

# Field Theory and Galois Theory.

Alec Zabel-Mena

January 16, 2023



# Contents

<b>1</b>	<b>Fields.</b>	<b>5</b>
1.1	Field Extensions. . . . .	5
1.2	Algebraic Extensions. . . . .	9
1.3	Splitting Fields . . . . .	13
1.4	Algebraic Closures. . . . .	16
1.5	Seperability. . . . .	17
1.6	Cyclotomic Polynomials. . . . .	21



# Chapter 1

## Fields.

### 1.1 Field Extensions.

**Definition.** We define the **characteristic** of a field  $F$  to be the smallest positive integer  $p$ , such that  $p \cdot 1 = 0$ , where  $1$  is the identity of  $F$ . We write  $\text{char } F = p$ , and if no such  $p$  exists, then we write  $\text{char } F = 0$ .

**Lemma 1.1.1.** *Let  $F$  be a field, then  $\text{char } F$  is either 0, or a prime integer.*

*Proof.* Let  $\text{char } F = p$ . If  $p = 0$ , then we are done. Now suppose that  $p = mn$ , with  $m, n \in \mathbb{Z}^+$ . Then  $p \cdot 1 = (mn)1 = (n \cdot 1)(m \cdot 1) = mn = 0$ , which makes  $m$  and  $n$  0 divisors. Since  $F$  is a field, and hence an integral domain, this is impossible, and hence  $p$  must be prime. ■

**Corollary.** *If  $\text{char } F = p$ , then for all  $a \in F$ ,  $pa = \underbrace{a + \cdots + a}_{p \text{ times}}$ .*

*Proof.* We have  $pa = p(a \cdot 1) = (p \cdot 1)a$ . ■

**Example 1.1.** (1) Both  $\mathbb{Q}$  and  $\mathbb{R}$  have  $\text{char} = 0$ . Similarly,  $\text{char } \mathbb{Z} = 0$ , even though  $\mathbb{Z}$  is just an integral domain.

(2)  $\text{char } \mathbb{Z}/p\mathbb{Z} = p$  and  $\text{char } \mathbb{Z}/p\mathbb{Z}[x] = p$  for any prime  $p$ .

**Definition.** We define the **prime subfield** of a field  $F$  to be the subfield of  $F$  generated by 1.

**Example 1.2.** (1) The prime subfields of  $\mathbb{Q}$  and  $\mathbb{R}$  is  $\mathbb{Q}$ .

(2) Let  $\mathbb{Z}/p\mathbb{Z}(x)$  the field of rational functions over  $\mathbb{Z}/p\mathbb{Z}$ . Then the prime subfield of  $\mathbb{Z}/p\mathbb{Z}(x)$  is  $\mathbb{Z}/p\mathbb{Z}$ . Similarly, the prime subfield for  $\mathbb{Z}/p\mathbb{Z}[x]$  is also  $\mathbb{Z}/p\mathbb{Z}$ .

**Definition.** If  $K$  is a field containing a field  $F$ , then we call  $K$  **field extension** over  $F$ , and write  $K/F$  (not the quotient field!) or denote it by the diagram

$$\begin{array}{c} K \\ | \\ F \end{array}$$

**Lemma 1.1.2.** *Every field is a field extension of its prime subfield.*

**Lemma 1.1.3.** *Let  $K$  an extension over a field  $F$ . Then  $K$  is a vector space over  $F$ .*

**Definition.** Let  $K/F$  a field extension. We define the **degree** of  $K$  over  $F$ ,  $[K : F]$  to be the dimension of  $K/F$  as a vector space.

**Definition.** Let  $F$  be a field, and  $f \in F[x]$  a polynomial. We call an element  $\alpha \in R$  a **root** (or **zero**) of  $f$  if  $f(\alpha) = 0$ .

**Lemma 1.1.4.** *Let  $\phi : F \rightarrow L$  a field homomorphism. Then either  $\phi = 0$ , or  $\phi$  is 1-1.*

**Lemma 1.1.5.** *Let  $F$  be a field, and  $p \in F[x]$  an irreducible polynomial. Then there exists a field  $K$  containing an embedding of  $F$ , such that  $p$  has a root in  $K$ .*

*Proof.* Consider  $K = F[x]/(p)$ . Since  $p$  is irreducible in a principle ideal domain,  $(p)$  is a maximal ideal, and hence  $K$  is a field. Now consider the canonical map  $\pi : F[x] \rightarrow K$  taking  $f \rightarrow f \bmod (p)$  and let  $\phi = \pi|_F$ . Then  $\phi \neq 0$ , since  $\pi : 1 \rightarrow 1$ . Then  $\phi$  is 1-1. And so  $\phi(F) \simeq F$ .

Now, consider  $F$  as a subfield of  $K$ . Then  $p(x \bmod (p)) \equiv p(x) \bmod (p) \equiv 0 \bmod (p)$ , so that  $x \bmod (p)$  is a root of  $p$  in  $K$ . ■

**Corollary.** *There exists a field extension of  $F$  containing a root of  $p$ .*

**Theorem 1.1.6.** *Let  $F$  be a field, and let  $p \in F[x]$  an irreducible polynomial of degree  $n$ , and let  $K = F[x]/(p)$ , and  $\theta = x \bmod (p)$ . Then  $\{1, \theta, \dots, \theta^{n-1}\}$  forms a basis for  $K$  as a vector space over  $F$  and  $[K : F] = n$ .*

*Proof.* Let  $a \in F[x]$ , since  $F[x]$  is Euclidean domain, there exist  $q, r \in F[x]$ ,  $q \neq 0$  for which

$$a(x) = q(x)p(x) + r(x) \text{ where } \deg r < n$$

Now, since  $pq \in (p)$ ,  $a(x) \equiv r(x) \bmod (p)$ , and every element of  $K$  is a polynomial of degree less than  $n$ . Then the elements  $\{1, \theta, \dots, \theta^{n-1}\}$  span  $K$ .

Now, suppose that there are  $b_0, \dots, b_{n-1} \in F$  not all 0 for which

$$b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} = 0$$

Then

$$b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} \equiv 0 \bmod (p)$$

so that  $p|(b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1})$  in  $F$ . But  $\deg p = n$  and  $p$  divides a polynomial of degree  $n - 1$ , which is a contradiction. Therefore we are left with  $b_0 = \dots = b_{n-1} = 0$ . ■

**Corollary.**  $K = \{\alpha_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} : a_i \in F \text{ for all } 1 \leq i \leq n - 1\}$

**Corollary.** *If  $a(\theta), b(\theta) \in K$ , are elements of degree less than  $n$ , and the operations of polynomial addition, and polynomial multiplication mod  $(p)$  are defined, then  $K$  forms a field.*

**Example 1.3.** (1) Consider the polynomial  $x^2 + 1$  over  $\mathbb{R}$ . Then one has the field

$$\mathbb{C} = \mathbb{R}[x] / (x^2 + 1)$$

an extension of  $\mathbb{R}$  of degree  $[\mathbb{C} : \mathbb{R}] = 2$ . Let  $i$  be a root of  $x^2 + 1$  in this field, then  $i^2 = -1$ , and the elements of  $\mathbb{C}$  are of the form  $a + ib$  where  $a, b \in \mathbb{R}$ . Then we have described the field of complex numbers, and the addition and multiplication (mod  $x^2 + 1$ ) of these elements are the addition and multiplication of complex numbers.

One might also construct  $\mathbb{C}$  differently by defining the isomorphism

$$\mathbb{R}[x] / (x^2 + 1) \rightarrow \mathbb{C} \text{ taking } a + xb \rightarrow a + ib$$

(2) Consider again  $x^2 + 1$  over  $\mathbb{Q}$ . Then we get the field

$$\mathbb{Q}(i) = \mathbb{Q}[x] / (x^2 + 1)$$

of degree  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ , and where  $i$  is a root of  $x^2 + 1$ , so that  $i^2 = -1$ . Then the elements of  $\mathbb{Q}(i)$  are of the form  $a + ib$  where  $a, b \in \mathbb{Q}$ , i.e. it is isomorphic to the set of all complex numbers with rational components.

(2) Consider  $x^2 - 2$  over  $\mathbb{Q}$ . by Eisenstein's criterion for  $p = 2$ ,  $x^2 - 2$  is irreducible over  $\mathbb{Q}$ . Let  $\alpha$  a root of  $x^2 - 2$ , so that  $\alpha^2 = 2$ . Then we have the field

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x] / (x^2 - 2)$$

of degree  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , and whose elements are of the form  $a + b\sqrt{2}$ . One can define an isomorphism between  $\mathbb{Q}(i)$  and  $\mathbb{Q}(\sqrt{2})$  by taking  $\sqrt{2} \rightarrow i$ .

