

# *Contents*

<b>1</b>	<b>Preliminary</b>	<b>3</b>
1.1	Intro: Fermat's Last Theorem . . . . .	3
1.2	Field Theory . . . . .	5
1.3	Galois Theory . . . . .	7
<b>2</b>	<b>Ring of Integers</b>	<b>8</b>
2.1	Algebraic Integers . . . . .	8
2.2	Cyclotomic Extensions . . . . .	11
2.3	Trace and Norm . . . . .	14
2.4	Units In Quadratic Fields . . . . .	16
2.5	Discriminants . . . . .	20
2.6	Integral Bases . . . . .	26
2.7	Structure Theorem of $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ . . . . .	29
2.8	Resultants . . . . .	38
<b>3</b>	<b>Dedekind Domains</b>	<b>46</b>
3.1	Basic Definitions . . . . .	46
3.2	Ideal Classes . . . . .	49
3.3	Prime Decomposition . . . . .	52
<b>4</b>	<b>Ideals In Ring of Integers</b>	<b>55</b>
4.1	Splitting Primes in $\mathcal{O}_K$ . . . . .	55
4.2	Norm on Ideals . . . . .	58

4.3	Norms and Indices . . . . .	60
<b>5</b>	<b>Ideal Class Group</b>	<b>67</b>
5.1	Finiteness of Ideal Class Group . . . . .	67
5.2	The Lattices . . . . .	70
5.3	The Unit Theorem . . . . .	75

# Chapter 1

## Preliminary

对酒当歌，人生几何！  
譬如朝露，去日苦多。  
慨当以慷，忧思难忘。  
何以解忧？唯有杜康

---

曹操

### 1.1 Intro: Fermat's Last Theorem

**Definition 1.1.1.** We define the *Gaussian integer* to be  $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ . This is Euclidean domain and so UFD.

**Example 1.1.2.** Solve  $x^2 + y^2 = z^2$  for integer solutions.

*Solution.* We may as well assume  $\gcd(x, y, z) = 1$ . In addition Observe  $x^2 + y^2 = z^2$  can be factored as  $(x - yi)(x + yi) = z^2$  in  $\mathbb{Z}[i]$ .

We claim  $x + yi$  can be written as  $u\alpha^2$  for some Gaussian integer  $\alpha$  and some Gaussian integer unit  $u$ . To do this, we will first show  $x + yi$  and  $x - yi$  are coprime in  $\mathbb{Z}[i]$ . Assume there exists  $\Pi \in \mathbb{Z}[i]$  so that  $\Pi \mid x - yi$  and  $\Pi \mid x + yi$ . Then we have  $\Pi$  divides  $(x + yi) + (x - yi) = 2x$ ,  $(x + yi)(x - yi) = z^2$  and  $(x + yi) - (x - yi) = 2yi$ . In particular, since  $x$  and  $y$  are coprime we have  $\Pi$  must be a prime dividing 2, i.e.  $\Pi \in \{1, -1, i, -i\}$ . Thus it is impossible for  $z$  to be even. Indeed,  $z$  is even imply  $4 \mid z^2$  and so mod the equation  $x^2 + y^2 = z^2$  by 4 we would have  $x^2 + y^2 \equiv 0 \pmod{4}$  which imply  $x$  and  $y$  are both even, contradicts the fact  $x$  and  $y$  are coprime. Hence  $\gcd(2, z) = 1$  and so  $\Pi \mid 1$ , which is a unit, i.e.  $x + iy$  and  $x - iy$  are coprime.

Now, we claim  $x + iy = u\alpha^2$  in  $\mathbb{Z}[i]$  as we have  $(x + iy)(x - iy) = z^2$  where we

may factor  $z = \prod_{i=1}^l \pi_i^{e_i}$  into product of primes and so  $(x+iy)(x-iy) = \prod \pi_i^{2e_i}$ . By coprime of  $x+iy$  and  $x-iy$ , WLOG, we have this splits into two distinct parts, i.e.  $x+iy = u \prod_{i=1}^k \pi_i^{2e_i}$  and  $x-iy = u^{-1} \prod_{i=k+1}^l \pi_i^{2e_i}$  where  $u$  is a unit. This finishes the proof of our claim that  $x+iy = u\alpha^2$ .

Next, observe  $u \in \{1, -1, i, -i\}$  as  $u$  is an unit. Therefore, assume  $\alpha = m + ni$  and we have

$$x+iy = u(m+ni)^2 = u((m^2-n^2) + (2mn)i)$$

and thus we must have  $\{x, y\} = \{\pm(m^2-n^2), \pm 2mn\}$  by compare the coefficient of above equation and take consideration in the value of  $u$ .

Hence, we have the integer solutions to be

$$\{x, y\} = \{\pm(m^2-n^2), \pm 2mn\}, z = \pm(m^2+n^2)$$



*Solution.* We also provide another solution to the above example.


Consider  $x^2 + y^2 = z^2$  with  $x, y, z$  coprime. Then, move from integers to rationals, we get

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

which is the circle. Hence, it suffice to find all rational solutions to

$$x^2 + y^2 = 1$$

Next, pick one solution  $(0, 1)$  to the equation  $x^2 + y^2 = 1$  and consider another real solution  $(x, y)$  to  $x^2 + y^2 = 1$ , we see  $(x, y) \in \mathbb{Q}^2$  if and only if the slope  $t$  of the line  $\ell : y - 1 = tx$  join  $(0, 1)$  and  $(x, y)$  is rational. Hence, we solve for  $(x, y)$  for the slope  $t \in \mathbb{Q} \setminus \{0\}$  and get  $x = -\frac{2t}{1+t^2}, y = \frac{1-t^2}{1+t^2}$ .

Thus, up to scalar, all  $\mathbb{Q}$  solution to  $x^2 + y^2 = z^2$  are given by  $(-2t, 1-t^2, 1+t^2)$ . 

**Example 1.1.3 (General Case).** Now, how about the solution to  $x^p + y^p = z^p$  where  $p$  is arbitrary prime?

In this case, we would have  $x^p + y^p = \prod_{i=0}^{p-1} (x + y\omega^i) = z^p$  where  $\omega = e^{2\pi i/p}$ . Then, we separate this into two cases,

1.  $p \nmid xyz$ ,
2.  $p \mid xyz$ .

In the first case, if  $p = 3$  then  $x^3 + y^3 \equiv z^3 \pmod{9}$  where each of these cubes is congruent to  $\pm 1 \pmod{9}$  due to  $3 \nmid xyz$ . However, this is impossible as we then would have  $2 \equiv 1 \pmod{9}$ . Therefore, we only need to consider  $p > 3$ .

Now, assume  $\mathbb{Z}[\omega]$  is a UFD, then it can be shown  $x + y\omega$  has the form  $u\alpha^p$  for some  $\alpha \in \mathbb{Z}[\omega]$  with  $x, y$  not divisible by  $p$ . This imply  $x \equiv y \pmod{p}$ . Similarly, writing  $x^p = (-z)^p = (-y)^p$  we obtain  $x \equiv -z \pmod{p}$ . Thus

$$2x^p \equiv x^p + y^p \equiv z^p \equiv -x^p \pmod{p} \Rightarrow p \mid 3x^p$$

This is a contradiction as  $p \nmid 3$  and  $p \nmid x$ . Hence, we established Fermat's last theorem<sup>1</sup> for all primes  $p$  which  $\mathbb{Z}[\omega]$  is UFD. However, this is not always the case as  $p = 23$  then  $\mathbb{Z}[\omega]$  is not UFD.

As one exam the argument we presented above, we see unique factorization in  $\mathbb{Z}[\omega]$  was needed only for the purpose of deducing  $x + y\omega = u\alpha^p$  while it may be deduced from the other way.

**Theorem 1.1.4 (Dedekind).** *The ideal in  $\mathbb{Z}[\omega]$  always factor uniquely into prime ideals.*

Use this theorem, we can show the principal ideal  $\langle x + y\omega \rangle$  is the  $p$ th power of some ideal  $I$ . For certain  $p$ , called regular primes, it then follows that  $I$  itself must be principal, say  $\langle \alpha \rangle$ . Then we have  $\langle x + y\omega \rangle = \langle \alpha \rangle^n = \langle \alpha^n \rangle$  and once again we have  $x + y\omega = u\alpha^n$ .

Then, we can again conclude that if  $p$  is regular prime, Fermat's Last Theorem holds. However, there exists non-regular primes, for example  $p = 37, 59$  or  $67$ .

In any case, our attempt (based on Gabriel Lamé's attempt) lead us to consider the ring  $\mathbb{Z}[\omega]$ .

