \{Q \in E[x] : Q \mid P_u^F\} \\ K &\mapsto P_u^K \end{aligned}$$

---

<sup>5</sup>If  $E/F$  is infinite and there is some  $u \in E$  for which  $E = F(u)$ , then  $u$  must be transcendental, which is not of our primary concern. Hence we restrict our attention to the finite case here.

The target domain is clearly finite. It remains to prove injectiveness of this map. For every fixed intermediate field  $K$ , let  $K_0$  be the field generated by all the coefficients of  $P_u^K$ , hence  $P_u^K \in K_0[x]$  and is irreducible  $\implies P_u^K$  is the minimal polynomial of  $u$  over  $K_0 \implies [E : K_0] = \deg P_u^K$ . On the other hand, by the original definition of  $P_u^K$  we have  $[E : K] = \deg P_u^K$ . Clearly there is a tower  $K_0 \subseteq K \subseteq E$ . The degree relation then implies  $K_0 = K$ . This means  $K$  is uniquely determined by its corresponding polynomial  $P_u^K$ . Hence the map is injective,  $\square$

It turns out this is also the sufficient condition for a finite extension (Q: Can this be weakened to algebraic?) to have a primitive element.

**Theorem 3.1.** *For a finite extension  $E/F$ , having a primitive element is equivalent to having finitely many intermediate fields.*

*Proof.* “ $\implies$ ”: By Lemma 3.1.

“ $\impliedby$ ”: This involves two cases.

- If  $F$  is a finite field then so is  $E$ , and hence  $E^\times$  is cyclic. The cyclic generator of  $E^\times$  is also a generator of  $E/F$ .
- If  $F$  is an infinite field then so is  $E$ , which gives us plenty of elements to choose from. We first prove the case  $E = F(u_1, u_2)$  for  $u_1, u_2$  algebraic over  $F$ . Consider the extensions

$$F(u_1 + cu_2) \quad c \in F$$

Since  $F$  is infinite (and we can surely assume  $u_2 \neq 0$ ), this gives us infinitely many intermediate fields. But by assumption at least two of them (with different  $c \in F$ ) are equal, i.e.

$$F(u_1 + c_1 u_2) = F(u_1 + c_2 u_2) \text{ for some } c_1 \neq c_2 \in F$$

Hence the field above contains  $(c_1 - c_2)u_2$  and hence  $u_2$ , and hence  $u_1$ , meaning

$$F(u_1, u_2) = F(u_1 + c_1 u_2)$$

For the general finite case, note that every finite extension is finitely generated by algebraic elements. Hence we can apply this result with induction.  $\square$

**Note 3.1.** To remember this proof, just remember that a primitive element should be taken in the form of a linear combination of known generators.

Still, intermediate fields do not work very nicely in practice, except for finite extensions of finite fields. For infinite fields we have another sufficient condition.

**Theorem 3.2.** *If  $F$  is infinite, and  $E/F$  is finite and separable, then  $E = F(u)$  for some  $u \in E$ .*

*Proof.* We still start with  $E = F(u_1, u_2)$  and aim to find a primitive element of the form  $u_1 + cu_2$ . But we shall conclude the existence of a primitive element with the help of embeddings. The key is to realize that **how large a field is can be described by how many different embeddings it has**, so that  $F(u_1 + cu_2)$ , as a subextension of  $F(u_1, u_2)$ , if it has the same number of embeddings as  $F(u_1, u_2)$ , then it must be equal to  $F(u_1 + cu_2)$ , except for a purely inseparable step, which does not exist since the whole step is separable. Also, every embedding of  $F(u_1 + cu_2)$  is a restriction of an embedding of  $F(u_1, u_2)$ . So we want to make the restriction of  $\text{Hom}_F(F(u_1, u_2), \overline{F})$  to  $F(u_1 + cu_2)$  as “diverse” as possible (actually, we want different embeddings to have different restrictions, since we are trying to find  $F(u_1 + cu_2) = F(u_1, u_2)$ ). What happens if  $\sigma_i \neq \sigma_j \in \text{Hom}_F(F(u_1, u_2), \overline{F})$  restricts to the same embedding on  $F(u_1 + cu_2)$ ? Since an embedding of  $F(u_1 + cu_2)$  is completely determined by its action on  $u_1 + cu_2$ , we would have

$$\sigma_i(u_1 + cu_2) = \sigma_j(u_1 + cu_2) \iff \sigma_i(u_1) + c\sigma_i(u_2) = \sigma_j(u_1) + c\sigma_j(u_2)$$

For this not to happen for any  $\sigma_i \neq \sigma_j$ , we need find a  $x = c \in F$  for which

$$\prod_{i \neq j} (\sigma_i(u_1 - u_2) + x\sigma_j(u_1 - u_2))$$

is not zero. The expression above is a nonzero polynomial in  $x$ . It can only have finitely many roots in  $F$ . Since  $F$  is infinite we choose any  $c \in F$  that is not a root to obtain a subextension  $F(u_1 + cu_2)$  for which

$$\begin{aligned} |\text{Hom}_F(F(u_1 + cu_2), \overline{F})| &\geq |\text{Hom}_F(F(u_1, u_2), \overline{F})| \\ \implies [F(u_1 + cu_2) : F]_s &\geq [F(u_1, u_2) : F]_s \end{aligned}$$

It is actually equality, implying  $F(u_1, u_2)/F(u_1 + cu_2)$  is purely inseparable, but it is separable by Theorem 2.28, and hence  $F(u_1, u_2) = F(u_1 + cu_2)$ . Use this with induction we can prove the general case when  $E/F$  is finite and separable.  $\square$

## 4 Galois Theory

### 4.1 Introduction: What Are We Trying to Achieve?

The central idea around Galois theory is that we are studying intermediate fields of an algebraic extension using its group of automorphisms. More precisely, let

$E/F$  be an extension. We consider the following maps<sup>6</sup>

$$\begin{aligned} \{K : F \subseteq K \subseteq L\} &\leftrightarrow \{H : H < \text{Aut}_F(E)\} \\ K &\mapsto \text{Aut}_K(E) \\ E^H &\leftrightarrow H \end{aligned}$$

where  $\text{Aut}_K(E)$  is the **group of  $K$ -automorphisms** of  $E$ , and  $E^H$  is the subset consisting of  $x \in E$  such that  $\forall \sigma \in H, \sigma x = x$ . Clearly  $F \subseteq E^H$ , for each  $\sigma \in H$  preserves  $F$ . Also,  $E^H$  is closed under field operations and is hence a field. We call  $E^H$  the **fixed field** of  $H$ .