(3) The polynomial  $x^3 - 2$  over  $\mathbb{Q}$  gives us the field

$$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x] / (x^3 - 2)$$

of degree  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$  over  $\mathbb{Q}$ . Here the elements are of the form  $a + b\xi + c\xi^2$  where  $\xi^3 = 2$ .

(4) Denote  $\mathbb{F}_2$  to be a finite field of 2 elements. Consider the polynomial  $x^2 + x + 1$  over  $\mathbb{F}_2$  which is irreducible. Then the field

$$\mathbb{F}_2(\alpha) = \mathbb{F}_2[x] / (x^2 + x + 1)$$

is a field of degree 2 over  $\mathbb{F}_2$ , whose elements are of the form  $a + b\alpha$ , where  $\alpha^2 = \alpha + 1$ . In fact, one can generate this field using the fact that  $\alpha^2 = \alpha + 1$ .

(5) Let  $F = K(t)$  the field of rational functions in  $t$  over a field  $K$ . Let  $p(x) = x^2 - t \in F[x]$ , then by Eisenstien's criterion with the ideal  $(t)$ ,  $p$  is irreducible over  $F[x]$ . Let  $\theta$  be a root for  $p$ , that is  $\theta = \sqrt{t}$ , then we get the field  $K(t, \sqrt{t})$  of degree  $[K(t, \sqrt{t}) : K] = 2$ , whose elements are of the form  $a(t) + b(t)\sqrt{t}$ .

**Lemma 1.1.7.** *Let  $F$  be a subfield of a field  $K$ , and let  $\alpha \in K$ . Then there exists a unique minimal subfield of  $K$  containing  $F$  and  $\alpha$ ; more precisely, it is the intersection of all subfields of  $K$  containing  $F$  and  $\alpha$ .*

**Definition.** Let  $K$  be any extension of a field  $F$ , and let  $\alpha, \beta, \dots \in K$ . Then we define the subfield **generated** by  $\alpha, \beta, \dots$  over  $F$  to be the unique minimal subfield containing all  $\alpha, \beta, \dots$  and  $F$  and we denote it  $F(\alpha, \beta, \dots)$ . Moreover, we call  $K$  a **simple extension** of  $F$  if  $K = F(\alpha, \beta, \dots)$ . If  $K = (F\alpha_1, \dots, \alpha_n)$  for  $\alpha_1, \dots, \alpha_n \in K$ , then it is a **finitely generated** simple extension.

**Theorem 1.1.8.** *Let  $F$  be a field, and  $p \in F[x]$  irreducible, and let  $K$  an extension of  $F$  containing a root  $\alpha$  of  $p$ . Then*

$$F(\alpha) \simeq F[x]_{(p)}$$

*Proof.* Consider the homomorphism  $F[x] \rightarrow F(\alpha)$  taking  $a(x) \rightarrow a(\alpha)$ . Since  $p(\alpha) = 0$ ,  $p$  is in the kernel of this homomorphism, and we get an induced homomorphism from  $F[x]_{(p)} \rightarrow F(\alpha)$ . Now, since  $p$  is irreducible,  $F[x]_{(p)}$  is a field, and since the homomorphism takes  $1 \rightarrow 1$ , it is 1–1. Then by the first isomorphism theorem for ring homomorphisms these two fields are isomorphic. ■

**Corollary.** *If  $\deg p = n$ , then  $F(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_i \in F \text{ for all } 1 \leq i \leq n-1\}$  and  $[F(\alpha) : F] = n$ .*

**Example 1.4.** (1) The polynomial  $x^2 - 2$  over  $\mathbb{Q}$  also has the root  $-\sqrt{2}$  in  $\mathbb{R}$ , so that  $\mathbb{Q}(-\sqrt{2})$  is of degree 2 over  $\mathbb{Q}$  with elements of the form  $a - b\sqrt{2}$ . Notice however that  $\mathbb{Q}(-\sqrt{2}) \simeq \mathbb{Q}(\sqrt{2})$  by taking  $a - b\sqrt{2} \rightarrow a + b\sqrt{2}$ .

(2) The polynomial  $x^3 - 2$  only has the solution  $\xi = \sqrt[3]{2}$  in  $\mathbb{R}$ . However, in  $\mathbb{Q}$  it has the solutions given by

$$\sqrt[3]{2} \left( \frac{-1 \pm i\sqrt{3}}{2} \right)$$

So that the subfields generated by either of these three elements (over  $\mathbb{C}$ ) are isomorphic.

**Theorem 1.1.9.** *Let  $\phi : F \rightarrow L$  a field isomorphism and  $p \in F[x]$ ,  $q \in L[x]$  irreducible polynomials, where  $q$  is obtained by applying  $\phi$  to the coefficients of  $p$ . Let  $\alpha$  a root of  $p$ , and  $\beta$  a root of  $q$ . Then there exists an isomorphism  $F(\alpha) \rightarrow L(\beta)$  taking  $\alpha \rightarrow \beta$  and extending  $\phi$ . That is, we have the following diagram*

$$\begin{array}{ccc} F(\alpha) & \longrightarrow & L(\beta) \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & L \end{array}$$



*Proof.* Notice that  $\phi$  induces a ring homomorphism between  $F[x]$  and  $L[x]$ , so that  $(p)$  is maximal. Since  $q$  is obtained from  $p$ ,  $(q)$  is also maximal, so that  $F[x]_{(p)}$  and  $L[x]_{(q)}$  are fields. Then we have an isomorphism

$$F[x]_{(p)} \simeq L[x]_{(q)}$$

Then, if  $\alpha$  is a root of  $p$ , and  $\beta$  a root of  $q$ , we obtain the isomorphism

$$F(\alpha) \simeq L(\beta)$$

moreover, this isomorphism takes  $\alpha \rightarrow \beta$ . ■

## 1.2 Algebraic Extensions.

**Definition.** Let  $K/F$  be a field extension. We say that an element  $\alpha \in K$  is **algebraic** over  $F$ , provided there exists a polynomial over  $F$  having  $\alpha$  as a root. Otherwise we call  $\alpha$  **transcendental**. If every  $\alpha \in K$  is algebraic, we call  $K$  **algebraic** and  $K/F$  an **algebraic extension**.

**Lemma 1.2.1.** *Let  $\alpha$  be algebraic over a field  $F$ . Then there exists a unique monic irreducible polynomial  $m \in F[x]$  having  $\alpha$  as a root. Moreover, if  $f \in F[x]$  is a polynomial, then  $f$  has  $\alpha$  as a root if, and only if  $m|f$ .*

*Proof.* Let  $m$  a polynomial of minimal degree having  $\alpha$  as a root. Suppose, also that  $m$  is monic. Now, if  $m$  were reducible, then  $m(x) = a(x)b(x)$  for some  $a, b \in F[x]$  polynomials both of degree less than  $\deg m$ . Then we also have that  $a(\alpha) = b(\alpha) = 0$ , which contradicts that  $m$  is the polynomial of minimal degree satisfying that condition. Hence,  $m$  is irreducible.

Now, let  $f \in F[x]$  have  $\alpha$  as a root, then by the division theorem, there exist  $q, r \in F[x]$ , with  $q \neq 0$  for which

$$f(x) = q(x)m(x) + r(x) \text{ where } \deg r < \deg m$$

Now, since  $f(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = 0$ , then  $r(\alpha) = 0$  for all  $\alpha$  lest we contradict the minimality of  $m$ . Hence  $m|f$ . Conversely, if  $m|f$ , then  $f$  has  $\alpha$  as a root.

Now, let  $g$  a polynomial of minimal degree for which  $g(\alpha) = 0$ . Then by above, we have that  $\deg g = \deg m$ , and that moreover,  $m|g$  and  $g|m$ . therefore  $g = m$  and uniqueness is established. ■

**Corollary.** *Let  $L/F$  be an extension, and  $\alpha$  algebraic over  $F$ . Let  $m_{\alpha,F}$  the unique monic irreducible polynomial over  $F$  having  $\alpha$  as root, and  $m_{\alpha,L}$  the unique monic irreducible polynomial over  $L$  having  $\alpha$  as root. Then  $m_{\alpha,L}|m_{\alpha,F}$  in  $L[x]$ .*

**Definition.** Let  $F$  be a field, and  $\alpha$  algebraic over  $F$ . We define the **minimal polynomial**  $m_{\alpha,F}$ , to be the polynomial over  $F$  of minimal degree having  $\alpha$  as a root. If the field is clear, we instead write  $m_\alpha$ , or even just  $m$  when the root itself is also clear. We define the **degree** of  $\alpha$  to be  $\deg \alpha = \deg m_\alpha$ .