**Remark 1.1.5.** For example, some questions regarding  $\mathbb{Z}[\omega]$  as follows

1. Is the ring  $\mathbb{Z}[\omega]$  a UFD?
2. What are the units in  $\mathbb{Z}[\omega]$ ?
3. What are irreducible elements in  $\mathbb{Z}[\omega]$ ?

Those questions forms a large portion of classical algebraic number theory and more accurately, these questions are asked in subring of arbitrary number fields, not just  $\mathbb{Q}[\omega]$ .

## 1.2 Field Theory

**Remark 1.2.1.** Primarily we consider subfields of  $\mathbb{C}$  in this note. A full treatment of introductory field theory and Galois theory, consider my notes on PMATH 348.

**Definition 1.2.2.** Let  $E, F$  be two fields, then we say  $E/F$  is a **field extension** if  $F$  is a subfield of  $E$ .

**Definition 1.2.3.** Let  $E/F$  be a field extension, we define the **degree of the extension** to be  $[E : F] = \dim_F(E)$  where we consider  $E$  as a vector space over  $F$ . We say  $E/F$  is finite extension if  $[E : F]$  is finite.

**Definition 1.2.4.** Let  $H$  be a field so  $F \subseteq H \subseteq E$  with  $H/F$  and  $E/H$  both field extension, then we say  $H$  is an **intermediate field** of  $E/F$ .

**Proposition 1.2.5.** *Let  $H$  be an intermediate field of  $E/F$  then we have*

$$[E : F] = [E : H][H : F]$$

---

<sup>1</sup>Fermat's Last Theorem states:  $x^n + y^n = z^n$  has no non-zero integer solution when  $n > 2$

*Proof.* See my Galois Theory course PMATH 348 Notes.

♡

**Definition 1.2.6.** A **number field** is a finite extension of  $\mathbb{Q}$ .

**Definition 1.2.7.** Let  $E/F$  be an field extension, then  $\alpha \in E$  is **algebraic over**  $F$  if there exists non-zero  $f(x) \in F[x]$  such that  $f(\alpha) = 0$ .

**Definition 1.2.8.** A polynomial  $f \in F[x]$  is **irreducible** if and only if  $\deg(f) \geq 1$  and  $f = gh$  imply at least one  $g$  or  $h$  are constant where  $g, h \in F[x]$ .

**Definition 1.2.9.** Let  $\alpha \in E$  where  $E/F$  is an extension, then  $F(\alpha)$  is the smallest subfield of  $E$  containing  $F$  and  $\alpha$ . Also,  $F[\alpha]$  is the smallest subring containing  $F$  and  $\alpha$ .

**Definition 1.2.10.** Let  $E/F$  be an field extension and  $\alpha \in E$  is algebraic over  $F$ . Then the minimal polynomial  $f(x) \in F[x]$  of  $\alpha$  is the smallest monic polynomial with  $\alpha$  as a root.

**Remark 1.2.11.** Let  $E/F$  and  $\alpha \in E$  be algebraic over  $F$ , then there exists a unique minimal polynomial of  $\alpha$  over  $F$ .

**Definition 1.2.12.** Let  $\alpha$  be algebraic over  $F$ , then the **degree of**  $\alpha$  over  $F$  is the degree of the minimal polynomial of  $\alpha$ .

**Remark 1.2.13.** Let  $E/F$  be an extension. If  $f(x)$  is the minimal polynomial of  $\alpha$  where  $\alpha$  is algebraic over  $F$ , then  $f(x)$  is irreducible and if  $g(x) \in F[x]$  vanishes  $\alpha$  then  $f(x) \mid g(x)$ .

**Theorem 1.2.14.** Let  $K \subseteq \mathbb{C}$ , if  $f(x) \in K[x]$  is irreducible in  $K[x]$  of degree  $n$ , then  $f(x)$  has  $n$  distinct roots.

**Definition 1.2.15.** We say  $E/F$  is a **simple extension** if  $E = F(\alpha)$  for some  $\alpha \in E$ .

**Definition 1.2.16.** Let  $E \subseteq \mathbb{C}$ , then the **algebraic closure** of  $E$ , denoted by  $\overline{E}$ , is the set of all elements that is algebraic over  $E$  in the extension  $\mathbb{C}/E$ .

**Definition 1.2.17.** Let  $K$  be a field. Let  $\alpha \in \overline{K}$ , the **conjugates** of  $\alpha$  is the set of elements that vanishes the minimal polynomial of  $\alpha$  (note they are all distinct).

**Theorem 1.2.18.** Let  $K \subseteq \mathbb{C}$  and  $\alpha$  algebraic over  $K$  of degree  $n$  and minimal polynomial  $p(x)$ , then we have

$$K(\alpha) \cong K[x]/\langle p(x) \rangle$$

and in particular,  $K(\alpha) = \text{span}_K(1, \alpha, \dots, \alpha^{n-1}) = K[\alpha]$

**Definition 1.2.19.** Let  $R, S$  be two rings, an injective ring homomorphism  $\phi : R \rightarrow S$  is an **embedding**.

**Theorem 1.2.20.** Let  $K$  be a subfield of  $\mathbb{C}$  and  $L$  a finite extension of  $K$ . Every embedding of  $K$  in  $\mathbb{C}$  extends to exactly  $[L : K]$  embeddings of  $L$  in  $\mathbb{C}$ .

**Theorem 1.2.21.** Let  $K \subseteq L \subseteq \mathbb{C}$  and  $L$  is a finite extension of  $K$ . Then  $L = K(\alpha)$  for some  $\alpha \in L$ .

## 1.3 Galois Theory

**Definition 1.3.1.** Let  $F \subseteq E \subseteq \mathbb{C}$ , then  $E/F$  is a **normal extension** if  $\alpha \in E$  then all conjugates of  $\alpha$  are also in  $E$ .

**Theorem 1.3.2.** Let  $K \subseteq L \subseteq \mathbb{C}$  with  $L/K$  a finite extension. Then  $L$  is normal over  $K$  if and only if every embedding of  $L$  into  $\mathbb{C}$  which fixes each element of  $K$  is an automorphism of  $L$ .

**Remark 1.3.3.** If  $K \subseteq L \subseteq \mathbb{C}$ , then  $L$  is normal over  $K$  if and only if there are  $[L : K]$  many automorphisms of  $L$  which fix each element of  $K$ . This is by Theorem 1.3.2 and Theorem 1.2.20.

**Theorem 1.3.4.** Let  $K \subseteq \mathbb{C}$ . Let  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$  be algebraic over  $K$ . Then  $L = (\alpha_1, \dots, \alpha_n)$  is normal over  $K$  if conjugates of  $\alpha_1, \dots, \alpha_n$  are all in  $L$ .

**Corollary 1.3.4.1.** Let  $K \subseteq L \subseteq \mathbb{C}$  with  $L/K$  a finite extension. Then there exists a finite extension of  $H$  which  $H$  is normal over  $K$ .

**Definition 1.3.5.** Let  $K \subseteq L \subseteq \mathbb{C}$ , we define the **Galois group** of  $L$  over  $K$ , denoted by  $\text{Gal}(L/K)$ , to be the group of automorphisms of  $L$  that fixes  $K$  with the composition as the operation.

**Definition 1.3.6.** Let  $H$  be a subgroup of  $\text{Gal}(L/K)$ , then the **fixed field**, denoted by  $F_H$  or  $L^H$ , is the field

$$\{\alpha \in L : \forall \phi \in H, \phi(\alpha) = \alpha\}$$

**Remark 1.3.7.** Note  $K \subseteq F_H \subseteq L$  if  $H \leq \text{Gal}(L/K)$ .

**Theorem 1.3.8.** Let  $K \subseteq L \subseteq \mathbb{C}$  where  $L/K$  is finite extension. Suppose  $L$  is a normal extension and  $G = \text{Gal}(L/K)$ . Then  $K = L^G$  and  $K$  is not the fixed field of any proper subgroup of  $G$ .

**Definition 1.3.9.** Let  $K \subseteq L \subseteq \mathbb{C}$  with  $L/K$  a finite normal extension. Then let  $\text{Int}(L/K)$  be the set of intermediate field between  $K$  and  $L$ , let  $\text{Sub}(G)$  be the set of subgroups of  $G := \text{Gal}(L/K)$ .

**Theorem 1.3.10 (Galois Correspondence).** Let  $L/K$  be a finite normal extension and  $G = \text{Gal}(L/K)$ . Consider the map  $\lambda : \text{Int}(L/K) \rightarrow \text{Sub}(G)$  given by  $\lambda(F) = \text{Gal}(L/F)$  and  $\mu : \text{Sub}(G) \rightarrow \text{Int}(L/K)$  given by  $\mu(H) = L^H$ .