## 4.2 Galois Extensions and Galois Groups

A field extension is called **Galois** if it is normal and separable<sup>7</sup>.

**Theorem 4.1** (Galois group). *If  $E/F$  is Galois, then the following hold.*

$$\text{Hom}_F(E, \overline{F}) \cong \text{Hom}_F(E, \sigma(E)) \cong \text{Hom}_F(E, E) = \text{Aut}_F(E)$$

where  $\sigma$  is any member of  $\text{Hom}_F(E, \overline{F})$ .

*Proof.* The first isomorphism is due to  $E/F$  being normal. The second holds by a composite with  $\sigma$ . The third holds for any algebraic extension.  $\square$

**Note 4.1.** The separable assumption is not reflected here, but one should be noted that the separable assumption makes  $\text{Aut}_F(E)$  as “large” as possible, so that is tells us enough information about the intermediate fields.

If  $E/F$  is Galois, we call its groups of  $F$ -automorphisms the **Galois group** of  $E/F$ , and denote it by  $\text{Gal}(E/F)$ .

It makes more sense to study Galois extensions together with their Galois groups.

**Theorem 4.2** (Order and Degree). *If  $E/F$  is finite Galois, then*

$$|\text{Gal}(E/F)| = [E : F]$$

---

<sup>6</sup>We write with the tacit understanding that  $\{K : F \subseteq K \subseteq L\}$  is the set of intermediate fields.

<sup>7</sup>Separable only makes sense for algebraic extensions. So the notion of a Galois extension should be discussed within the scope of algebraic extensions. Although, I am not sure whether there are generalizations to transcendental extensions.

*Proof.*

$$|\mathrm{Gal}(E/F)| = |\mathrm{Hom}_F(E, \overline{F})| = [E : F]_s = [E : F]$$

The three equalities comes respectively from  $E/F$  being normal (and Theorem 4.1), the definition of the separable degree and  $E/F$  being finite separable.  $\square$

We introduce some result regarding intermediate fields of a Galois extension.

**Theorem 4.3** (Closed under a base field lift). *If in a tower  $F \subseteq E \subseteq L$ ,  $L/F$  is Galois, then  $L/E$  is also Galois.*

*Proof.*  $L$  is a splitting field for some polynomials over  $F$  and hence over  $E$ .  $L/F$  is then normal. Also  $L/E$  is separable because  $L/F$  is.  $\square$

**Theorem 4.4** (Conjugation of a Galois group). *Let  $F \subseteq E \subseteq L$  be such that  $L/F$  is Galois. Then by Theorem 4.3,  $L/E$  is also Galois, hence it makes sense to talk about  $\mathrm{Gal}(L/E)$ . For any  $\sigma \in \mathrm{Gal}(L/F)$ , we have<sup>8</sup>*

$$\sigma \mathrm{Gal}(L/E) \sigma^{-1} = \mathrm{Gal}(L/\sigma(E))$$

*Proof.* Direct computation.  $\square$

**Theorem 4.5** (Conditions for lower step Galois<sup>9</sup>). *Let  $E/F$  be Galois. Then for any intermediate field  $K$ ,*

$$K/F \text{ is Galois} \iff \sigma(K) = K, \forall \sigma \in \mathrm{Gal}(E/F) \iff \mathrm{Gal}(E/K) \triangleleft \mathrm{Gal}(E/F)$$

### 4.3 The Galois Correspondence

**Lemma 4.1** (Fixed field). *Let  $E/F$  be Galois, then  $E^{\mathrm{Gal}(E/F)} = F$ .*

*Proof.* Clearly  $F \subseteq E^{\mathrm{Gal}(E/F)}$ . For the converse, we prove that if  $u \in E$ ,  $u \notin F$ , then there exists  $\sigma \in \mathrm{Gal}(E/F)$  such that  $\sigma u \neq u$ . Now let  $u \in E \setminus F$ . Since  $u \notin F$ , its minimal polynomial  $P_u$  over  $F$  has degree  $\geq 2$ , and hence has at least two roots. Since  $u$  is separable, these roots are distinct. Let  $v$  be any root other than  $u$ . We can extend  $u \mapsto v$  to a homomorphism:

$$\begin{aligned} \sigma : F(u) &\rightarrow \overline{F} \\ u &\mapsto v \end{aligned}$$

---

<sup>8</sup>Note that  $F \subseteq \sigma(E) \subseteq L$  since  $\sigma \in \mathrm{Gal}(L/F)$ .