**Lemma 1.2.2.** *Let  $\alpha$  algebraic over  $F$ . Then*

$$F(\alpha) \simeq F[x]/(m_{\alpha,F})$$

**Corollary.**  $[F(\alpha) : F] = \deg m_\alpha = \deg \alpha$ .

**Example 1.5.**

- (1) The minimal polynomial for  $\sqrt{2}$  over  $\mathbb{Q}$  is  $x^2 - 2$ .
- (3) The minimal polynomial for  $\sqrt[3]{2}$  over  $\mathbb{Q}$  is  $x^3 - 2$ .
- (3) Let  $n > 1$ , then by the Eisenstein-Schömann criterion,  $x^n - 2$  is irreducible over  $\mathbb{Q}$ . Moreover,  $x^n - 2$  has as root in  $\mathbb{R}$   $\sqrt[n]{2}$ . Then  $\mathbb{Q}(\sqrt[n]{2})$  is a field of degree  $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ . Moreover  $x^n - 2$  is the minimal polynomial of  $\sqrt[n]{2}$ . Notice, that over  $\mathbb{R}$ ,  $\deg [n]2 = 1$ , and that  $m_{\sqrt[n]{2}, \mathbb{R}}(x) = x - \sqrt[n]{2}$ .
- (4) Consider  $p(x) = x^3 - 3x - 1$  over  $\mathbb{Q}$ . Notice that  $p$  is irreducible over  $\mathbb{Q}$  and let  $\alpha$  a root of  $p$ . Then  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ .

**Lemma 1.2.3.** *An element  $\alpha$  is algebraic over a field  $F$  if, and only if the simple extension  $F(\alpha)/F$  is finite.*

*Proof.* If  $\alpha$  is algebraic over  $F$  then  $[F(\alpha) : F] = \deg \alpha \leq n$  if  $\alpha$  satisfies a polynomial of degree  $n$ . Conversely, if  $\alpha$  is an element of the finite extension  $K/F$ , of degree  $n$ , then the set  $\{1, \alpha, \dots, \alpha^n\}$  is linearly dependent over  $F$ . Hence there exist  $b_0, \dots, b_n \in F$  not all 0 for which

$$b_0 + b_1\alpha + \dots + a_n\alpha^n = 0$$

making  $\alpha$  a root of a nonzero polynomial over  $F$  of degree  $\deg \leq n$ . ■

**Corollary.** *If an extension  $K/F$  is finite, then it is algebraic.*

*Proof.* If  $\alpha \in K$  is algebraic, then  $K/F$  implies that  $F(\alpha)/F$  is finite, since  $F(\alpha) \subseteq K$ . ■

**Example 1.6.** Let  $F$  a field of char  $F \neq 2$ , and let  $K$  an extension field of  $F$  of degree  $[K : F] = 2$ . Let  $\alpha \in K$  not in  $F$ , then  $\alpha$  satisfies an polynomial of at most degree 2 over  $F$ . Now, since  $\alpha \notin F$ , this polynomial must have degree greater than 1. Hence it satisfies a polynomial of degree 2. Then the minimal polynomial of  $\alpha$  is a quadratic

$$m_\alpha(x) = x^2 + bx + c \text{ with } b, c \in F$$

Since  $F \subseteq F(\alpha) \subseteq K$ , and  $F(\alpha)$  is a vector space over  $F$  of dimension 2, then we must have  $K = F(\alpha)$ ; that is  $K/F$  is simple.

Now, the roots of  $m_\alpha$  are

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Since  $\alpha \notin F$ ,  $b^2 - 4c$  is not a square in  $F$ , and  $\sqrt{b^2 - 4c}$  is a root of the equation  $x^2 - (b^2 - 4c) = 0$  in  $K$ .

Conversely,  $\sqrt{b^2 - 4c} = \pm(b + 2\alpha)$  which puts  $\sqrt{b^2 - 4c} \in F(\alpha)$ . That is  $F(\sqrt{b^2 - 4c}) = F(\alpha)$ . Moreover,  $x^2 - (b^2 - 4c)$  does not have solutions in  $K$ .

We call field extensions  $K/F$  of degree 2 **quadratic field extension**, where  $K = F(\sqrt{D})$ , and  $D$  is a squarefree element of  $F$ .

**Theorem 1.2.4.** *Let  $F \subseteq K \subseteq L$ . Then  $[L : F] = [L : K][K : F]$ .*

*Proof.* Let  $[L : K] = m$  and  $[K : F] = n$ . Let  $\{\alpha_1, \dots, \alpha_m\}$  and  $\{\beta_1, \dots, \beta_n\}$  be bases for the extensions  $L/K$  and  $K/F$ . Now, the elements of  $L$  over  $K$  are of the form

$$a_1\alpha_1 + \dots + a_m\alpha_m \text{ where } a_i \in K \text{ for all } 1 \leq i \leq m$$

Since each  $a_i \in K$ , which is an extension over  $F$ , they have the form

$$a_i = b_{i1}\beta_1 + \dots + b_{in}\beta_n \text{ where } b_{ij} \in F \text{ for all } 1 \leq j \leq n$$

That is, every element of  $L$ , as a vector space over  $F$  are of the form

$$\sum b_{ij}\alpha_i\beta_j$$

So the set  $\{\alpha_1\beta_1, \dots, \alpha_m\beta_n\}$  spans  $L$ . It remains to show that this set is linearly independent.

Suppose that

$$\sum b_{ij}\alpha_i\beta_j = 0$$

for some  $b_{ij} \in F$ . Since  $\{\alpha_1, \dots, \alpha_m\}$  are linearly independent in  $L$  over  $K$ , we have that the coefficients  $a_1 = \dots = a_n = 0$  which makes

$$a_i = b_{i1}\beta_1 + \dots + b_{in}\beta_n = 0$$

Now, since  $\{\beta_1, \dots, \beta_n\}$  is linearly independent in  $K$  over  $F$ , this implies that  $b_{i1} = \dots = b_{in} = 0$  which makes the collection  $\{\alpha_1\beta_1, \dots, \alpha_m\beta_n\}$  linearly independent, and hence, a basis. Moreover, notice that this basis has size  $mn$ . ■

**Example 1.7.** (1) The element  $\sqrt{2} \notin \mathbb{Q}(\alpha)$ , where  $\alpha$  is the root of  $x^3 - 3x - 1$ ; since  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , and  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ .

(2) We have  $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ , and since  $(\sqrt[6]{2})^3 = \sqrt{2}$ , we observe that  $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$ . Moreover, notice that by theorem 1.2.4  $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ . Then we have the following tower of fields for

$$\begin{array}{c} \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2}) \\ \mathbb{Q}(\sqrt[6]{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

**Lemma 1.2.5.** *Let  $\alpha, \beta$  be algebraic over a field  $F$ . Then  $F(\alpha, \beta) = (F(\alpha))(\beta)$ .*

*Proof.* By definition,  $F(\alpha, \beta)$  contains  $F$ , and  $\alpha$ , and hence contains  $F(\alpha)$ . It also contains  $\beta$  so that  $(F(\alpha))(\beta) \subseteq F(\alpha, \beta)$ . By the same argument,  $(F(\alpha))(\beta)$  contains  $F$ ,  $\alpha$  and  $\beta$  so that  $F(\alpha, \beta) \subseteq (F(\alpha))(\beta)$ . ■

**Corollary.** *The elements of  $F(\alpha, \beta)$  are of the form  $\sum a_{ij}\alpha^ib^j$ , where  $1 \leq i \leq \deg \alpha$  and  $1 \leq j \leq \deg \beta$ .*

**Example 1.8.** Consider  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  generated by  $\sqrt{2}$  and  $\sqrt{3}$ . Notice that  $\deg \sqrt{3} = 2$  over  $\mathbb{Q}$  so that  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$ . Now  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$  if, and only if the polynomial  $x^2 - 3$  is irreducible over  $\mathbb{Q}(\sqrt{2})$ . Then it is irreducible if, and only if  $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$ . It can be shown that this is not the case by trying to find  $a, b \in \mathbb{Q}$  for which  $\sqrt{3} = a + b\sqrt{2}$ . Moreover we have

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

**Theorem 1.2.6.** *An extension field  $K/F$  is finite if, and only if it is generated by finitely many algebraic elements over  $F$ .*

*Proof.* Let  $K/F$  finite of degree  $n$ , and  $\{\alpha_1, \dots, \alpha_n\}$  a basis. Then by theorem 1.2.4,  $[F(\alpha_i) : F] \mid [K : F]$  for all  $1 \leq i \leq n$ . So each  $\alpha_i$  is algebraic over  $F$ . Then  $K$  is generated by finitely many algebraic elements.