Then,

1.  $\lambda$  and  $\mu$  are inverse of each other.
2.  $F$  is normal over  $K$  if and only if  $\lambda(F)$  is a normal subgroup of  $G$ .
3. If  $F$  is normal over  $K$ , then  $G/\lambda(F)$  is isomorphic to  $\text{Gal}(F/K)$  via the map  $\sigma + \lambda(F) \mapsto \sigma|_F$ , the restriction map.

## Chapter 2

### Ring of Integers

白日何短短，百年苦易满。  
苍穹浩茫茫，万劫太极长。  
麻姑垂两鬓，一半已成霜。  
天公见玉女，大笑亿千场。  
吾欲揽六龙，回车挂扶桑。  
北斗酌美酒，劝龙各一觞。  
富贵非所愿，与人驻颜光。

李白

## 2.1 Algebraic Integers

**Definition 2.1.1.**  $\alpha$  is said to be **algebraic number** if  $\alpha$  is algebraic over  $\mathbb{Q}$ .

**Definition 2.1.2.**  $\alpha$  is said to be **algebraic integer** if  $\alpha$  is a root of a monic polynomial in  $\mathbb{Z}[x]$  where a monic polynomial is a polynomial with leading coefficient 1.

**Example 2.1.3.** Consider the extension  $\mathbb{Q}/\mathbb{Z}$ , then  $\frac{1}{2}$  is algebraic over  $\mathbb{Z}$  but not algebraic integer as the polynomial  $2x - 1$  does not have 1 as leading coefficient.

**Theorem 2.1.4.** Let  $\alpha$  be an algebraic integer. Then the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  is in  $\mathbb{Z}[x]$ .

*Proof.* Since  $\alpha$  is an algebraic integer, by definition  $\alpha$  is a root of some monic polynomial  $h(x) \in \mathbb{Z}[x]$ . Let  $p(x) \in \mathbb{Q}[x]$  be the minimal polynomial of  $\alpha$ . Then  $h(x) = p(x)g(x)$  for some  $g(x) \in \mathbb{Q}[x]$ . Since both  $h(x)$  and  $p(x)$  are monic, we must have  $g(x)$  to be monic. Now, choose  $a, b \in \mathbb{Z}$  so that  $ap(x), bg(x)$  are primitive and in  $\mathbb{Z}[x]$ , then  $abh(x) = (ap(x))(bg(x))$ . By Gauss's lemma, which states the product



of primitive polynomials is still primitive, we have  $(ap(x))(bg(x))$  is primitive and so  $ab = \pm 1$ , i.e.  $p(x) \in \mathbb{Z}[x]$ .  $\heartsuit$

**Corollary 2.1.4.1.** *The only algebraic integers in  $\mathbb{Q}$  are the ordinary integers.*

*Proof.* Let  $\alpha \in \mathbb{Q}$  be algebraic integer. Since  $\alpha \in \mathbb{Q}$  the degree of minimal polynomial  $h(x)$  of  $\alpha$  over  $\mathbb{Q}$  is 1, i.e.  $h(x) = x - \alpha$ . However, by Theorem 2.1.4, we must have  $h(x) \in \mathbb{Z}[x]$ , i.e.  $h(x) = cx + d$  where  $c, d \in \mathbb{Z}$ . However, since  $h(x)$  must be monic by definition, we have  $h(x) = x + d$ , i.e.  $\alpha = -d$  and the proof follows.  $\heartsuit$

**Corollary 2.1.4.2.** *Let  $d$  be a squarefree integer, i.e. it is divisible by no squares. Then the set of algebraic integers in  $\mathbb{Q}[\sqrt{d}]$  is*

$$\begin{cases} \{r + s\sqrt{d} : r, s \in \mathbb{Z}\}, & \text{when } d \equiv 2, 3 \pmod{4} \\ \{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod{2}\}, & \text{when } d \equiv 1 \pmod{4} \end{cases}$$

*Proof.* Let  $\alpha = r + s\sqrt{d}$  be an algebraic integer in  $\mathbb{Q}[\sqrt{d}]$  where  $r, s \in \mathbb{Q}$ . If  $s = 0$  then we are done as  $\alpha = r \in \mathbb{Q}$  which by the above corollary we have  $\alpha \in \mathbb{Z}$ . Hence, suppose  $s \neq 0$ .

The minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  is given by

$$p(x) = (x - (r + s\sqrt{d}))(x - (r - s\sqrt{d})) = x^2 - 2rx + r^2 - ds^2 \in \mathbb{Q}[x]$$

In particular, observe  $p(x) \in \mathbb{Z}[x]$  by Theorem 2.1.4 and so  $2r, r^2 - ds^2$  are both integers. Now we consider two cases based on the fact that  $2r$  is an integer:

1.  $r \in \mathbb{Z}$ . Then  $ds^2 \in \mathbb{Z}$ . Let  $q$  be a prime factor of the denominator of  $s$ . Then  $q^2 \mid d$ , which is a contradiction to the fact that  $d$  is square free. Hence the denominator of  $s$  has no prime factor (hence denominator must be  $\pm 1$ ) and  $s \in \mathbb{Z}$ .
2. If  $r \in \mathbb{Z}/2$ . Then  $r = \frac{2n+1}{2}$  for  $n \in \mathbb{Z}$ . Since  $r^2 - ds^2$  is an integer, we have

$$(\frac{2n+1}{2})^2 - ds^2 = k \in \mathbb{Z} \Rightarrow 4(n^2 + n) + 1 - 4ds^2 = 4k \in \mathbb{Z}$$

However, observe in the above equation, after mod out by 4, we have  $1 - 4ds^2 \equiv 0 \pmod{4}$ . In particular, we must have  $4ds^2$  is an integer that is not divisible by 4 as  $4 \mid 4ds^2$  then  $1 \equiv 0 \pmod{4}$ . Therefore, let  $p$  be a prime factor of the denominator of  $s$ , we must have  $p^2 \mid 4$  or  $p^2 \mid d$ , i.e. the only possible denominator of  $s$  is  $p = 2$  and we must have this  $p = 2$ . Therefore,  $s = \frac{b}{2}$  where  $b \in \mathbb{Z}$  and thus

$$db^2 \equiv 1 \pmod{4} \Leftrightarrow d \equiv 1 \pmod{4}, b \equiv 1 \pmod{2}$$

This concludes our proof.  $\heartsuit$

**Theorem 2.1.5.** *Let  $\alpha$  be a complex number, then the following are equivalent:*

1.  $\alpha$  is an algebraic integer.
2. The additive group of the ring  $\mathbb{Z}[\alpha]$  is finitely generated.
3.  $\alpha$  is a member of some subring of  $\mathbb{C}$  have a finitely generated additive group.
4.  $\alpha A = \{\alpha\beta : \beta \in A\} = \subseteq A$  for some finitely generated additive group  $A$  of  $\mathbb{C}$

*Proof.*

(1)  $\Rightarrow$  (2): By Theorem 1.2.18, we have  $\mathbb{Z}[\alpha]$  is generated by  $1, \alpha, \dots, \alpha^{n-1}$  where  $n$  is the degree of  $\alpha$  over  $\mathbb{Q}$ . Thus it is finitely generated.

(2)  $\Rightarrow$  (3): Immediate.

(3)  $\Rightarrow$  (4): Immediate.