<sup>9</sup>The tower property holds naturally for many extensions, for example, algebraic extensions, separable extensions and finite extensions, but not for Galois extensions. More precisely, it does not hold for normal extensions. For a subextension of a Galois extension  $L/F$  to be normal, one needs to consider its embeddings, which are certainly restrictions of embeddings (automorphism) of  $L$ .

and extend it to an  $F$ -embedding  $\sigma : E \rightarrow \overline{F}$ . We can use  $\overline{E}$  as  $\overline{F}$ , hence the map is actually  $E \rightarrow \overline{E}$ . Since  $E/F$  is normal, the image of the map is actually  $E$ . Therefore  $\sigma \in \text{Aut}_F(E) = \text{Gal}(E/F)$ .  $\square$

**Lemma 4.2** (Artin, automorphism group). *Let  $E$  be a field and let  $\text{Aut}(E)$  be the group of its automorphisms. Then for any finite subgroup  $H < \text{Aut}(E)$ ,  $E/E^H$  is Galois and*

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

*This implies further that  $E/E^H$  is finite and has a primitive element.*

*Proof.* For any  $u \in E$ , consider its orbit under  $H$ :  $O = \{\sigma(u) : \sigma \in H\}$  which is finite and  $|O| \leq |H|$ . Let<sup>10</sup>  $P_u(x) = \prod_{\alpha \in O} (x - \alpha) \in E[x]$ . Note that for all  $\tau \in H$ ,  $\tau O = O$ , hence  $\tau(P_u) = P_u$ . This means  $P_u \in E^H[x]$ . Hence any  $u \in E$  is separable over  $E^H$  and its minimal polynomial  $P_u$  satisfies  $\deg P_u = |O_{u,H}| = |H|$ . And clearly,  $E$  is the splitting field for the family  $\{P_u \in E^H[x] : u \in E\}$ . Hence  $E/E^H$  is a Galois extension. It remains to show  $H = \text{Gal}(E/E^H)$ . Clearly  $H \subseteq \text{Gal}(E/E^H)$  by the definition of  $E^H$ . And by Theorem 4.2,

$$|H| \leq |\text{Gal}(E/E^H)| = [E : E^H]$$

On the other hand we wish to prove  $[E : E^H] \leq |H|$ . Since  $[E^H(u) : E^H] \leq |H|$  for any  $u \in E$ , we can choose some  $u$  with  $[E^H(u) : E^H]$  maximal. Then  $E^H(u) = E$ , otherwise a further extension  $E^H(u, v)/E^H(u)$  with  $v \notin E^H(u)$  is also finite and separable, and therefore has a primitive element  $w$ . Then  $E^H(w) \supsetneq E^H(u)$  has a larger degree over  $E^H$ . Hence

$$[E : E^H] = [E^H(u) : E^H] \leq |H|$$

It follows that  $H = \text{Gal}(E/F)$  and  $[E : E^H] = |H| < \infty$ . Also the  $u$  obtained above is a primitive element of  $E/E^H$ .  $\square$

The following lemma is inspired by the proof above.

**Lemma 4.3.** *If  $E/F$  is separable and such that for all  $u \in F$ ,  $[F(u) : F]$  is bounded, then  $E/F$  is finite and has the same bound on its degree.*

**Corollary 4.1.** *For a finite extension  $E/F$ , it is Galois  $\iff [E : F] = |\text{Aut}_F(E)|$ .*

---

<sup>10</sup>The reason that we don't write  $P_u(x) = \prod_{\sigma \in H} (x - \sigma u)$  is that this might lead to a root with multiplicity.

*Proof.* (“ $\Rightarrow$ ”): By normality and separability. (“ $\Leftarrow$ ”): Let  $H = \text{Aut}_F(E)$  which is a subgroup of  $\text{Aut}(E)$ . Then prove  $H$  is finite and apply Lemma 4.2 to the tower  $F \subseteq E^H \subseteq E$  to prove  $F = E^H$ . For the finiteness of  $H$  we have

$$|H| = |\text{Aut}_F(E)| \leq |\text{Hom}_F(E, \overline{F})| = [E : F]_s \leq [E : F] < \infty$$

Then by Lemma 4.2, we have  $[E : E^H] = |H| = [E : F]$  (the second equality is by assumption). Hence  $F = E^H$  and  $E/F = E/E^H$  is Galois.  $\square$

Now we can move on to the Galois correspondence.

**Theorem 4.6** (Fundamental theorem of Galois theory, Galois correspondence). *For a finite Galois extension  $E/F$ , the following maps are mutually inverses of each other.*

$$\begin{aligned} \{K : F \subseteq K \subseteq L\} &\leftrightarrow \{H : H < \text{Gal}(E/F)\} \\ K &\mapsto \text{Aut}_K(E) \\ E^H &\leftarrow H \end{aligned}$$

*They give rise to a one-to-one ordering reversing correspondence between the sets  $\{K : F \subseteq K \subseteq L\}$  and  $\{H : H < \text{Gal}(E/F)\}$ , called the **Galois correspondence**.*

*Proof.* First note that by Theorem 4.3  $\text{Aut}_K(E) = \text{Gal}(E/K)$  for any intermediate field  $K$ . Also by Theorem 4.2  $\text{Gal}(E/F)$  is finite. Hence by Lemma 4.1 and Lemma 4.2, we have the composites

$$K \mapsto \text{Gal}(E/K) \mapsto E^{\text{Gal}(E/K)} = K$$

$$H \mapsto E^H \mapsto \text{Gal}(E/E^H) = H$$

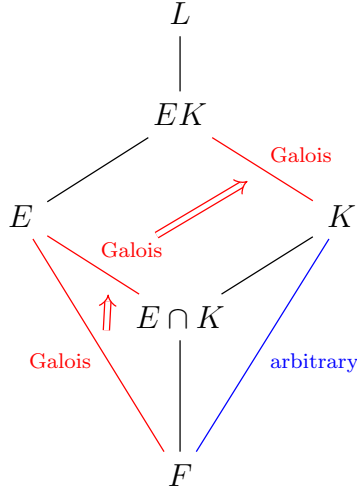
This means  $K \mapsto \text{Gal}(E/K)$  and  $H \mapsto E^H$  are mutual inverses, and each of them therefore must be a bijection. The order-reversing property is evident by definition.  $\square$

## 4.4 More on Galois Extensions

**Theorem 4.7** (Closed under a lifting). *Let  $E/F$  be finite Galois and  $K/F$  arbitrary. Then  $EK/K$  is Galois and we have the isomorphism:*

$$\begin{aligned} \text{Gal}(EK/K) &\xrightarrow{\cong} \text{Gal}(E/E \cap K) \\ \sigma &\mapsto \sigma|_E \end{aligned}$$