Conversely, let  $K = F(\alpha_1, \dots, \alpha_k) = (F(\alpha_1, \dots, \alpha_{k-1}))(\alpha_k)$ . We obtain  $K$  by taking the extensions  $F_{i+1}/F_i$  iteratively, where  $F_{i+1} = F_i(\alpha_{i+1})$ , and obtain the sequence

$$F = F_0 \subseteq \dots \subseteq F_k = K$$

Now, if the elements  $\alpha_1, \dots, \alpha_k$  are algebraic over  $F$ , each of  $\deg \alpha_i = n_i$  for  $1 \leq i \leq k$ , then the extension  $F_{i+1}/F_i$  is a simple extension, and  $[F_{i+1} : F_i] = \deg m_{\alpha_{i+1}} \leq \deg \alpha_{i+1} = n_{i+1}$ . Then we have

$$[K : F] = [F_k : F_{k-1}] \dots [F_1, F] \leq n_1 \dots n_k$$

which makes  $K/F$  a finite extension. ■

**Corollary.** *If  $\alpha, \beta$  are algebraic over  $F$ , then so are  $\alpha \pm \beta$ ,  $\alpha\beta$ , and  $\alpha\beta^{-1}$  (for  $\beta \neq 0$ ).*

**Corollary.** *If  $L/F$  is an extension, then the collection of elements of  $L$  which are algebraic over  $F$  forms a subfield of  $L$ .*

**Example 1.9.** (1) Consider the extension  $\mathbb{C}/\mathbb{Q}$ , and let  $\text{cl } \mathbb{Q}$  the subfield of all elements of  $\mathbb{C}$  which are algebraic over  $\mathbb{Q}$ . Then  $\sqrt[n]{2} \in \text{cl } \mathbb{Q}$  for all  $n \geq 1$ , so that  $[\text{cl } \mathbb{Q} : \mathbb{Q}] \geq n$ . This makes  $\text{cl } \mathbb{Q}$  an infinite algebraic extension, and we call  $\text{cl } \mathbb{Q}$  the **field of algebraic numbers**.

(2) Consider  $\text{cl } \mathbb{Q} \cap \mathbb{R}$  as a subfield of  $\mathbb{R}$  (i.e. the subfield of all algebraic elements of  $\mathbb{Q}$ ). Since  $\mathbb{Q}$  is countable, so is the field  $\mathbb{Q}[x]$ , and each polynomial in  $\mathbb{Q}[x]$  has at most  $n$  roots in  $\mathbb{R}$ , hence the number of all algebraic elements of  $\mathbb{R}$  over  $\mathbb{Q}$  is also countable. This means that  $\text{cl } \mathbb{Q}$  must also be countable. Now, since  $\mathbb{R}$  is uncountable, then there exist uncountably transcendental numbers of  $\mathbb{R}$  over  $\mathbb{Q}$ . Most notably the irrational numbers  $\pi$  and  $e$  are transcendental.

**Theorem 1.2.7.** *If  $K$  is algebraic over  $F$ , and  $L$  algebraic over  $K$ , then  $L$  is algebraic over  $F$ .*

*Proof.* Let  $\alpha \in L$ , since  $L$  is algebraic over  $K$ , there exists a  $p \in K[x]$  having  $\alpha$  as root. Let  $p(x) = a_0 + a_1x + \cdots + a_nx^n$ . Consider then  $F(\alpha, a_0, \dots, a_n)$ . Since  $K/F$  is algebraic,  $a_0, \dots, a_n$  are algebraic over  $F$ , and so  $F(\alpha, a_0, \dots, a_n)$  is a finite extension over  $F$ . Then  $\alpha$  generates an extension field of degree less than  $n$ , and we get

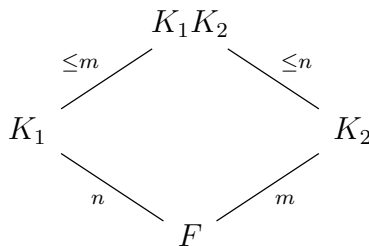
$$[F(\alpha, a_0, \dots, a_n) : F] = [F(\alpha, a_0, \dots, a_n) : F(a_0, \dots, a_n)][F(a_0, \dots, a_n) : F]$$

is finite, and  $F(\alpha, a_0, \dots, a_n)$  is algebraic over  $F$ . That is,  $\alpha$  is algebraic over  $F$ , and so  $L$  is algebraic over  $F$ . ■

**Definition.** Let  $K_1$  and  $K_2$  subfields of a field  $K$ . The **composite field**  $K_1K_2$  is the smallest subfield of  $K$  containing both  $K_1$  and  $K_2$ .

**Example 1.10.** The composite field of  $\mathbb{Q}(\sqrt[3]{2})$  and  $\mathbb{Q}(\sqrt{2})$  is  $\mathbb{Q}(\sqrt[6]{2})$ .

**Lemma 1.2.8.** Let  $K_1$  and  $K_2$  be extensions of a field  $F$  contained in a field  $K$ . Then  $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$  with equality holding if, and only if a basis of  $F$  in the other field is linearly independent. Moreover if  $\{\alpha_1, \dots, \alpha_m\}$  and  $\{\beta_1, \dots, \beta_n\}$  are bases for  $K_1$  and  $K_2$ , then  $\{\alpha_1\beta_1, \dots, \alpha_m\beta_n\}$  span  $K_1K_2$ .



**Corollary.** If  $[K_1 : F] = m$ , and  $[K_2 : F] = n$  with  $m$  and  $n$  coprime, then  $[K_1K_2 : F] = [K_1 : F][K_2 : F]$ .

*Proof.* We have that  $m, n | [K_1K_2 : F]$  and since  $K_1, K_2 \subseteq K_1K_2$  are subfields of  $K_1K_2$ , we get the least common multiple  $[m, n] | [K_1K_2 : F]$ . Now, since  $(m, n) = 1$ , we get  $[m, n] = mn$  so that  $mn \leq [K_1K_2 : F]$ . ■

## 1.3 Splitting Fields

**Definition.** Let  $K$  be an extension of a field  $F$ . We say a polynomial  $f$  over  $F$  **splits completely** over  $K$  if  $f$  factors into linear factors over  $K$ . If  $f$  splits completely over  $K$ , and in no other proper subfield, then we say  $K$  is the **splitting field** of  $f$  over  $F$ .

**Theorem 1.3.1.** If  $f$  is a polynomial over a field  $F$ , then there exists a splitting field  $K$  of  $f$  over  $F$ .

*Proof.* Let  $E$  an extension of  $F$  with  $[E : F] = n$ . By induction on  $n$ , for  $n = 1$ , we take  $E = F$  and we are done. Now, for  $n \geq 1$ , suppose the irreducible factors of  $f$  are of deg = 1. Then  $f$  has all its roots in  $F$ , and hence splits completely over  $F$ . Then take  $E = F$ . On

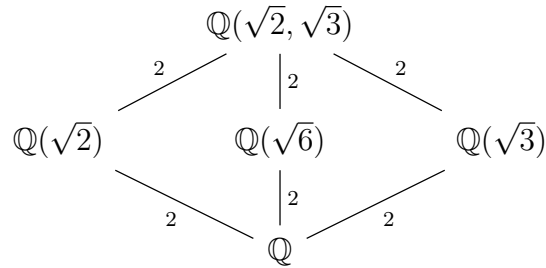
the other hand, if  $f$  has at least one irreducible factor of  $\deg \geq 2$ , then there is an extension  $E_1$  of  $F$  for which  $f$  has the factor  $(x - \alpha)$  for some root  $\alpha$ . Then  $f(x) = (x - \alpha)f_1(x)$  where  $\deg f_1 = n - 1$ . Therefore by the induction hypothesis, there is an extension  $E$  of  $E_1$  containing all the roots of  $f_1$ . Hence, it contains all the roots of  $f$  and  $f$  splits completely over  $E$ .

Now, let  $K$  be the intersection of all subfields of  $E$  for which  $f$  splits; i.e. all subfields containing the roots of  $f$ . Then by definition,  $K$  is the splitting field of  $f$  over  $F$ . ■

**Definition.** If  $K$  is an algebraic extension of  $F$  such that it is the splitting field for a collection of polynomials over  $F$ , then we say that  $K$  is a **normal extension** of  $F$ .

**Example 1.11.** (1) The splitting field of  $x^2 - 2$  over  $\mathbb{Q}$  is  $\mathbb{Q}(\sqrt{2})$ , since  $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$  and  $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$  and  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , so there is no other subfield in between.