(4)  $\Rightarrow$  (1): Suppose  $\beta_1, \dots, \beta_m$  generates  $A$  and since  $\alpha A \subseteq A$ , for  $1 \leq i \leq m$  we have

$$\alpha\beta_i = c_{i1}\beta_1 + \dots + c_{im}\beta_m, c_{i1}, \dots, c_{im} \in \mathbb{Z}$$

Thus define

$$M = \begin{bmatrix} c_{11} & \dots & c_{1m} \\ \vdots & \ddots & \vdots \\ c_{m1} & \dots & c_{mm} \end{bmatrix}$$

and we have, if define  $I_m$  to be the  $m \times m$  identity matrix, that

$$(\alpha I_m - M) \cdot \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Therefore, we must have  $\det(\alpha I_m - M) = 0$  as  $\beta_1, \dots, \beta_m$  are not all zero. However, observe  $\det(xI_m - M)$  is a monic polynomial in  $\mathbb{Z}[x]$  that vanishes  $\alpha$ , i.e.  $\alpha$  is an algebraic integer.  $\heartsuit$

**Corollary 2.1.5.1.** *If  $\alpha, \beta$  are two algebraic integers, then  $\alpha\beta$  and  $\alpha + \beta$  are both algebraic integers.*

*Proof.* Suppose  $\alpha$  has degree  $n$  and  $\beta$  has degree  $m$ . Then  $\mathbb{Z}[\alpha, \beta]$  is generated by  $\{\alpha^i \beta^j : 1 \leq i \leq n, 1 \leq j \leq m\}$  over  $\mathbb{Z}$ . Clearly  $\alpha + \beta$  and  $\alpha\beta \in \mathbb{Z}[\alpha, \beta]$  and hence the result follows from apply Theorem 2.1.5's (3)  $\Rightarrow$  (1) direction.  $\heartsuit$

**Remark 2.1.6.** This imply the set of algebraic integers form a ring.

**Theorem 2.1.7.** *Let  $\alpha$  be an algebraic number, then there exists positive integer  $r$  so that  $r\alpha$  is algebraic integer.*

*Proof.* Since  $\alpha$  is algebraic number, we have  $\alpha$  is a root of a polynomial  $q(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0$  where  $b_{n-1}, \dots, b_0 \in \mathbb{Q}$ . Clear out the denominator and we get

$$h(x) = rq(x) = rx^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x], r \in \mathbb{Z}_{\geq 1}$$

and  $h(\alpha) = rq(\alpha) = 0$ . Therefore, we have

$$r^{n-1}h(\alpha) = 0 \Rightarrow (r\alpha)^n + a_{n-1}(r\alpha)^{n-1} + \dots + a_1r^{n-2}(r\alpha) + a_0r^{n-1} = 0$$

Therefore,  $r\alpha$  is a root of the monic polynomial  $x^n + a_{n-1}x^{n-1} + \dots + a_1r^{n-2}x + a_0r^{n-1}$  and it is an algebraic integer as desired.  $\heartsuit$

## 2.2 Cyclotomic Extensions

**Definition 2.2.1.** We denote  $\mathbb{A}$  to be the *ring of algebraic integers*. For any finite extension  $K$  of  $\mathbb{Q}$ , let  $\mathbb{A} \cap K$  be the *ring of algebraic integers of  $K$* , which is also known as the *number ring of  $K$* .

**Remark 2.2.2.** Now we studied all the ring of algebraic integers of any quadratic extension of  $\mathbb{Q}$  in Corollary 2.1.4.2. As motivated by Fermat's last theorem, we turn our attention to cyclotomic extensions.

**Definition 2.2.3.** We define a *cyclotomic extension* over  $\mathbb{Q}$  to be  $\mathbb{Q}(\omega)$  where  $\omega$  is a root of unity. In particular, we define, for  $n \in \mathbb{Z}_{\geq 1}$  and  $\zeta_n = e^{2\pi i/n}$ , the polynomial

$$\Phi_n(x) = \prod_{j \leq n, \gcd(j,n)=1} (x - \zeta_n^j)$$

**Theorem 2.2.4.** For all  $n \in \mathbb{Z}_{\geq 1}$ ,  $\Phi_n(x)$  is irreducible over  $\mathbb{Q}$ .

*Proof.* We prove this by four steps.

**Step 1** : We claim  $\zeta_n$  is an algebraic integer. Since  $\zeta_n$  is a root of a monic polynomial  $x^n - 1$ , we have  $\zeta_n$  is algebraic integer as desired.

**Step 2** : We claim all possible conjugates of  $\zeta_n$  over  $\mathbb{Q}$  are of the form  $\zeta_n^j$  where  $1 \leq j \leq n$  and  $\gcd(n, j) = 1$ .

Since

$$x^n - 1 = \prod_{i=1}^n (x - \zeta_n^i)$$

The possible conjugates of  $\zeta_n$  are of the form  $\zeta_n^i$ . Suppose  $\gcd(n, i) = k > 1$ , then we have  $\zeta_n^i$  is a root of  $x^{n/k} - 1$  and because  $\zeta_n$  is not a root of  $x^{n/k} - 1$  for any  $k > 1$  we must have  $\zeta_n^i$  is not conjugate to  $\zeta_n$ . Viz, we must have  $\gcd(n, i) = 1$ .

**Step 3** : Let  $\theta = \zeta_n^t$  where  $\gcd(n, t) = 1$  and  $p$  a prime which is coprime with  $n$ . We claim  $\theta^p$  is a conjugate of  $\theta$  over  $\mathbb{Q}$ .

Let  $f(x)$  be the minimal polynomial of  $\theta$  over  $\mathbb{Q}$ . Thus there exists  $g(x) \in \mathbb{Q}[x]$  such that

$$x^n - 1 = f(x)g(x)$$

By Gauss's lemma, we have  $f(x), g(x) \in \mathbb{Z}[x]$ . Since  $\theta^p$  is also a root of  $x^n - 1$ , it is a root either of  $f(x)$  or  $g(x)$ . If it is a root of  $f(x)$ , then we are done.

Now suppose  $\theta^p$  is not a root of  $f(x)$  and is a root of  $g(x)$  for contradiction. Then  $\theta$  is a root of  $g(x^p)$ . Since  $f(x)$  is minimal, we have  $f(x) \mid g(x^p)$ . By Gauss's lemma again, the divisibility carries to  $\mathbb{Z}[x]$ .

For any  $h(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ , we define the **reduction** of  $h$  mod  $p$ , denoted by  $\bar{h}(x)$ , to be a polynomial in  $\mathbb{Z}/p\mathbb{Z}$  given by

$$\bar{h}(x) = \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n$$

and we observe  $v : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$  given by  $v(h) = \bar{h}$  is a ring homomorphism. Moreover, we have

$$(\bar{h}(x))^p = \bar{a}_0^p + \dots + \bar{a}_n^p(x^n)^p = \bar{a}_0 + a_1x^p + \dots + \bar{a}_nx^{np} = \bar{h}(x^p)$$

Thus, since  $f(x)$  divides  $g(x^p)$  we have  $\bar{f}(x)$  divides  $\bar{g}(x^p) = (\bar{g}(x))^p$ . Since  $\mathbb{Z}_p[x]$  is UFD, there exists irreducible polynomial  $\bar{r}(x) \in \mathbb{Z}_p[x]$  such that  $\bar{r}(x) \mid \bar{f}(x)$  and  $\bar{r}(x) \mid \bar{g}(x)$ . Hence we have

$$x^n - 1 = f(x)g(x) \Rightarrow x^n - \bar{1} = \bar{f}(x)\bar{g}(x) \Rightarrow \bar{r}(x)^2 \mid x^n - \bar{1}$$

Take the derivative and we get

$$\bar{r}(x) \mid \bar{n}x^{n-1}$$

Since  $\gcd(n, p) = 1$  we have  $\bar{n} \neq \bar{0}$  and so  $\bar{n}x^{n-1}$  is non-zero polynomial. Since all zeros of  $\bar{n}x^{n-1}$  are  $\bar{0}$  where  $\bar{0}$  is not a root of  $x^n - \bar{1}$ , we must have  $\bar{n}x^{n-1}$  and  $x^n - \bar{1}$  are coprime. Hence  $\bar{r}(x)$  is a constant as  $\bar{r}(x)$  divides both polynomials. This contradicts the fact that  $\bar{r}(x)$  is irreducible.

**Step 4** : We claim for all  $1 \leq j \leq n$  and  $\gcd(j, n) = 1$ , we have  $\zeta_n^j$  is conjugate of  $\zeta_n$  over  $\mathbb{Q}$ .

Given a  $j$ , we can factorize  $j$  into a product of primes. Since  $\gcd(j, n) = 1$  we have all prime factors of  $j$  are coprime to  $n$ . We start with  $\zeta_n$  and repeatedly use Step 3. Then  $\zeta_n^j$  is conjugate of  $\zeta_n$  over  $\mathbb{Q}$ . The proof follows as  $\Phi_n(x)$  is exactly the minimal polynomial of  $\zeta_n$  and hence it is irreducible.  $\heartsuit$

**Theorem 2.2.5.** For all  $n \in \mathbb{Z}_{\geq 1}$ , let  $\zeta_n = e^{2\pi i/n}$ . Then

1.  $\{\zeta_n^j : 1 \leq j \leq n, \gcd(n, j) = 1\}$  are all the conjugates of  $\zeta_n$  over  $\mathbb{Q}$ .
2. The cyclotomic extension  $\mathbb{Q}(\zeta_n)$  is a normal extension of  $\mathbb{Q}$ .

3.  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$  where  $\phi$  is the Euler phi function.

*Proof.* (1): This is immediate from the proof of Theorem 2.2.4.