An illustration is as follows (assuming all these fields are contained in a larger field  $L$ ):



*Proof.* By Theorem 2.19 and Theorem 2.30,  $EK/K$  is Galois. For the group isomorphism, first note that

$$\begin{aligned} \text{Gal}(EK/K) &\rightarrow \text{Gal}(E/E \cap K) \\ \sigma &\mapsto \sigma|_E \end{aligned}$$

is well-defined, i.e.  $\sigma|_E(E) = E$  and  $\sigma|_{E \cap K} = \text{id}_{E \cap K}$ . The latter is evident since  $\sigma|_K = \text{id}_K$ . This also implies that  $\sigma|_E \in \text{Hom}_F(E, EK)$  (Q: What?). Since  $E/F$  is normal, we have  $\sigma|_E(E) \subseteq E \implies \sigma|_E(E) = E$ . It follows easily that  $\sigma \mapsto \sigma|_E$  is a group homomorphism. For injectiveness, if  $\sigma|_E = \text{id}_E$ , then  $\sigma$  fixes both  $E$  and  $K$  and hence  $EK \implies \sigma = \text{id}_{EK}$ . For surjectiveness, let  $H$  be the image of this group homomorphism. By the finiteness assumption  $[E : F]$  we have  $|H| < |\text{Gal}(E/E \cap K)| = [E : E \cap K] \leq [E : F] < \infty$ . Applying Lemma 4.2 to  $E^H \subseteq E$ , we have

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

We also have  $u \in E^H \subseteq (EK)^{\text{Gal}(EK/K)} = K \implies u \in E \cap K$ . Hence  $E^H \subseteq E \cap K$ , while the reverse inclusion is obvious. Hence  $E^H = E \cap K \implies H = \text{Gal}(E/E^H) = \text{Gal}(E/E \cap K)$ .  $\square$

**Note 4.2.** This holds even when  $[E; F] = \infty$ . The second half part of the proof needs to be modified using the Krull topology and Lemma 4.2 would not be applicable.

## 5 More Interesting Extensions

### 5.1 Cyclotomic Extensions

The need for cyclotomic extensions arises from the attempt to classify all finite Galois extensions over a base field.

#### 5.1.1 Over $\mathbb{Q}$ , and the Cyclotomic Polynomials

If  $w \in \mathbb{C}^\times$  satisfies  $w^n = 1$ , then  $w$  is called a  **$n$ -th root of unity**. The extension  $\mathbb{Q}(w)/\mathbb{Q}$  is called a **cyclotomic extension**. If moreover,  $\text{ord}_{\mathbb{C}^\times}(w) = n$ , then  $w$  is called a **primitive  $n$ -th root of unity**. The set of all  $n$ -th roots of unity is denoted by  $\mu_n$ .

We have the following theorems for the cyclotomic extension  $\mathbb{Q}(w)/\mathbb{Q}$ .

**Theorem 5.1.** *Cyclotomic extensions are Galois.*

*Proof.* Consider  $\mathbb{Q}(w)$  where  $w^n = 1$ . Let  $n = \text{ord}_{\mathbb{C}^\times}(w)$  without loss of generality. Then  $\mathbb{Q}(w)/\mathbb{Q}$  is separable because it is over  $\mathbb{Q}$ , and normal because it is the splitting field of  $x^n - 1 = (x - 1)(x - w) \cdots (x - w^{n-1})$ .<sup>11</sup>  $\square$

**Lemma 5.1.** *Let  $\mu_n$  denote the set of all  $n$ -th roots of unity and let  $w$  be a primitive  $n$ -th root of unity. Then*

$$\text{Gal}(\mathbb{Q}(w)/\mathbb{Q}) \hookrightarrow \text{Aut}(\mu_n)$$

**Note 5.1.** Note that in general we can only say that the Galois group is a subgroup of the symmetric group of the set of the roots of some polynomial. However, in this case, we can further say that it is a subgroup of the automorphism group of the roots of  $x^n - 1$ . This is because  $\mu_n$  has a group structure while in general the set of the roots of some polynomials does not.

*Proof.* We first observe that each  $\sigma \in \text{Gal}(\mathbb{Q}(w)/\mathbb{Q})$  restricted to  $\mu_n$  is a well-defined injective (hence surjective) map, i.e. a permutation on  $\mu_n$ . Moreover,  $\sigma$  preserves multiplication and inverses, hence preserve the group structure of  $\mu_n$ . It follows that each  $\sigma$  restricted to  $\mu_n$  is a group automorphism. Conversely, each  $\sigma$  can be uniquely determined by its action on  $\mu_n$  (actually its action on  $w$  alone would suffice), hence the map is an embedding (clearly a homomorphism):

$$\begin{aligned} \text{Gal}(\mathbb{Q}(w)/\mathbb{Q}) &\rightarrow \text{Aut}(\mu_n) \\ \sigma &\mapsto \sigma|_{\mu_n} \end{aligned}$$

$\square$

---

<sup>11</sup> $w$  must be a primitive  $n$ -th root of unity for this factorization to hold.

Before continuing to give more theorems about cyclotomic extensions, we introduce the cyclotomic polynomials. Let  $\{w_i : 1 \leq i \leq \phi(n)\}$  be all the primitive  $n$ -th roots of unity. The polynomials

$$\Psi_n(x) = \prod_{i=1}^{\phi(n)} (x - w_i)$$

is called the  **$n$ -th cyclotomic polynomial**.

**Theorem 5.2.** *The following are true about the cyclotomic polynomials  $\Psi_n(x)$ .*

- (i)  $\Psi_n(x) \in \mathbb{Q}[x]$ .
- (ii)  $\prod_{d|n} \Psi_d(x) = x^n - 1$ .
- (iii)  $\Psi_n(x) \in \mathbb{Z}[x]$  and are monic.
- (iv)  $\Psi_n$  is irreducible over  $\mathbb{Q}$ . And if  $w$  is a primitive  $n$ -th root of unity, then  $\Psi_n$  is the minimal polynomial of  $w$  over  $\mathbb{Q}$ .