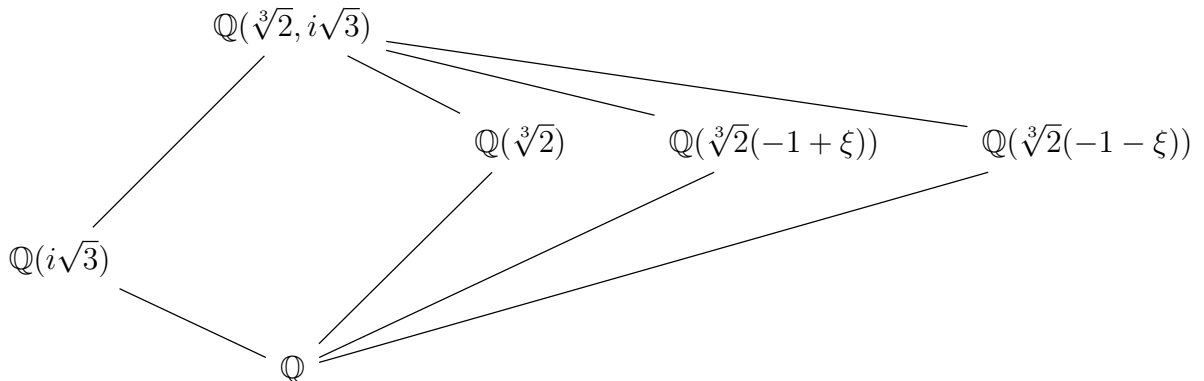
(2) The splitting field for  $(x^2 - 2)(x^2 - 3) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$  is  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Now,  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$  and the lattice of fields is



(3) Let  $\xi = i\sqrt{3}$ . Notice that  $x^3 - 2$  factors into  $x^3 - 2 = (x - \sqrt[3]{2})(x + \sqrt[3]{2}(-1 + \xi))(x + \sqrt[3]{2}(-1 - \xi))$ . Now,  $-1 + \xi, -1 - \xi \notin \mathbb{Q}(\sqrt[3]{2})$ , so  $\mathbb{Q}(\sqrt[3]{2})$  is not the splitting field for  $x^3 - 2$ . Let  $K$  be the splitting field of  $x^3 - 2$ . Then  $K$  contains  $-1 \pm \xi$ , so that  $i\sqrt{3} \in K$ . Thus

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

Moreover,  $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] \geq 2$  and since  $\mathbb{Q}(\sqrt[3]{2})$  is not the splitting field,  $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$ . Hence  $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$ . We have the following lattice.



- (4) Notice that  $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$  over  $\mathbb{Q}$  which is irreducible by Eisenstein's criterion. Using the quadratic formula, we get  $\pm 1$  and  $\pm i$  as the roots, moreover, notice that  $\pm 1, \pm i \in \mathbb{Q}(i)$  and since  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$  there are no subfields between  $\mathbb{Q}$  and  $\mathbb{Q}(i)$  so that  $\mathbb{Q}(i)$  is the splitting field of  $x^4 + 4$  over  $\mathbb{Q}$ .

**Lemma 1.3.2.** *A splitting field of a polynomial of degree  $n$  over a field  $F$  is of degree at most  $n!$  over  $F$ .*

*Proof.* Let  $f \in F[x]$  a polynomial of  $\deg f = n$ . Adjoining one root of  $f$  to  $F$ , we have an extension  $F_1/F$  of degree  $[F_1 : F] = n$ . Now,  $f$  over  $F_1$  has at least one linear factor, and so any root of  $f$  satisfies a polynomial of degree  $n - 1$ . Hence proceeding inductively gives the result. ■

**Example 1.12.** Consider the polynomial  $x^n - 1$  over  $\mathbb{Q}$ . Then the roots of  $x^n - 1$  are of the form  $\xi$  where  $\xi^n = 1$ . Notice, that in  $\mathbb{C}$ ,  $\xi = e^{\frac{2i\pi}{n}}$ , so that  $\mathbb{C}$  contains a splitting field of  $x^n - 1$ . Hence  $\mathbb{Q}(\xi) \subseteq \mathbb{C}$  is a splitting field of  $x^n - 1$  over  $\mathbb{Q}$ . Notice that the set of all roots  $\xi$  of  $x^n - 1$  forms a cyclic group generated by  $\xi$ .

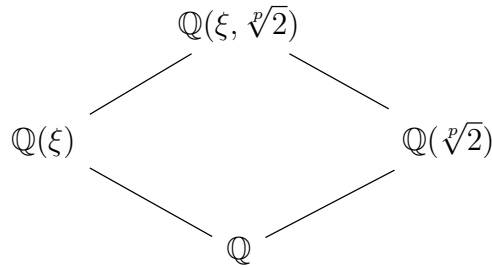
**Definition.** Consider a field  $F$  and the polynomial  $x^n - 1$  over  $F$ . We call the roots  $\xi$  of  $x^n - 1$ , where  $\xi^n = 1$  the **primitive  $n$ -th roots of unity** over  $F$ . We call  $F(\xi)$  the **cyclotomic field** over  $F$ .

**Example 1.13.** Let  $p$  be a prime, and consider the splitting field  $x^p - 2$  over  $\mathbb{Q}$ . If  $\alpha$  is a root, then  $\alpha^p = 2$  so that  $(\xi\alpha)^p = 2$  where  $\xi$  is a primitive  $p$ -th root of unity over  $\mathbb{Q}$ . So the roots of  $x^p - 2$  are

$$\sqrt[p]{2} \text{ and } \xi \sqrt[p]{2}$$

Notice that  $\frac{\xi \sqrt[p]{2}}{\sqrt[p]{2}} = \xi$  so the splitting field contains  $\mathbb{Q}(\xi, \sqrt[p]{2})$ . Moreover,  $\mathbb{Q}(\xi, \sqrt[p]{2})$  contains all the roots of  $x^p - 2$  so that  $\mathbb{Q}(\xi, \sqrt[p]{2})$  is the splitting field of  $x^p - 2$  over  $\mathbb{Q}$ .

Notice, that  $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\xi, \sqrt[p]{2})$  so that  $[\mathbb{Q}(\xi, \sqrt[p]{2}) : \mathbb{Q}(\xi)] \leq p$ . not, since  $\mathbb{Q}(\sqrt[p]{2})$  is also a subfield, we get  $[\mathbb{Q}(\xi, \sqrt[p]{2}) : \mathbb{Q}] \leq p(p - 1)$ . Since  $(p, p - 1) = 1$  (i.e. they are coprime), we have  $p(p - 1) | [\mathbb{Q}(\xi, \sqrt[p]{2}) : \mathbb{Q}]$  so that  $[p]2 : \mathbb{Q}] = p(p - 1)$ . We have the following lattice.



**Theorem 1.3.3.** *Let  $\phi : F \rightarrow F'$  a field isomorphism. Let  $f$  and  $f'$  polynomials over  $F$  and  $F'$ , where  $f'$  is obtained by applying  $\phi$  to the coefficients of  $f$ . Let  $E$  and  $E'$  be splitting fields of  $f$  and  $f'$  over  $F$  and  $F'$ , respectively. Then  $\phi$  extends to an isomorphism between  $E$  and  $E'$ ; i.e.  $E \simeq E'$ .*

$$\begin{array}{ccc}
 E & \longrightarrow & E' \\
 \downarrow & & \downarrow \\
 F & \xrightarrow{\phi} & F'
 \end{array}$$

*Proof.* Let  $\deg f = n$ . By induction on  $n$ . If  $f$  has all its roots in  $F$ ,  $f$  splits completely over  $F$ , and  $f'$  over  $F'$ . Then take  $E = F$  and  $E' = F'$  and we are done for  $n = 1$ .

Now, for  $n \geq 1$ , suppose the theorem is true. Let  $p$  an irreducible factor of  $f$ , and  $p'$  an irreducible factor of  $f'$ . If  $\alpha$  and  $\alpha'$  are roots of  $p$  and  $p'$ , respectively, then extend  $\phi$  to  $F(\alpha)$  and  $F'(\alpha')$ . Then  $f(x) = (x-\alpha)f_1(x)$  and  $f'(x) = (x-\alpha')f'_1(x)$ ; with  $\deg f_1 = \deg f'_1 = n-1$ . Then let  $E$  the splitting field of  $f_1$  over  $F(\alpha)$ , and  $E'$  the splitting field of  $f'_1$  over  $F'(\alpha')$

$$\begin{array}{ccc} E & \longrightarrow & E' \\ | & & | \\ F(\alpha) & \longrightarrow & F'(\alpha') \\ | & & | \\ F & \xrightarrow{\phi} & F' \end{array}$$

The roots of  $f_1$  and  $f'_1$  are in  $E$  and  $E'$ , respectively, and hence so are the roots of  $f$  and  $f'$ . Then by the induction hypothesis, we can extend  $\phi$  to  $E$  and  $E'$  so that  $E \simeq E'$ . ■

**Corollary.** *Any two splitting fields of a given polynomial over a field are isomorphic.*

*Proof.* Take  $\phi$  to be the identity map. ■

## 1.4 Algebraic Closures.

**Definition.** We define the **algebraic closure** of a field  $F$  to be the algebraic extension,  $\text{cl } F$ , over  $F$  for which every polynomial over  $F$  splits. We call a field  $K$  **algebraically closed** if every polynomial over  $K$  has at least one root in  $K$ .