(2): The roots of  $x^n - 1$  are  $\zeta_n, \zeta_n^2, \dots, \zeta_n^n$  and therefore, we have  $\mathbb{Q}(\zeta_n, \dots, \zeta_n^n) = \mathbb{Q}(\zeta_n)$  is normal over  $\mathbb{Q}$ .

(3): Since  $\Phi_n$  is the minimal polynomial of  $\zeta_n$  over  $\mathbb{Q}$ , we have  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n(x)) = \phi(n)$  as desired.  $\heartsuit$

**Theorem 2.2.6.** Let  $n \in \mathbb{Z}_{\geq 1}$ . The Galois group of  $\mathbb{Q}(\zeta_n)$  over  $\mathbb{Q}$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^\times$ , the group of units in  $\mathbb{Z}/n\mathbb{Z}$ . In particular,  $\mathbb{Q}(\zeta_n)$  is an abelian extension.

*Proof.* Let  $j = 1, \dots, n$  with  $\gcd(j, n) = 1$ . Define the automorphism  $\sigma_j$  of  $\mathbb{Q}(\zeta_n)$  to be  $\sigma(\zeta_n) = \zeta_n^j$ . Then we see

$$G = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_j : 1 \leq j \leq n, \gcd(j, n) = 1\}$$

Therefore, we define the map  $v : G \rightarrow \mathbb{Z}_n^\times$  by  $v(\sigma) = j + n\mathbb{Z}$  and we should see this is a bijective group homomorphism.  $\heartsuit$

**Theorem 2.2.7.** Let  $n \in \mathbb{Z}_{\geq 1}$ . If  $n$  is even, the only roots of unity in  $\mathbb{Q}(\zeta_n)$  are the  $n$ -th roots of unity. If  $n$  is odd then the only roots of unity in  $\mathbb{Q}(\zeta_n)$  are the  $2n$ -th roots of unity.

*Proof.* Let  $\gamma = e^{2\pi i(l/s)}$  with  $\gcd(l, s) = 1$  be an element in  $\mathbb{Q}(\zeta_n)$ . Let  $b = \text{lcm}(s, n)$ . Since  $\gcd(ln, s) = 1$ , by Bezout's identity we have integers<sup>1</sup>  $v$  and  $w$  so that  $lnv + sw = \gcd(s, n)$  and hence

$$\gamma^v \zeta_n^w = e^{2\pi i(vl/s)} \cdot e^{2\pi i(w/n)} = e^{2\pi i(\frac{lv}{s} + \frac{w}{n})} = e^{2\pi i(\frac{\gcd(s, n)}{sn})} = e^{2\pi i/b}$$

The degree of  $\mathbb{Q}(\zeta_b)$  over  $\mathbb{Q}$  is  $\phi(b)$  and since  $\mathbb{Q}(\zeta_b)$  is contained in  $\mathbb{Q}(\zeta_n)$ , we must have  $\phi(b) \mid \phi(n)$ . However, note  $b = \text{lcm}(s, n)$  and so  $n \mid b$ . Suppose

$$n = p_1^{l_1} \dots p_r^{l_r}, \quad b = p_1^{k_1} \dots p_t^{k_t}$$

where  $l_i, k_i \in \mathbb{Z}_{\geq 1}$ ,  $l_i \leq k_i$  and  $r \leq t$  with  $p_i$ 's all distinct prime.

Then, we have

$$\phi(n) = \prod_{i=1}^r (p_i^{l_i} - p_i^{l_i-1}), \quad \phi(b) = \prod_{i=1}^t (p_i^{k_i} - p_i^{k_i-1}) \Rightarrow \phi(n) \mid \phi(b)$$

Therefore, we must have  $\phi(n) = \phi(b)$ . However, exam the product above, we see there are only two possibilities:

---

<sup>1</sup>In particular, by Bezout's identity we have  $x$  and  $y$  so  $lnx + ys = 1$  and hence let  $v = \gcd(s, n)x$  and  $w = \gcd(s, n)y$  we are done.

1.  $n = b$ . If this is the case then  $s$  divides both  $b$  and  $n$  and so  $\gamma$  is a  $n$ th root of unity.
2.  $n \neq b$ . By look at the product above, we see the only possibilities that for  $n$  and  $b$  with  $n \neq b$  while still get the same value for the phi function is that there exists exactly one more prime factor of  $b$  with power 1, namely a copy of 2 (so we will get  $2^1 - 2^0 = 1$  in the product). Therefore, since  $n$  divides  $b$  while  $n \neq b$  we must have  $n$  is odd (since if  $n$  is even then they share a factor of 2) and  $b = 2n$ .

♡

**Corollary 2.2.7.1.** *The  $m$ th cyclotomic field for  $m$  even, are all distinct, and in fact pairwise non-isomorphic.*

**Example 2.2.8.** Let  $n, m \geq 1$  and  $\gcd(m, n) = 1$ , then show we have

$$\Phi_n(x^m) = \prod_{d|m} \Phi_{dn}(x)$$

*Solution.* Observe  $f(y) := \Phi_n(x^m) = \prod_{\gcd(i,n)=1} (x^m - \zeta_n^i)$ . We will show they agree by showing they have same factorization on  $\mathbb{C}$  in linear terms.

If  $f(a_0) = 0$  is a root, we must have  $a_0^m = \zeta_n^i$  for some  $i$ , i.e.  $a_0$  is a  $mn$ -th root of unity as  $(a_0^m)^n = (\zeta_n^i)^n = 1$ . Viz  $a_0 = \zeta_{mn}^k = e^{\frac{2\pi i k}{mn}}$  for some  $k$ . Hence let  $t = \gcd(m, k)$ , we have  $h_1 t = k$  and  $h_2 t = m$  with  $\gcd(h_1, h_2) = 1$  for if they are not coprime then  $t$  is not the greatest common factor. Moreover, we would have  $a_0 = e^{\frac{2\pi i h_1}{h_2 n}}$  and we observe  $h_1$  does not divide  $n$  or  $h_1 = 1$  because if it does we must have  $\gcd(m, n) \neq 1$ , i.e.  $x h_1 = n$  and  $t h_1 = m$  so  $h_1$  divides both  $n$  and  $m$ . Therefore, we have  $a_0$  is an  $h_2 n$ -th root of unity with  $a_0 = \zeta_{h_2 n}^{h_1}$  where  $\gcd(h_1, h_2 n) = 1$ , i.e.  $x - a_0$  is a factor of  $\Phi_{h_2 n}(x)$  where  $h_2 \mid m$ .

Conversely we see every  $\zeta_{dn}^i$  is a root of  $\Phi_n(x^m)$  where  $d \mid m$  and  $\gcd(i, dn) = 1$ . Thus the proof follows.

♠

## 2.3 Trace and Norm

**Remark 2.3.1.** We remark that if  $K = \mathbb{Q}(\theta)$  with degree  $n$ . Then let  $\sigma_1, \dots, \sigma_n$  be all the embeddings of  $K$  into  $\mathbb{C}$  with  $\mathbb{Q}$  fixed are precisely the following maps:  $\theta \mapsto \theta^i$  for  $1 \leq i \leq n$ , i.e. maps that send  $\theta$  to it's conjugates.

**Definition 2.3.2.** Let  $K$  be a number field and let  $\sigma_1, \dots, \sigma_n$  be all the embeddings of  $K$  in  $\mathbb{C}$  where  $n = [K : \mathbb{Q}]$ . Define the **trace**, denoted by  $T^K$  or just  $T$ , to be the function as follows: for each  $\alpha \in K$ , we have

$$T(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$$

**Definition 2.3.3.** Let  $K$  be a number field and  $\sigma_1, \dots, \sigma_n$  be all the embeddings of  $K$  in  $\mathbb{C}$ . Then we define the **norm**, denoted by  $N^K$  or just  $N$ , to be the function as follows: for each  $\alpha \in K$ , we have

$$N(\alpha) = \sigma_1(\alpha) \cdot \dots \cdot \sigma_n(\alpha)$$

**Remark 2.3.4.** Observe  $T$  is additive and  $N$  is multiplicative, i.e.  $T(a + b) = T(a) + T(b)$  and  $N(ab) = N(a)N(b)$ .