*Proof.* (i) Let  $w$  be a primitive  $n$ -th root of unity. Note that each  $\sigma \in \text{Gal}(\mathbb{Q}(w)/\mathbb{Q})$  restricts to an automorphism of  $\mu_n$ .  $\sigma$  must send generators to generators, and hence primitive roots to primitive roots, this means  $\sigma$  permutes all the primitive roots in  $\mu_n$ . It follows that  $\Psi_n$  is invariant under any  $\sigma \in \text{Gal}(\mathbb{Q}(w)/\mathbb{Q})$ . Hence

$$\Psi_n(x) \in (\mathbb{Q}(w)^{\text{Gal}(\mathbb{Q}(w)/\mathbb{Q})})[x] = \mathbb{Q}[x]$$

(ii) Let  $w$  be an primitive  $n$ -th root of unity. Then

$$x^n - 1 = (x - 1)(x - w) \cdots (x - w^{n-1})$$

Each root is of the form  $w^i$  ( $0 \leq i \leq n-1$ ). Let  $d = \text{ord}(w^i)$ . Then  $d \mid n$  and  $w^i$  is a primitive  $d$ -th root. Hence  $w^i$  is a root of  $\Psi_d$  and hence of  $\prod_{d|n} \Psi_d$ . It follows that every root of  $x^n - 1$  is also one of  $\prod_{d|n} \Psi_d$ . Note that these roots are distinct, hence  $x^n - 1 \mid \prod_{d|n} \Psi_d$ . For the converse, obviously each root of  $\Psi_d$  with  $d \mid n$  is a root of  $x^n - 1$ . Also each  $\Psi_d$  has no multiple roots, and  $\Psi_{d_1}, \Psi_{d_2}$  have no common roots by definition. Hence  $\prod_{d|n} \Psi_d \mid x^n - 1$ . It follows that  $x^n - 1 = \prod_{d|n} \Psi_d(x)$ .

(iii) By induction. Clearly  $\Psi_1(x) = x-1 \in \mathbb{Z}[x]$ . Suppose  $n \geq 2$  and  $\Psi_1, \dots, \Psi_{n-1}$  are in  $\mathbb{Z}[x]$ . Then by

$$\Psi_n = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Psi_d}$$

we know  $\Psi_n$  can be obtained by the Euclidean algorithm, whose result must be in  $\mathbb{Z}[x]$  because  $\Psi_d$  with  $d < n$  are all monic and in  $\mathbb{Z}[x]$ , and also  $x^n - 1$  is monic and in  $\mathbb{Z}[x]$ .

- (iv) Let  $P_w(x) \in \mathbb{Q}[x]$  be the minimal polynomial of  $w$  over  $\mathbb{Q}$ . Since  $\Psi_n(w) = 0$  and  $\Psi_n(x) \in \mathbb{Q}[x]$ ,  $P_w \mid \Psi_n$ . Hence it suffices to prove that  $\Psi_n$  is irreducible to conclude that  $\Psi_n$  is the minimal polynomial of  $w$ . □

**Theorem 5.3.** *Let  $\mu_n$  denote the set of all  $n$ -th roots of unity and let  $w$  be a primitive  $n$ -th root of unity. Then*

$$\text{Gal}(\mathbb{Q}(w)/\mathbb{Q}) \cong \text{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

*Proof.* We have proved that  $\Psi_n$  is irreducible over  $\mathbb{Q}$ . Then  $P_w \mid \Psi_n \implies P_w = \Psi_n$ , so that

$$[\mathbb{Q}(w) : \mathbb{Q}] = \deg \Psi_n = \phi(n) = |\text{Aut}(\mu_n)|$$

This implies  $\text{Gal}(\mathbb{Q}(w)/\mathbb{Q}) \hookrightarrow \text{Aut}(\mu_n)$  must be surjective. □

## 5.2 Cyclic Extensions and Abelian Extensions

A **cyclic extension** is a Galois extension whose Galois group is cyclic. An **abelian extension** is a Galois extension whose Galois group is abelian.

## 5.3 Kummer Extensions

Let  $F$  be a field. If  $w \in \overline{F}^\times$  is such that  $w^n = 1$  then  $w$  is called an  **$n$ -th root of unity**. If moreover,  $\text{ord}_{\overline{F}^\times}(w) = n$ , then  $w$  is a **primitive  $n$ -th root of unity**.

**Note 5.2.** The existence of a primitive  $n$ -th root of unity is not guaranteed for a general field  $F$ . A necessary condition is as follows.

**Lemma 5.2** (Necessary condition for the existence of a primitive root). *If  $F$  has a primitive  $n$ -th root of unity, then  $\text{char } F \nmid n$ .*

**Hint:**  $x^n - 1 = (x^m - 1)^p$  if  $n = pm$ .

We wish to classify all cyclic extensions of degree  $n$  of  $F$  when  $F$  has a primitive  $n$ -th root of unity, and the answer would be of the form  $F(\sqrt[n]{a})$ . And the following questions are to be asked.

- Is  $F(\sqrt[n]{a})/F$  Galois?
- Is  $F(\sqrt[n]{a})/F$  cyclic?

- Does  $[F(\sqrt[n]{a}) : F] = n$ ?