**Lemma 1.4.1.** *A field  $K$  is algebraically closed if, and only if every polynomial over  $K$  has all of its roots in  $K$ .*

*Proof.* Certainly, if a polynomial  $f$  over  $K$  contains all of its roots in  $K$ , then  $K$  is algebraically closed, by definition.

Now, suppose that  $K$  is algebraically closed, and let  $f$  a polynomial over  $K$ . Then  $f$  contains at least one root in  $K$ . Hence  $f(x) = (x-\alpha)f_1(x)$  for some root  $\alpha$  of  $f$ , and where  $f_1 \in K[x]$ . But then by definition again,  $f_1$  contains at least one root in  $K$ . Hence, we proceed until we exhaust all the roots of  $f$ , and obtain that every root of  $f$  lies in  $K$ . ■

**Corollary.**  *$K$  is algebraically closed if, and only if  $\text{cl } K = K$ .*

**Lemma 1.4.2.** *Let  $F$  be a field, and  $\text{cl } F$  its algebraic closure. Then  $\text{cl } F$  is algebraically closed; i.e.  $\text{cl}(\text{cl } F) = \text{cl } F$ .*

*Proof.* Let  $f \in \text{cl } F[x]$ , and  $\alpha$  a root of  $f$ . Then  $\alpha$  generates all of  $\text{cl } F(\alpha)$ , making  $\text{cl } F$  algebraic over  $F$ . Hence  $\alpha$  is algebraic over  $F$ , but  $\alpha \in \text{cl } F$ , so that  $\text{cl}(\text{cl } F) = \text{cl } F$ . ■

**Lemma 1.4.3.** *For every field  $F$ , there exists an algebraically closed set containing  $F$ .*



*Proof.* Consider the polynomial ring  $F[\dots, x_n, \dots]$  where  $f(x_n)$  is a nonconstant polynomial over  $F$ . Consider the ideal  $(f)$ . Then, if  $(f) = (1)$ , then

$$g_1 f_1(x_1) + \dots + g_n f_n(x_n) = 1$$

where  $g_i \in F[x_i]$ . Then we get

$$g_1(x_1, \dots, x_m) f_1(x_1) + \dots + g_n(x_1, \dots, x_m) f_n(x_n) = 1$$

Now, let  $F'$  an extension of  $F$  containing a root  $\alpha_i$  of  $f_i$ . Then we observe that  $0 = 1$  in the above equation which is a blatant contradiction. So  $(f)$  must be a proper ideal.

Now, by Zorn's lemma, there exists a maximal ideal  $M$  containing  $I$ . Then the quotient

$$K_1 = F[\dots, x_n, \dots] / M$$

is a field containing an imbedding of  $F$ . Moreover,  $f$  has a root in  $K_1$ , so that  $f(x_n) \in (f) \subseteq M$ . Then  $K_1$  is a field in which every polynomial over  $F$  has a root. Proceeding as before with  $K_1$ , we obtain  $K_2$  in which every polynomial over  $K_1$  has a root. Hence, proceeding recursively, we obtain the sequence

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$$

in which every polynomial over  $K_n$  has all its roots in  $K_{n+1}$ . Now, let

$$K = \bigcup K_n$$

Then  $F \subseteq K$ , and every polynomial over  $K$  has a root in  $K_N$ , for  $N$  large enough; but  $K_N \subseteq K$ , so that  $K$  is algebraically closed. ■

**Lemma 1.4.4.** *Let  $K$  be algebraically closed, and let  $F \subseteq K$ . Then the collection of elements of the algebraic closure  $\text{cl } F$  of  $F$  that are algebraic over  $F$  is an algebraic closure of  $F$ .*

*Proof.* By definition,  $\text{cl } F / F$  is algebraic. Then every polynomial  $f$  over  $F$  splits over  $K$  into linear factors  $(x - \alpha)$ , where  $\alpha$  is a root of  $f$ . So  $\alpha$  is algebraic over  $F$ , and hence  $\alpha \in \text{cl } F$ . then all linear factors have a coefficient in  $\text{cl } F$ , so that  $f$  splits completely over  $\text{cl } F$ . ■

**Corollary.** *Algebraic closures are unique up to isomorphism.*

**Theorem 1.4.5** (The Fundamental Theorem of Algebra).  *$\mathbb{C}$  is algebraically closed.*

**Corollary.**  *$\mathbb{C}$  contains the an algebraic closure of any of its subfields.*

## 1.5 Seperability.

**Definition.** Let  $f$  be a polynomial over a field  $F$  with factorization

$$f(x) = a_n(x - \alpha_1)^{n_1} \dots (x - \alpha_k)^{n_k}$$

where  $\alpha_1, \dots, \alpha_k$  are roots of  $f$ , and  $a_n$  is the leading coefficient of  $f$ . If  $n_i > 1$ , we call  $\alpha_i$  a **multiple root** of  $f$ , and if  $n_i = 1$ , we call  $\alpha_i$  a **simple root**. We call  $n_i$  the **multiplicity** of  $\alpha_i$ .

**Definition.** A polynomial over a field  $F$  is said to be **seperable** if it has only simple roots. Otherwise, we say it is **inseperable**.

**Lemma 1.5.1.** *Seperable polynomials have all their roots distinct.*

**Definition.** We say a field  $F$  is a **finite field** if it has a finite number of elements. If  $|F| = n$ , then we denote  $F$  as  $\mathbb{F}_n$ .

**Lemma 1.5.2.** *Every finite field has finite characteristic.*

*Proof.* Recall that the characteristic is just the additive order of the element 1 in the field. ■

**Example 1.14.** (1)  $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$  is seperable over  $\mathbb{Q}$ . However  $(x^2 - 1)^n$  is inseperable.

(2) Consider  $x^2 - t$  over the field  $\mathbb{F}_2(t)$  of rational functions over  $t$ .  $x^2 - t$  is irreducible, but inseperable. Let  $\sqrt{t}$  a root, then  $(x - \sqrt{t})^2 = x^2 - t$  since  $\text{char } \mathbb{F}_2 = 2$ .

**Definition.** The **derivative** of a polynomial  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  over a field  $F$  is the polynomial

$$Df(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

over  $F$ .

**Lemma 1.5.3.** *For any two polynomials  $f$  and  $g$  over a field, the following are true.*

$$(1) D(f + g) = Df + D(g).$$

$$(2) D(fg) = fDg + gDf.$$

**Lemma 1.5.4.** *A polynomial  $f$  has a multiple root  $\alpha$  if, and only if  $\alpha$  is a root of  $Df$ . Moreover, the minimal polynomial of  $\alpha$ ,  $m_\alpha$  divides  $(f, Df)$ .*

*Proof.* Let  $\alpha$  a multiple root of  $f$ . Then  $f(x) = (x - \alpha)^n g(x)$  for some polynomial  $g$ . Hence

$$Df(x) = n(x - \alpha)^{n-1}g(x) + (x - \alpha)^n Dg(x)$$

so that  $\alpha$  is a root of  $Df$ .

Conversly, suppose that  $\alpha$  is a root of both  $f$  and  $Df$ . Then  $f(x) = (x - \alpha)g(x)$  for some polynomial  $g$ , and  $Df(x) = g(x) + (x - \alpha)Dg(x)$ . Now, since  $Df(\alpha) = 0$ , we get  $h(\alpha) = 0$ , so that  $h$  has a linear factor  $(x - \alpha)$ . This makes  $\alpha$  a multiple root of  $f$ . ■

**Corollary.**  *$f$  is seperable if and only if  $(f, Df) = 1$ .*

**Corollary.** *Every irreducible polynomial in a field  $F$  of  $\text{char } F = 0$  is seperable. Moreover, a polynomial over such a field is irreducible if, and only if it is the product of distinct irreducible factors.*

*Proof.* Let  $p$  an irreducible polynomial over  $F$  of  $\deg p = n$ . Then  $\deg Dp = n - 1$ . Up to constant factors, the factors of  $p$  are 1 and itself, so that  $(p, Dp) = 1$ . This makes  $p$  seperable. Therefore every irreducible polynomial over  $F$  is seperable, and the rest follows. ■

**Example 1.15.** (1) Let  $p$  prime and  $f(x) = x^{p^n} - x$  over the finite field  $\mathbb{F}_p$ , of char  $\mathbb{F}_p = p$ . Then  $Df(x) = p^n x^{p^n-1} - 1 \equiv -1 \pmod{p}$ . Then  $Df$  has no roots, which makes  $f$  seperable.