**Proposition 2.3.5.** Let  $r \in \mathbb{Q}$  and  $\alpha \in K$  where  $[K : \mathbb{Q}]$ , then we always have

$$T(r\alpha) = rT(\alpha), N(r\alpha) = r^n N(\alpha)$$

*Proof.* Observe for any embedding  $\sigma_i : K \rightarrow \mathbb{C}$  we always have  $\sigma_i(r\alpha) = r\sigma_i(\alpha)$ . Hence the proof follows immediately.  $\heartsuit$

**Theorem 2.3.6.** Let  $K$  be a number field with  $[K : \mathbb{Q}] = n$  and  $\alpha \in K$  with  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ . Then

$$T^K(\alpha) = \frac{n}{d}(T^{\mathbb{Q}(\alpha)}(\alpha)), N^K(\alpha) = (N^{\mathbb{Q}(\alpha)}(\alpha))^{n/d}$$

*Proof.* For each of the  $d$  embeddings of  $\mathbb{Q}(\alpha)$  to  $\mathbb{C}$  which fix  $\mathbb{Q}$  extends to  $[K : \mathbb{Q}(\alpha)] = \frac{n}{d}$  embeddings of  $K$  to  $\mathbb{C}$  which fixes  $\mathbb{Q}$ . Hence the result follows from definition.  $\heartsuit$

**Corollary 2.3.6.1.** Let  $K$  be a number field and  $\alpha \in K$ , then  $T(\alpha)$  and  $N(\alpha)$  are rational. Furthermore, if  $\alpha$  is algebraic integer then  $T(\alpha)$  and  $N(\alpha)$  are integers.

*Proof.* Consider  $\alpha \in \mathbb{Q}(\alpha)$ . Then we know all the embeddings of  $\mathbb{Q}(\alpha)$  to  $\mathbb{C}$  are of the form  $\alpha$  sends to another conjugate of  $\alpha$ . Hence, we have  $T^{\mathbb{Q}(\alpha)}(\alpha)$  is just the sum of conjugates and  $N^{\mathbb{Q}(\alpha)}(\alpha)$  is the product of all conjugates of  $\alpha$ . However, observe the minimal polynomial of  $\alpha$ , which is equal  $(x - \alpha_1) \dots (x - \alpha_n)$  where  $\alpha_1, \dots, \alpha_n$  are all the conjugates<sup>1</sup> of  $\alpha$ , has rational coefficients if  $\alpha \in K$  is algebraic number and has integer coefficients if  $\alpha$  is algebraic integer. In particular, the sum of conjugates occur in the minimal polynomial as the constant term and the product occur as the  $x^{n-1}$  term's coefficient.

Hence the proof follows as we use Theorem 2.3.6.  $\heartsuit$

**Example 2.3.7.** For  $K = \mathbb{Q}[\sqrt{m}]$  where  $m$  is square-free, we have  $T(a + b\sqrt{m}) = 2a$  and  $N(a + b\sqrt{m}) = a^2 - mb^2$ .

**Definition 2.3.8.** Let  $K \subseteq L \subseteq \mathbb{C}$  with  $L$  a finite extension of  $K$  with degree  $[L : K] = n$ . Let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $L$  in  $\mathbb{C}$  which fix  $K$ . Let  $\alpha \in L$ . Define the **trace** and **norm** of  $\alpha$  to be

$$T_K^L(\alpha) = \sum \sigma_i(\alpha), N_K^L(\alpha) = \prod \sigma_i(\alpha)$$

---

<sup>1</sup>including  $\alpha$  itself

**Theorem 2.3.9.** *Let  $K, L$  and  $M$  be finite extensions of  $\mathbb{Q}$  and  $K \subseteq L \subseteq M$ . Then, for all  $\alpha \in M$ , we have*

$$T_K^M(\alpha) = T_K^L(T_L^M(\alpha)), N_K^M(\alpha) = N_K^L(N_L^M(\alpha))$$

*Proof.* Let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $L$  in  $\mathbb{C}$  which fix  $K$ ,  $\tau_1, \dots, \tau_m$  be the embeddings of  $M$  in  $\mathbb{C}$  which fix  $L$ . Let  $N$  be a normal cover of  $M$  over  $\mathbb{Q}$ , i.e.  $N$  is the smallest normal extension over  $\mathbb{Q}$  which contains  $M$ . Each map  $\sigma_i$  (resp.  $\tau_j$ ) can be extended to an automorphism  $\sigma'_i$  (resp.  $\tau'_j$ ) of  $N$ .

Next, we will show that the all the  $mn$  embeddings of  $M$  which fix  $K$  are given by  $\sigma'_i \tau'_j|_M$  where  $|_M$  is the restriction and  $1 \leq i \leq n, 1 \leq j \leq m$ . Note we already have  $nm$  embeddings, it suffice to show they are all distinct embeddings.

Suppose  $\sigma'_i \tau'_j|_M = \sigma'_r \tau'_s|_M$ . Let  $L = K(\theta)$  for some  $\theta \in L$  (this can be done by primitive element theorem). Then we have

$$\sigma_i(\theta) = \sigma'_i(\theta) = \sigma'_i(\tau'_j(\theta)) = \sigma'_i \tau'_j|_M(\theta) = \sigma'_r \tau'_s|_M(\theta) = \sigma'_r(\tau'_s(\theta)) = \sigma'_r(\theta) = \sigma_r(\theta)$$

Since the behavior of  $\sigma_i$  is completely determined by the generator  $\theta$ , we have  $\sigma_i = \sigma_r$  and so  $i = r$ .

Next, let  $M = L(\kappa)$  for some  $\kappa \in M$ . A similar argument concludes that  $\tau_j(\kappa) = \tau_s(\kappa)$  and so  $s = j$ . Hence we have  $\sigma_i \tau_j|_M$  are all distinct for  $1 \leq i \leq n$  and  $1 \leq j \leq m$ . In particular, this imply  $\sigma'_i \tau'_j|_M$  are all the embeddings of  $M$  to  $\mathbb{C}$  fix  $K$ .

Now, for the trace, we have

$$T_K^L(T_L^M(\alpha)) = \sum_{i=1}^n \sigma_i \left( \sum_{j=1}^m \tau_j(\alpha) \right) = \sum_{i=1}^n \sum_{j=1}^m \sigma'_i \tau'_j(\alpha) = \sum_{i=1}^n \sum_{j=1}^m \sigma'_i \tau'_j|_M(\alpha) = T_K^M(\alpha)$$

The assertion for norm is identical. ♡

## 2.4 Units In Quadratic Fields

**Theorem 2.4.1.** *Let  $K$  be a number field and  $\alpha \in \mathbb{A} \cap K$ . Then  $\alpha$  is a unit in  $\mathbb{A} \cap K$  if and only if  $N_{\mathbb{Q}}^K(\alpha) = \pm 1$ .*

*Proof.* Suppose  $\alpha$  is a unit, then  $\exists \beta \in \mathbb{A} \cap K$  such that  $\alpha\beta = 1$ . Thus we have  $N_{\mathbb{Q}}^K(\alpha\beta) = N_{\mathbb{Q}}^K(1) = 1$ . However, recall norm is multiplicative, so  $1 = N_{\mathbb{Q}}^K(\alpha) \cdot N_{\mathbb{Q}}^K(\beta)$  where  $N_{\mathbb{Q}}^K(\alpha)$  and  $N_{\mathbb{Q}}^K(\beta)$  are both integers because  $\alpha, \beta$  are algebraic integers. Hence  $N_{\mathbb{Q}}^K(\alpha) = \pm 1$ .

Conversely, say  $N_{\mathbb{Q}}^K(\alpha) = \pm 1$ . Then  $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = \pm 1$ . Let  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$  be all the conjugates of  $\alpha$ . Then the minimal polynomial of  $\alpha$  is  $p(x) = (x - \alpha_1) \dots (x - \alpha_n)$



and we recall that  $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = N^{\mathbb{Q}(\alpha)}(\alpha)$  is just the constant coefficient in the minimal polynomial of  $\alpha$ . Thus, we have  $\alpha_1\alpha_2\ldots\alpha_n = \pm 1$  and this imply  $\alpha_1 = \alpha$  has an inverse of the form  $\mp\alpha_2 \cdot \ldots \cdot \alpha_n$ .

♡

**Remark 2.4.2.** Observe that units in  $\mathbb{A} \cap K$  forms a group and in the following, we are going to study the structure of those groups for quadratic extension.

Recall that  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d}) = \{l + m\sqrt{d} : l, m \in \mathbb{Z}\}$  if  $d \neq 4n + 1$  for some  $n$ . Thus, we have  $\alpha \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  is a units if and only if  $l^2 - dm^2 = \pm 1$ .

On the other hand, if  $d = 4n + 1$  for some  $n$ , then  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  is equal  $\{\frac{l+m\sqrt{d}}{2} : l, m \in \mathbb{Z}, l \equiv m \pmod{2}\}$  and so  $\alpha$  is a unit iff  $l^2 - dm^2 = \pm 4$  when  $l$  and  $m$  are odd.