**Lemma 5.3** (The polynomial of an  $n$ -th root). *Let  $F$  be a field. If there is a primitive  $n$ -th root of unity  $w \in F$ , then for any  $a \in F$ ,  $x^n - a$  is separable.*

*Proof.* Let  $\alpha \in \overline{F}$  be any  $n$ -th root of  $a$ . Then  $\alpha, w\alpha, \dots, w^{n-1}\alpha$  are  $n$  distinct roots of  $x^n - a$ . Hence it splits over  $\overline{F}$  as

$$x^n - a = \prod_{i=0}^{n-1} (x - w^i \alpha)$$

□

**Theorem 5.4.** *Let  $F$  be a field. If there is a primitive  $n$ -th root of unity  $w \in F$ , then for any  $a \in F$ , and any  $n$ -th root  $\sqrt[n]{a}$  of  $a$  in  $\overline{F}$ ,  $F(\sqrt[n]{a})/F$  is Galois.*

*Proof.* By Lemma 5.3  $\sqrt[n]{a}$  is separable. Also since  $w \in F$ , we have  $F(\sqrt[n]{a}) = F(\sqrt[n]{a}, w\sqrt[n]{a}, \dots, w^{n-1}\sqrt[n]{a})$ . It follows that it is the splitting field of  $x^n - a$ . □

**Theorem 5.5.** *Let  $F$  be a field with a primitive  $n$ -th root of unity  $w \in F$ . Then for any  $a \in F$  and any of its  $n$ -th root  $\alpha$ ,  $F(\alpha)/F$  is cyclic.*

**Hint:** Embed  $\text{Gal}(F(\alpha)/F)$  into  $\mu_n$  by  $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$ .

*Proof.* Let  $\alpha = \alpha$ . Consider this map ( $\mu_n$  is the group of  $n$ -th roots, namely,  $\mu_n = \{1, w, w^2, \dots, w^{n-1}\}$ ):

$$\begin{aligned} \phi : \text{Gal}(F(\alpha)/F) &\rightarrow \mu_n \\ \sigma &\mapsto \frac{\sigma(\alpha)}{\alpha} \end{aligned}$$

Note that  $\frac{\sigma(\alpha)}{\alpha}$  indeed lies in  $\mu_n$  because  $\sigma$  is a permutation of the set

$$\{\alpha, w\alpha, \dots, w^{n-1}\alpha\}$$

of the roots of  $x^n - a$  (cf. Lemma 5.3). Moreover,  $\sigma$  is uniquely determined by where  $\sigma$  sends  $\alpha$ , and hence uniquely determined by  $\frac{\sigma(\alpha)}{\alpha}$ , i.e.  $\phi$  is injective. Also,  $\phi$  is a group homomorphism: suppose  $\phi(\sigma_1) = w^{i_1}$ ,  $\phi(\sigma_2) = w^{i_2}$ , then

$$\phi(\sigma_1\sigma_2) = \frac{\sigma_1\sigma_2\alpha}{\alpha} = \frac{\sigma_1(w^{i_2}\alpha)}{\alpha} = w^{i_2} \frac{\sigma_1(\alpha)}{\alpha} = w^{i_2} w^{i_1} = \phi(\sigma_1)\phi(\sigma_2)$$

and  $\phi(1) = \frac{\alpha}{\alpha} = 1$ . Hence  $\text{Gal}(F(\alpha)/F)$  is isomorphic to a subgroup of  $\mu_n$ . The latter is abelian and it follows that so is the former. □

Finally we consider when  $[F(\sqrt[n]{a}) : F] = n$ , i.e. when  $x^n - a$  is irreducible. We need some preparations. Let  $\alpha = \sqrt[n]{a}$  as above.

**Lemma 5.4.** *If  $\text{Gal}(F(\alpha)/F)$  has order  $d$ , then  $d \mid n$  and  $\alpha^d = \alpha$ .*

*Proof.* Since  $\text{Gal}(F(\alpha)/F)$  is isomorphic to a cyclic subgroup of  $\mu_n$  by Theorem 5.5, we have  $d \mid n$ . Suppose  $\tau$  is a generator for  $\text{Gal}(F(\alpha)/F)$ . Then  $\frac{\tau\alpha}{\alpha}$  is a generator of some subgroup of order  $d$  of  $\mu_n$ , i.e.  $(\frac{\tau\alpha}{\alpha})^d = 1$ . It suffices to prove  $\tau(\alpha^d) = \alpha^d$ . Indeed,

$$\frac{\tau(\alpha^d)}{\alpha^d} = \frac{(\tau\alpha)^d}{\alpha^d} = \left(\frac{\tau\alpha}{\alpha}\right)^d = 1$$

□

**Theorem 5.6.** *Let  $F$  and  $\alpha = \sqrt[n]{a}$  be as before. The following are equivalent.*

- (i)  $[F(\alpha) : F] = n$ ;
- (ii)  $x^n - a$  is irreducible;
- (iii)  $a$  has no  $m$ -th root in  $F$  for  $m > 1$ ,  $m \mid n$ .
- (iv)  $\alpha^d \notin F$  for  $d \mid n$ ,  $d < n$ .
- (v)  $\text{ord}_{F^\times/(F^\times)^n}(a) = n$ .

*Proof.* (i)  $\iff$  (ii): Obvious.

(ii)  $\implies$  (iii): Suppose  $a$  has an  $m$ -th root  $\beta$  in  $F$  for some  $m > 1$ ,  $m \mid n$ . Then  $a = \beta^m$ . Let  $n = md$ . We have

$$x^n - a = x^{md} - \beta^m = (x^d)^m - \beta^m = (x^d - \beta)((x^d)^{m-1} + (x^d)^{m-2}\beta + \dots + \beta^{m-1})$$

Hence  $x^n - a$  is reducible.

(iii)  $\implies$  (iv): If  $\alpha^d \in F$  for some  $d \mid n$ ,  $d < n$ , then let  $m = n/d$ . We have  $m > 1$ ,  $m \mid n$  and  $\alpha^d \in F$  is an  $m$ -th root of  $a$ .

(iv)  $\implies$  (i): If  $[F(\alpha)/F] = |\text{Gal}(F(\alpha)/F)| = d < n$ , then by Lemma 5.4,  $d \mid n$  and  $\alpha^d \in F$ .