(2)  $D(x^n - 1) = nx^{n-1}$  for any field of char coprime to  $p$ . Then  $D(x^n - 1)$  has a root 0 of multiplicity  $n > 1$ , but 0 is not a root of  $x^n - 1$  so that  $x^n - 1$  is seperable. That is,  $x^n - 1$  has  $n$  distinct roots of unity  $\xi$ .

(3) Let  $F$  a field of char  $F = p$ , where  $p|n$ . Then there are fewer than  $n$  distinct  $n$ -th roots of unity over  $F$ , since  $n \equiv 0 \pmod{p}$ . Then  $D(x^n - 1) = 0$ , and every root of  $x^n - 1$  is a multiple root.

**Lemma 1.5.5.** *If  $f$  is a polynomial over a field  $F$  whose derivative is 0, then there exist a polynomial  $g$  for which  $f(x) = g(x^p)$  where char  $F = p$ .*

*Proof.* Let  $f(x) = a_0 + a_1x + \cdots + a_nx^n$ . Then  $Df(x) = a_1 + \cdots + na_nx^{n-1} = 0$ , so that every exponent  $i \equiv 0 \pmod{p}$ . That is,  $f(x) = a_0 + a_1x^p + \cdots + a_mx^{mp}$ . Then let

$$g(x) = a_0 + a_1x + \cdots + a_mx^m$$

then  $f(x) = g(x^p)$ . ■

**Lemma 1.5.6.** *Let  $F$  a field of char  $F = p$ . Then for every  $a, b \in F$ ,  $(a + b)^p = a^p + b^p$  and  $(ab)^p = a^p b^p$ .*

*Proof.* The binomial theorem gives

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$$

Now, since  $\binom{p}{i} \in \mathbb{Z}$  for any  $1 \leq i \leq p-1$ , and  $p$  is prime (the characteristic of a field has to be prime), then  $p|\binom{p}{i}$ . Hence  $\binom{p}{i} \equiv 0 \pmod{p}$ , so that the binomial expansion above reduces to

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

Now, let  $\phi : a \rightarrow a^p$ , then  $\phi$  is an automorphism of fields taking  $(ab)^p = a^p b^p$ . ■

**Corollary.** *Let  $F$  be a finite field of char  $F = p$ . Then every element of  $F$  is a  $p^{\text{th}}$  power in  $F$ .*

**Definition.** Let  $F$  be a field. We call the automorphism  $F \rightarrow F$  defined by  $a \rightarrow a^p$  where  $p \in \mathbb{Z}$  the **Frobenius automorphism**.

**Lemma 1.5.7.** *Every irreducible polynomial in a finite field  $F$  is seperable.*

*Proof.* Suppose otherwise. Since  $F$  has finite characteristic, there is a polynomial  $q$  over  $F$  for which  $p(x) = q(x^l)$ , where  $p$  is the irreducible polynomial in question, and char  $F = l$ . Let

$$q(x) = a_0 + a_1x + \cdots + a_nx^n$$

then  $a_i = b_i^p$  for some  $b_i \in F$ , and

$$\begin{aligned} p(x) &= q(x^l) \\ &= a_0 + a_1 x^p + \cdots + a_n x^{pn} \\ &= b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} \\ &= (b_0 + b_1 x + \cdots + b_n x^n)^p \end{aligned}$$

which is a contradiction. ■

**Definition.** A field  $K$  of characteristic  $\text{char } K = p$  is called **perfect** if for every  $a \in K$ , there exists a  $b \in K$  for which  $a = b^p$ , or  $p = 0$ .

**Example 1.16.** Let  $n > 0$  and consider the splitting field of the polynomial  $x^{p^n} - x$  over the finite field  $\mathbb{F}_p$ . Then  $x^{p^n} - x$  has precisely  $p^n$  roots.

Let  $\alpha, \beta$  be roots. Then  $\alpha^{p^n} = \alpha$ , and  $\beta^{p^n} = \beta$ . Then  $(\alpha\beta)^{p^n} = \alpha\beta$  and  $(\alpha^{-1})^{p^n} = \alpha^{-1}$ . Moreover,  $(\alpha + \beta)^{p^n} = \alpha + \beta$ . So the set of  $p^n$  distinct roots of  $x^{p^n} - x$  is closed under addition, multiplication, and inverses in its splitting field. Let  $F$  be that splitting field. Notice that  $F \subseteq \mathbb{F}_{p^n}$ , moreover,  $[F : \mathbb{F}_p] = n$  so that  $|F| = p^n$ . We also have that  $\mathcal{U}(F)$  is a cyclic group of order  $p^n - 1$ , so that  $F_{p^n} \subseteq F$ , since  $\alpha^{p^n-1} = 1$ . Therefore  $\mathbb{F}_{p^n}$  is the splitting field of  $x^{p^n} - x$  over  $\mathbb{F}_p$ , and so contains all the roots of  $x^{p^n} - x$ . Hence finite fields of order  $p^n$  exist and are unique up to isomorphism.

**Lemma 1.5.8.** Let  $f$  an irreducible polynomial over a field  $F$  of  $\text{char } F = p$ . Then there exists a unique integer  $k \geq 0$  and a unique separable polynomial  $s$  such that  $f(x) = s(x^{p^k})$ .

*Proof.* We have that since  $\text{char } F = p$ , there exists a polynomial  $f_1$  over  $F$  for which  $f(x) = f_1(x^p)$ . Now, if  $f_1$  is separable, take  $k = 1$  and we are done. Otherwise, there is a polynomial  $f_2$  over  $F$  for which  $f_2(x) = f_1(x^p)$ , so that  $f(x) = f_1(x^p) = f_2(x^{p^2})$ . Then proceeding in this fashion, we obtain a separable polynomial  $s$  for which  $f(x) = s(x^{p^k})$  where  $k \geq 0$ . ■

**Definition.** Let  $f$  an irreducible polynomial over a field of characteristic  $p$ , a prime. Let  $f_s$  the polynomial for which  $f(x) = f_s(x^{p^k})$  for some unique integer  $k \geq 0$ . Then we call the degree of  $f_s$  the **separable degree** of  $f$  and write  $\deg_s f = \deg f_s$ . We call the integer  $p^k$  the **inseparable degree** and write  $\deg_i f = p^k$ . We call  $f_s$  the **separable part** of  $f$ .

**Lemma 1.5.9.** A polynomial  $f$  is separable if, and only if  $\deg_i f = 1$  and  $\deg_s f = \deg f$ . Moreover,

$$\deg f = \deg_s f \cdot \deg_i f$$

**Example 1.17.** (1)  $x^p - t$  over  $\mathbb{F}_p(t)$  is irreducible with derivative  $D = 0$ . Hence  $x^p - t$  is inseparable. We call  $x^p - t$  a **purely inseparable polynomial**. Notice that  $x^p - t$  has separable part  $(x - t)$ .

(2)  $x^{p^n} - t$  over  $\mathbb{F}_p(t)$  is irreducible with separable part  $(x - t)$ , and  $\deg_i = p^n$ .

(3) Let  $f(x) = (x^{p^n} - t)(x^p - t)$  over  $\mathbb{F}_p(t)$ . Then  $p$  has two inseparable irreducible factors, and so is inseparable.

**Definition.** An extension  $K$  over a field  $F$  is called **seperable** if every  $\alpha \in K$  is the root of a seperable polynomial over  $F$ . Otherwise, we call  $K$  **inseperable**.

**Lemma 1.5.10.** *Every fnite extension of a perfect field is seperable.*

**Corollary.** *Finite extension fields of  $\mathbb{Q}$  and  $\mathbb{F}_p$  are seperable.*

## 1.6 Cyclotomic Polynomials.

**Definition.** We define **Euler's totient** to be the map  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  defined by the rule  $\phi(n) = |\{a \in \mathbb{Z} : (a, n) = 1\}|$ . That is,  $\phi$  of  $n$  is the number of all integers less than  $n$ , coprime to  $n$ .