**Theorem 2.4.3.** *Let  $d$  be a negative square-free integer. The units in  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  are*

1.  $\{1, -1\}$ , if  $d \notin \{-1, -3\}$ .
2.  $\{\pm 1, \pm i\}$  if  $d = -1$ .
3.  $\{\pm 1, \frac{\pm 1 \pm \sqrt{3}}{2}\}$  if  $d = -3$ .

*Proof.* First consider  $d \not\equiv 1 \pmod{4}$ . Then we have  $\alpha = l + m\sqrt{d}$  is a unit iff  $l^2 - dm^2 = \pm 1$ . Since  $d < 1$  we only need to consider  $l^2 - dm^2 = 1$ . If

1.  $d = -1$ , then the solutions are  $(l, m) = (\pm 1, 0)$  or  $(0, \pm 1)$ , which corresponds to  $\{\pm 1, \pm i\}$  as claimed.
2. If  $d < -1$ , the only solution are  $(l, m) = (\pm 1, 0)$  and we are done.

Then, consider  $d \equiv 1 \pmod{4}$ . In this case, we only need to consider  $l^2 - dm^2 = 4$  with  $l, m$  both odd. If

1.  $d = -3$ , then  $l^2 + 3m^2 = 4$  has odd solutions  $(\pm 1, \pm 1)$ , which corresponds to  $\frac{(\pm 1 \pm \sqrt{-3})}{2}$ . Hence, the units are as claimed.
2. If  $d < -3$ , clearly we have no solution and hence the units are  $\pm 1$ .

♡

**Remark 2.4.4.** Next, we are going to establish the structural result of unit group for  $d > 0$ . However, it is a hard question and we need some helps.

**Lemma 2.4.5 (Dirichlet's Theorem).** *Let  $\alpha$  be a real irrational number and  $Q > 1$  be an integer. Then there exists integers  $p, q$  with  $1 \leq q \leq Q$  such that  $|q\alpha - p| < \frac{1}{Q}$ . Furthermore, there exists infinitely many pairs of integers  $(p, q)$  for which  $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$ .*

*Proof.* We prove the first assertion. For any real number  $x$ , let  $\{x\}$  denote the fractional part of  $x$  and  $[x]$  denote the greatest integer less or equal to  $x$ . Then we have  $x = [x] + \{x\}$ .

Now let  $Q$  be given and consider the  $Q + 1$  numbers

$$0, 1, \{\alpha\}, \dots, \{(Q - 1)\alpha\}$$

By the pigeonhole principle there is an integer  $j$  with  $1 \leq j \leq Q$  such that two of the numbers are in the interval  $[(j - 1)/Q, j/Q]$ . Thus, there exists integers  $n$  and  $m$  with  $n \neq m$ ,  $1 \leq m < n \leq Q$  such that  $|\{n\alpha\} - \{m\alpha\}| \leq \frac{1}{Q}$ , or there exists an integer  $n$ ,  $1 \leq n \leq Q$  such that  $|\{n\alpha\} - t| \leq \frac{1}{Q}$  where  $t = 0$  or  $1$ .

In the first case, we have

$$\begin{aligned} |\{n\alpha\} - \{m\alpha\}| &= |(n\alpha - [n\alpha]) - (m\alpha - [m\alpha])| \\ &= |(n - m)\alpha - ([n\alpha] - [m\alpha])| \\ &< \frac{1}{Q} \end{aligned}$$

Pick  $q = n - m$  and  $p = [n\alpha] - [m\alpha]$  and we are done (we remark we have the strict inequality because  $\alpha$  is irrational).

In the second case, pick  $q = n$  and  $p = [n\alpha] + t$  and the result follows.

Now we prove the second assertion by induction. Let  $Q_1 = 2$ , we can find  $(q_1, p_1)$  so that

$$|q_1\alpha - p_1| \leq \frac{1}{2} \leq \frac{1}{q_1}$$

Inductively, assume we have found  $(p_i, q_i)$  for  $1 \leq i \leq n$  such that

$$|q_i\alpha - p_i| \leq \frac{1}{q_i}$$

and  $q_1 < q_2 < q_3 < \dots < q_n$ .

Let  $Q_{n+1}$  be the positive integer such that  $1/Q_{n+1}$  is smaller than any  $|y\alpha - x|$  where  $(x, y) \in \mathbb{N}^2$  with  $1 \leq y \leq q_n$ . By the claim, we can find  $(p_{n+1}, q_{n+1})$  such that

$$|q_{n+1}\alpha - p_{n+1}| < \frac{1}{Q_{n+1}} \leq \frac{1}{q_{n+1}}$$

By our choice of  $Q_{n+1}$  we have  $q_{n+1}$  is greater than  $q_n$  and hence it finishes the second assertion.

♡

**Theorem 2.4.6.** *Let  $d$  be square-free positive integer with  $d > 1$ . Then there exists a smallest unit larger than 1 in  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ , denoted by  $\epsilon$  and are called the **fundamental element/fundamental unit**. Then, the unit group of  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  is*

$$\{(-1)^k \epsilon^j : k \in \{0, 1\}, j \in \mathbb{Z}\}$$

*Proof.* We will first show there exists an integer  $m$  and infinitely many  $\beta \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  for which  $N_{\mathbb{Q}(\sqrt{d})}(\beta) = N(\beta) = m$ . Let  $\theta = p + q\sqrt{d}$  with  $p, q \in \mathbb{Z}, q > 0$ . Then

$$|N(\theta)| = |p + q\sqrt{d}| \cdot |p - q\sqrt{d}| = \left| \frac{p}{q} + \sqrt{d} \right| \cdot \left( q^2 \left| \frac{p}{q} - \sqrt{d} \right| \right)$$

By Dirichlet's theorem 2.4.5, we have infinitely many pairs of  $(p, q)$  for which  $q^2|p/q - \sqrt{d}| < 1$ . For such  $p, q$  and  $\theta = p + q\sqrt{d}$ , we have

$$|N(\theta)| \leq \left| \frac{p}{q} + \sqrt{d} \right| < \left| \frac{p}{q} \right| + \sqrt{d} < (\sqrt{d} + 1) + \sqrt{d} = 2\sqrt{d} + 1$$

Therefore, we have infinitely many  $\theta \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  for which  $|N(\theta)| \leq 2\sqrt{d} + 1$ . As a consequence, there exists an integer  $m$  such that there are infinitely many  $\theta \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  for which  $N(\theta) = m$ . Indeed, observe  $\theta \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  and so  $N(\theta)$  must be integer. Now, consider pigeonhole principle applied to the finite many integers  $1 < 2 < 3 < \dots < k < 2\sqrt{d} + 1$ . Since we have infinitely many  $\theta$  with  $N(\theta) < 2\sqrt{d} + 1$  while they can only be mapped to  $\{1, 2, \dots, k\}$  by the norm function, there must exist  $1 \leq m \leq k$  so infinitely many  $\theta$  satisfies  $N(\theta) = m$ . This establishes our first step.

Furthermore, we can find a set  $\Theta$  with infinitely  $\theta$ 's such that  $\theta \in \Theta \Rightarrow N(\theta) = m$  and  $\theta_1 = p_1 + q_1\sqrt{d}, \theta_2 = p_2 + q_2\sqrt{d} \in \Theta$  then  $p_1 \equiv p_2 \pmod{m}$  and  $q_1 \equiv q_2 \pmod{m}$ . Indeed, note the set with norm equal  $m$ , say  $\{p + q\sqrt{d} : N(p + q\sqrt{d}) = m\}$ , has infinitely many elements while we only have finite many possibilities for  $(p, q) \equiv (i, j) \pmod{m}$  where  $0 \leq i, j \leq m - 1$ . Hence one possible  $(i, j)$  must have infinitely many  $\theta$  with  $p_1 \equiv i \equiv p_2 \pmod{m}$  and  $q_1 \equiv j \equiv q_2 \pmod{m}$ . Thus we get our set  $\Theta$  as desired.