(iv)  $\implies$  (v): Let  $\text{ord}_{F^\times/(F^\times)^n}(a) = d$ . Certainly  $d \mid n$ . If  $d < n$ , then  $\alpha^{dn} = a^d \in (F^\times)^n \implies$  there is  $b \in F^\times$  such that  $\alpha^{dn} = b^n \implies \alpha^d = bw^k$  for some  $k \implies \alpha^d \in F$ . A contradiction.

(v)  $\implies$  (iv): If (iv) does not hold, then there is some  $d \mid n$ ,  $d < n$ , such that  $\alpha^d \in F \implies a^d = \alpha^{dn} = (\alpha^d)^n \in (F^\times)^n \implies \text{ord}_{F^\times/(F^\times)^n}(a) = d < n$ . □

To conclude, we combine all the results into one theorem.

**Theorem 5.7** (Extensions by adding an  $n$ -th root). *Let  $F$  be a field in which there exists a primitive  $n$ -th root. For any  $a \in F$  and any  $n$ -th root  $\alpha$  of  $a$ . The extension  $F(\alpha)/F$  is Galois and cyclic, whose degree  $d$  is a factor of  $n$ , and is equal to  $n$  if and only if  $\alpha^k \notin F$  for all  $k \mid n$ ,  $k < n$ .*

Surprisingly, the converse is also true, i.e. when  $F$  has a primitive  $n$ -th root of unity every finite cyclic extension of degree  $n$  can be obtained by adding an  $n$ -th root of some element.

**Lemma 5.5** (Eigenvector of a root of unity). *Let  $F$  have a primitive root of unity  $w \in F$  and let  $E/F$  be a cyclic extension of degree  $n$ . Suppose  $\text{Gal}(E/F) = \langle \tau \rangle$ . Then there exists  $\alpha \in E^\times$  for which  $\tau\alpha = w\alpha$ .*

*Proof.* Note that  $\tau$  has order  $n$ , hence  $\tau^n = 1$ . We claim  $x^n - 1$  is the minimal polynomial of  $\tau$ . If not, then its minimal polynomial must be of a smaller degree, i.e.

$$P(\tau) = \sum_{k=0}^m a_k \tau^k = 0$$

for  $a_k \in F$  and  $m < n$ . Note that  $1, \tau, \dots, \tau^m$  are distinct characters of  $E$  in  $E$  (maybe they are called “on  $E$ ”?). Hence  $P = 0$  as a polynomial, contradicting  $\deg P = m$ . Now we think of  $\tau$  as an  $F$ -linear transformation on  $E$ . Then its eigenvalues are precisely the roots of  $x^n - 1$ . Since  $w^n = 1$ ,  $w$  is an eigenvalue, which has then an eigenvector  $\alpha \in E$ , i.e.  $\tau\alpha = w\alpha$ .  $\square$

**Theorem 5.8** (Finite cyclic extensions). *Let  $F$  have a primitive root of unity  $w \in F$  and let  $E/F$  be a cyclic extension of degree  $n$ . Then  $E = F(\alpha)$  for some  $\alpha \in E$  with  $\alpha^n \in F$ .*

*Proof.* Let  $\tau$  generate  $\text{Gal}(E/F)$ . By Lemma 5.5, there is some  $\alpha \in E^\times$  with  $\tau\alpha = w\alpha$ . Note that the upper step in the tower

$$F \subseteq F(\alpha) \subseteq E$$

is also Galois. And we have

$$\text{Gal}(E/F(\alpha)) = \{\tau^k : \tau^k \alpha = \alpha\} = \{\tau^k : w^k \alpha = \alpha\} = \{\tau^k : k = 0\} = \{1\}$$

Hence  $E = F(\alpha)$ . Finally,  $\tau(\alpha^n) = w^n \alpha^n = \alpha^n \implies \alpha^n \in F$ .  $\square$

The last part of this section will be dedicated to giving a classification theorem for finite cyclic extension of degree  $n$ . For this purpose we need to think of  $F^\times$  as a multiplication group and also think of

$$(F^\times)^n = \{y^n : y \in F^\times\}$$

as a multiplicative subgroup of  $F^\times$ .

**Lemma 5.6.** *Let  $F$  be a field with a primitive  $n$ -th root of unity  $w \in F$ . If  $a, b \in F^\times$ , then  $F(\sqrt[n]{a}) = F(\sqrt[n]{ab^n})$ . It follows that the map is well-defined:*

$$\begin{aligned} F^\times / (F^\times)^n &\rightarrow \{\text{cyclic extensions}\} \\ a &\mapsto F(\sqrt[n]{a})/F \end{aligned}$$

*Proof.* We see that  $\sqrt[n]{ab^n}$  is a root of  $x^n - ab^n$ , all of whose roots are then  $\sqrt[n]{ab^n}w^i$  ( $0 \leq i \leq n-1$ ). On the other hand,  $\sqrt[n]{ab}$  is also an  $n$ -th root of  $ab^n$ , hence  $\sqrt[n]{ab} = \sqrt[n]{ab^n}w^i$ . Note that  $b, w \in F$ , so that

$$F(\sqrt[n]{ab^n}) = F(\sqrt[n]{ab}w^{-i}) = F(\sqrt[n]{a})$$

□

In view of Lemma 5.6, we may talk about  $F(\sqrt[n]{a})$  while thinking of  $a$  as an element of  $F^\times / (F^\times)^n$  (this subgroup has order  $d \mid n$ ).