**Definition.** We define  $\Xi_n$  to be the **group of all primitive  $n$ -th roots of unity**,  $\xi$  for which  $\xi^n = 1$ .

**Lemma 1.6.1.**  $\Xi_n \simeq \mathbb{Z}/n\mathbb{Z}$ .

*Proof.* The map  $a \rightarrow \xi^a$  defines the required isomorphism. ■

**Corollary.**  $\text{ord } \Xi_n = \phi(n)$  where  $\phi$  is Euler's totient.

*Proof.* Since  $\xi^n \equiv \xi^{0 \bmod n} \equiv 1$ , we have every non identity power of  $\xi$  has exponenct coprime to  $n$ . That is there are  $\phi(n)$  such distinct powers of  $\xi$ . ■

**Corollary.** *If  $d|n$ , then  $\Xi_d \leq \Xi_n$ .*

*Proof.* Notice that if  $d|n$ , then  $d = mn$  for some  $m \in \mathbb{Z}^+$ . Then  $\xi^d = 1$  implies  $(\xi^d) = \xi^{dm} = \xi^n = 1$ . ■

**Definition.** We define the  **$n$ -th cyclotomic polynomial** to be the polynomial

$$\Phi_n(x) = \prod (x - \xi)$$

having as roots all  $n$ -primitive roots of unity.

**Lemma 1.6.2.** *The  $n$ -th cyclotomic polynomial  $\Phi_n$  has degree  $\deg \Phi_n = \phi(n)$ , where  $\phi$  is Euler's totient.*

*Proof.* Recall that  $\text{ord } \Xi_n = \phi(n)$ , and since the elements of  $\Xi_n$  are the roots of  $\Phi_n$ , there are  $\phi(n)$  such roots. This puts  $\deg \Phi_n = \phi(n)$ . ■

**Example 1.18** (Computing Cyclotomic Polynomials). Recall that the polynomial  $x^n - 1$  has as roots precisely all  $n$ -th roots of unity  $\xi$ , that is  $\xi^n = 1$ . If  $x^n - 1 \in F[x]$ ,  $F$  a field, the the splitting field of  $x^n - 1$  is  $F(\xi)$ . Then we have

$$x^n - 1 = \prod_{\xi \in \Xi_n} (x - \xi)$$

Now, grouping those factors where  $\xi^d = 1$  for some  $d|n$ , then we have

$$x^n - 1 = \prod_{\xi \in \Xi_d} (x - \xi) \prod_{\xi \in \Xi_n} (x - \xi) = \prod_{d|n} d \prod_{\xi \in \Xi_n} (x - \xi) = \prod_{d|n} \Phi_d(x)$$

that is,

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

which gives a method for computing  $\Phi_n$  recursively.

We have  $\Phi_1(x) = x - 1$  and  $\Phi_2(x) = x + 1$ . Now,  $\Phi_3(x) = \Phi_1(x)\Phi_3(x) = (x - 1)\Phi_3(x)$ , so that

$$\Phi_3(x) = x^2 + x + 1$$

We have  $\Phi_4(x) = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x - 1)(x + 1)\Phi_4(x) = (x^2 - 1)\Phi_4(x)$ . So

$$\Phi_4(x) = x^2 + 1$$

Similarly,

$$\begin{aligned} \Phi_5(x) &= x^4 + x^3 + x + 1 \\ \Phi_6(x) &= x^2 - x + 1 \\ \Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ \Phi_8(x) &= x^4 + 1 \\ \Phi_9(x) &= x^6 + x^3 + 1 \\ \Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\ \Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ \Phi_{12}(x) &= x^4 - x^2 + 1 \end{aligned}$$

Also observe that if  $p$  is prime, then

$$\Phi_p(x) = \sum_{i=0}^{p-1} x^i = x^{p-1} + x^{p-2} + \cdots + x + 1$$

**Lemma 1.6.3.**  $\Phi_n(x)$  is monic over  $\mathbb{Z}$ .

*Proof.* Notice that since  $x^n - 1 = \prod \Phi_d(x)$ , is monic, then each  $\Phi_d$  must also be monic for all  $d|n$ .

Now, by induction on  $n$ , for  $n = 1$ , it is clear that  $x - 1$  has coefficients in  $\mathbb{Z}$  (if  $x^n - 1 \in \mathbb{Z}[x]$  we are done, if not, just take  $1_F \rightarrow 1_{\mathbb{Z}}$ , where  $F$  is the underlying field of  $x^n - 1$ ). Now, suppose that  $\Phi_d(x) \in \mathbb{Z}[x]$  for all  $1 \leq d < n$ , and  $d|n$ . Then  $x^n - 1 = f(x)\Phi_n(x)$ , where  $f(x) = \prod \Phi_d(x)$  is monic over  $\mathbb{Z}$ . Moreover,  $f|x^n - 1$ , in the splitting field  $\mathbb{Q}(\xi)$  (since we take  $1_F \rightarrow 1_{\mathbb{Z}}$ , where  $\xi^n = 1$ ). Then  $f|x^n - 1$  over  $\mathbb{Q}$  by the division theorem, and by Gauss' lemma,  $f|x^n - 1$  in  $\mathbb{Z}$ . So  $\Phi_n \in \mathbb{Z}[x]$ .  $\blacksquare$

**Theorem 1.6.4.**  $\Phi_n$  is irreducible over  $\mathbb{Z}$ .

*Proof.* Again, if  $x^n - 1 \in F[x]$  for some field  $F$ , take  $1_F \rightarrow 1_{\mathbb{Z}}$  so that  $x^n - 1 \in \mathbb{Z}[x]$ . Suppose then that  $\Phi_n(x) = f(x)g(x)$  where  $f$  and  $g$  are monic, and  $f$  is irreducible. Let  $\xi^n = 1$ , a primitive  $n$ -th root, so that  $\xi$  is a root of  $f$ . Then  $f$  is the minimal polynomial for  $\xi$  over  $\mathbb{Q}$ . Now, let  $p$  a prime such that  $p \nmid n$ . Then  $\xi^p$  is a  $n$ -th root, of  $f$  or  $g$ . If  $f(\xi^p) = 0$ , then for all  $a$  with  $(a, n) = 1$ , we have  $\xi^a$  is a root of  $f$ . Moreover,  $a = p_1 \dots p_k$  where each  $p_i \nmid n$  is prime. That means tht  $\xi^{p_1}, (\xi^{p_1})^{p_2}, \dots, \xi^n$  are all roots of  $f$  making  $f = \Phi_n$  and we are done.

Suppose then that  $g(\xi^p) = 0$ . Then  $\xi$  is root of  $g(x^p)$ , and since  $f$  is minimal,  $f|g(x^p)$  in  $\mathbb{Z}[x]$ . Then we have  $g(x^p) = f(x)h(x)$  for  $f, h \in \mathbb{Z}[x]$ . reducing mod  $p$ , we get  $g(x^p) \equiv f(x)h(x) \pmod{p}$  in  $\mathbb{F}_p[x]$ ; but  $g(x^p) \equiv (g(x))^p \pmod{p}$ . Since  $\mathbb{F}_p[x]$  is a unique factorization domain, we get that  $f \pmod{p}$  and  $g \pmod{p}$  have a common factor. Then  $\Phi_n(x) \equiv f(x)g(x) \pmod{p}$  has a multiple root in  $\mathbb{F}_p[x]$ ; implying that  $x^n - 1$  has a multiple root, which is impossible; since  $x^n - 1$  has  $n$  distinct roots. Therefore  $\xi^p$  is a root of  $f$ . ■

**Corollary.**  $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$ .

*Proof.* We have by above that  $\Phi_n$  is the minimal polynomial for  $\xi$  over  $\mathbb{Q}$ . ■

**Example 1.19.** Let  $\xi^8 = 1$  an 8-th root of unity. Then  $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$  and  $\mathbb{Q}(\xi)$  has minimal polynomial  $\Phi_8(x) = x^4 + 1$ . Moreover,  $\mathbb{Q}(\xi)$  contains a primitive 4-th root of unity  $i^4 = 1$  (over  $\mathbb{C}$ ,  $i^2 = -1$ ). So that  $\mathbb{Q}(i) \subseteq \mathbb{Q}(\xi)$ . We als get that  $\xi + \xi^7 = \sqrt{2}$  (since  $\xi = e^{\frac{2i\pi}{8}}$  over  $\mathbb{C}$ ), and  $\mathbb{Q}(\xi) = \mathbb{Q}(i, \sqrt{2})$ .





# Bibliography

- [1] D. Dummit, *Abstract algebra*. Hoboken, NJ: John Wiley & Sons, Inc, 2004.
- [2] I. N. Herstein, *Topics in algebra*. New York: Wiley, 1975.