**Lemma 5.7.** *If  $a \in F^\times / (F^\times)^n$ , then  $F(\sqrt[n]{\langle a \rangle}) = F(\sqrt[n]{a})$ , where  $\langle a \rangle$  is the subgroup generated by  $a$  in  $F^\times / (F^\times)^n$ .*

*Proof.* Certainly,  $F(\sqrt[n]{a}) \subseteq F(\sqrt[n]{\langle a \rangle})$ . Conversely,

$$F(\sqrt[n]{\langle a \rangle}) = F(\sqrt[n]{a}, \sqrt[n]{a^2}, \dots, \sqrt[n]{a^{n-1}})$$

Note that  $\sqrt[n]{a^k} = (\sqrt[n]{a})^k w^{jk}$ . So that

$$F(\sqrt[n]{\langle a \rangle}) = F(\sqrt[n]{a}, (\sqrt[n]{a})^2, \dots, (\sqrt[n]{a})^{n-1}) \subseteq F(\sqrt[n]{a})$$

□

**Lemma 5.8.** *For a cyclic subgroup  $\Delta = \langle a \rangle$  of  $F^\times / (F^\times)^n$  of order  $n$ , we have the following isomorphism:*

$$\begin{aligned} \Delta &\xrightarrow{\cong} \text{Hom}(\text{Gal}(F(\sqrt[n]{\Delta})/F), \mu_n) \cong \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto \left( \sigma \mapsto \frac{\sigma \sqrt[n]{a}}{\sqrt[n]{a}} \right) \end{aligned}$$

*Proof.* Note that  $\frac{\sigma \sqrt[n]{a}}{\sqrt[n]{a}}$  is independent of which root of  $a$  we chose, hence we may assume  $\sqrt[n]{a^k} = \sqrt[n]{a}^k$ .  $\text{Hom}(\text{Gal}(F(\sqrt[n]{\Delta})/F), \mu_n)$  can be made into a group in the following way:  $\phi_1, \phi_2 \in \text{Hom}(\text{Gal}(F(\sqrt[n]{\Delta})/F), \mu_n)$ , we define  $(\phi_1 \phi_2)(\sigma) = \phi_1(\sigma) \phi_2(\sigma)$  and  $\phi_1^{-1}(\sigma) = (\phi_1(\sigma))^{-1}$ . **Unfinished, not sure what  $\text{Hom}(\text{Gal}(F(\sqrt[n]{\Delta})/F), \mu_n)$  is.** □

**Theorem 5.9** (Classification theorem for cyclic extensions of order  $n$ ). *Let  $F$  be a field with a primitive  $n$ -th root  $w \in F$ . There is a bijection:*

$$\begin{aligned} \{\text{cyclic subgroups of order } n \text{ in } F^\times/(F^\times)^n\} &\rightarrow \{\text{cyclic } E/F \text{ of order } n\} \\ \Delta &\mapsto F(\sqrt[n]{\Delta}) \end{aligned}$$

*Proof. Surjectiveness:* By Theorem 5.8, we can find  $\alpha \in E$  such that  $\alpha^n \in F$  and  $E = F(\alpha)$ . Let  $a = \alpha^n$  (so that  $\alpha = \sqrt[n]{a}$ ), and let  $\Delta$  be the subgroup generated by  $a$  in  $F^\times/(F^\times)^n$ . Then  $E = F(\sqrt[n]{a}) = F(\sqrt[n]{\Delta})$ . It suffices to prove that  $\Delta$  has order  $n$ , i.e.  $a$  has order  $n$  in  $F^\times/(F^\times)^n$ . Suppose not, then  $\text{ord}_{F^\times/(F^\times)^n}(a) = d \mid n$  but  $d < n$ . Hence  $a^d = \alpha^{dn} \in (F^\times)^n$ . We can find some  $b \in F^\times$  such that  $\alpha^{dn} = b^n \implies \alpha^d = bw^k$  for some  $k$ . But  $b, w \in F$ , hence  $\alpha^d \in F$ , contradicting  $[E : F] = n$  by Theorem 5.6.

*Injectiveness:* Let  $\Delta_1, \Delta_2$  be two cyclic subgroups of  $F^\times/(F^\times)^n$  of order  $n$ , and  $F(\sqrt[n]{\Delta_1}) = F(\sqrt[n]{\Delta_2})$ . By Lemma 5.3,

$$\Delta_1 \cong \text{Hom}(\text{Gal}(F(\sqrt[n]{\Delta_1})/F), \mu_n) = \text{Hom}(\text{Gal}(F(\sqrt[n]{\Delta_2})/F), \mu_n) \cong \Delta_2$$

This means for every  $a_1 \in \Delta_1$ , there exists  $a_2 \in \Delta_2$ , such that

$$\begin{aligned} \sigma \mapsto \frac{\sigma \sqrt[n]{a_1}}{\sqrt[n]{a_1}} \text{ and } \sigma \mapsto \frac{\sigma \sqrt[n]{a_2}}{\sqrt[n]{a_2}} \text{ are identical in } \text{Hom}(\text{Gal}(F(\sqrt[n]{\Delta_1})/F), \mu_n) \\ \implies \forall \sigma \in \text{Gal}(F(\sqrt[n]{\Delta_1})/F), \frac{\sigma \sqrt[n]{a_1}}{\sqrt[n]{a_1}} = \frac{\sigma \sqrt[n]{a_2}}{\sqrt[n]{a_2}} \\ \implies \frac{\sqrt[n]{a_1}}{\sqrt[n]{a_2}} \in F \implies \frac{a_1}{a_2} \in (F^\times)^n \implies a_1 = a_2 \text{ in } F^\times/(F^\times)^n \end{aligned}$$

This actually implies  $\Delta_1 \subseteq \Delta_2$ . The converse is true, by symmetry.  $\square$

The **exponent** of a group  $G$  is defined as  $e(G) = \text{lcm}(\text{ord}_G(g) : g \in G)$ . An  **$n$ -Kummer extension** is an abelian extension  $E/F$  where the base field has a primitive  $n$ -th root of unity and  $e(\text{Gal}(E/F)) \mid n$ .

**Theorem 5.10** (Classification theorem for  $n$ -Kummer extensions). *Let  $F$  be a field with a primitive  $n$ -th root of unity. There is a bijection:*

$$\begin{aligned} \{\text{finite subgroups of } F^\times/(F^\times)^n\} &\rightarrow \{\text{finite } n\text{-Kummer extension of } F\} \\ \Delta &\mapsto F(\sqrt[n]{\Delta}) \end{aligned}$$

*Proof. None provided.*  $\square$