Now, take  $\theta_1 = p_1 + q_1\sqrt{d}, \theta_2 = p_2 + q_2\sqrt{d} \in \Theta$ , we remark we have  $m \mid p_1 - p_2, q_1 - q_2$ . Since the norm is multiplicative, we have

$$N\left(\frac{\theta_1}{\theta_2}\right) = \frac{N(\theta_1)}{N(\theta_2)} = 1$$

Now, let  $\theta'_2$  be the conjugate of  $\theta_2$  over  $\mathbb{Q}$  so that  $N(\theta_2) = \theta_2\theta'_2 = m$ , we get

$$\begin{aligned} \frac{\theta_1}{\theta_2} &= 1 + \frac{\theta_1 - \theta_2}{\theta_2} = 1 + \frac{\theta_1 - \theta_2}{\theta_2\theta'_2} \theta'_2 \\ &= 1 + \left( \underbrace{\left(\frac{p_1 - p_2}{m}\right)}_{in \ \mathbb{Z}} + \underbrace{\left(\frac{q_1 - q_2}{m}\right)}_{in \ \mathbb{Z}} \sqrt{d} \right) \theta'_2 \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d}) \end{aligned}$$

Now, since  $N(\frac{\theta_1}{\theta_2}) = 1$  and  $\frac{\theta_1}{\theta_2} \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ , we have  $\frac{\theta_1}{\theta_2}$  is a unit in  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ . Choose  $\theta_1, \theta_2$  such that  $\frac{\theta_1}{\theta_2} \neq -1$  as if they do then choose other  $\theta_3 \in \Theta$  then one of  $\frac{\theta_1}{\theta_2}, \frac{\theta_2}{\theta_3}, \frac{\theta_3}{\theta_1}$  must be different from  $-1$  as  $\frac{\theta_1}{\theta_2} \cdot \frac{\theta_2}{\theta_3} \cdot \frac{\theta_3}{\theta_1} = 1$ .

Since  $\pm 1$  is the only roots of unity in  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$ , we have found a unit in  $\mathbb{A} \cap \mathbb{Q}(\sqrt{d})$  which is not a root of unity. Consider the set

$$S = \{\gamma \in \mathbb{A} \cap \mathbb{Q}(\sqrt{d}) : \gamma > 0, \gamma \text{ is a unit}\}$$

We have shown that  $S$  contains an element different from 1. Thus, taking inverse if necessary, it contains an element strictly greater than 1.

**Claim** : Let  $\gamma_0$  be an element of  $S$  with  $\gamma_0 > 1$ . Then there are only finitely many elements  $\beta$  in  $S$  such that  $1 < \beta < \gamma_0$ .

First, we observe it is clear that we only have finitely many<sup>1</sup>  $\beta = \frac{a+b\sqrt{d}}{2}$ ,  $a, b \in \mathbb{Z}_{\geq 1}$  such that  $1 < \beta < \gamma_0$ .

Next, we show if  $\gamma = \frac{a+b\sqrt{d}}{2} \in S$  with  $1 < \gamma$  then we must have  $a, b \in \mathbb{Z}_{\geq 1}$ . This will finish our claim because our first observation. Suppose for a contradiction that we have  $ab < 0$ . We can assume  $a \geq 0, b \leq 0$  because if  $a \leq 0, b \geq 0$  then we consider  $\gamma^2 = \frac{(a^2+b^2d)+2ab\sqrt{d}}{4} = \frac{a'+b'\sqrt{d}}{2} \in S$  where now  $a' \geq 0, b' \leq 0$  and  $a'b' < 0$ . Let  $\gamma'$  be the conjugate of  $\gamma$ , i.e.  $\gamma' = \frac{a-b\sqrt{d}}{2} > \gamma$ . Since  $\gamma \in S$  and  $\gamma, \gamma' > 1$ , we have  $N(\gamma) = \gamma \cdot \gamma' > 1$ . This is a contradiction to the fact that  $\gamma$  is a unit. Hence we must have  $a, b$  both positive. This finishes the claim.

This claim immediately imply there exists a smallest element  $\epsilon \in S$  which is strictly greater than 1.

Hence we must have  $S = \{\epsilon^n : n \in \mathbb{Z}\}$ . Indeed, say  $\lambda \in S$  and  $\lambda$  is not a power of  $\epsilon$ , then let  $m$  be so that

$$\epsilon^m < \lambda < \epsilon^{m+1}$$

Observe  $\frac{\lambda}{\epsilon^m} \in S$  and so

$$1 < \frac{\lambda}{\epsilon^m} < \epsilon$$

This contradicts the minimality of  $\epsilon$ .

Finally, the full group of unit is just  $\{\pm\epsilon^n : n \in \mathbb{Z}\}$  as  $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ . ♡

## 2.5 Discriminants

**Remark 2.5.1.** In this part, when we say  $[a_{ij}]_{i,j}$  or  $[a_{ij}]$ , we mean a matrix with  $(i, j)$  entry equal  $a_{ij}$ . When we say  $[a_{ij}]_{(i,j)}$ , we mean the  $(i, j)$  entry of the matrix  $[a_{ij}]_{i,j}$ .

Also, matrix with vertical bar means determinant.

**Definition 2.5.2.** Let  $K$  be a number field of degree  $n$  over  $\mathbb{Q}$  and  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $K$  in  $\mathbb{C}$  fix  $\mathbb{Q}$ . For  $(\alpha_1, \dots, \alpha_n) \in K^n$ , we define the **discriminant** to

---

<sup>1</sup>We remark by consider the possibilities that  $a, b$  divisible by 2, number of the following form includes all algebraic integers

be

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \left( \text{Det}([\sigma_i(\alpha_j)]_{i,j}) \right)^2 = \left| \begin{matrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{matrix} \right|^2$$

**Remark 2.5.3.** Note the way we arrange the  $n$  embeddings does not matter because when we swap two embedding's order, we are swapping the rows of the determinant and that would introduce a negative sign to the determinant. However, we are taking square of the determinant so it is indeed well-defined.

**Theorem 2.5.4.** Let  $K$  be a number field of degree  $n$  over  $\mathbb{Q}$  and  $\alpha_1, \dots, \alpha_n \in K$ . Then

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \text{Det}([T_{\mathbb{Q}}^K(\alpha_i \alpha_j)]_{i,j}) = \left| \begin{matrix} T_{\mathbb{Q}}^K(\alpha_1 \alpha_1) & \dots & T_{\mathbb{Q}}^K(\alpha_1 \alpha_n) \\ \vdots & \ddots & \vdots \\ T_{\mathbb{Q}}^K(\alpha_n \alpha_1) & \dots & T_{\mathbb{Q}}^K(\alpha_n \alpha_n) \end{matrix} \right|^2$$

*Proof.* Let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $K$  in  $\mathbb{C}$  fix  $\mathbb{Q}$ . Then for any  $1 \leq i, j \leq n$  we have

$$\sum_{k=1}^n (\sigma_k(\alpha_i))(\sigma_k(\alpha_j)) = \sum_{k=1}^n (\sigma_k(\alpha_i \alpha_j)) = T_{\mathbb{Q}}^K(\alpha_i \alpha_j)$$

Then, we have

$$\begin{aligned} \text{disc}(\alpha_1, \dots, \alpha_n) &= (\text{Det}([\sigma_i(\alpha_j)]_{i,j}))^2 = \text{Det}([\sigma_k(\alpha_i)]_{k,i}) \cdot \text{Det}([\sigma_k(\alpha_j)]_{k,j}^T) \\ &= \text{Det}([\sigma_k(\alpha_i)]_{k,i} \cdot [\sigma_k(\alpha_j)]_{k,j}^T) = \text{Det} \left( \left[ \sum_{k=1}^n (\sigma_k(\alpha_i))(\sigma_k(\alpha_j)) \right]_{i,j} \right) \\ &= \text{Det}([T_{\mathbb{Q}}^K(\alpha_i \alpha_j)]_{i,j}) \end{aligned}$$

♡

**Corollary 2.5.4.1.** Let  $K$  be a number field of degree  $n$  of  $\mathbb{Q}$  and  $\alpha_1, \dots, \alpha_n \in K$ . Then  $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$ . In particular, if  $\alpha_1, \dots, \alpha_n \in \mathbb{A} \cap K$ , we have  $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}$ .

*Proof.* Note  $T_{\mathbb{Q}}^K(\alpha_i \alpha_j) \in \mathbb{Q}$ , the first assertion follows immediately from definition. Also, since algebraic integers are closed under addition and multiplication, we have  $\alpha_i \alpha_j$  are all algebraic integers. Hence, if  $\alpha_1, \dots, \alpha_n$  are all algebraic integers, we have  $T_{\mathbb{Q}}^K(\alpha_i \alpha_j)$  are all integers. Then the second claim follows by Theorem 2.5.4 as determinant of a matrix with all integer entries is also integer. ♡

**Theorem 2.5.5.** Let  $K$  be a number field of degree  $n$  over  $\mathbb{Q}$  and  $\alpha_1, \dots, \alpha_n \in K$ . Then  $\text{disc}(\alpha_1, \dots, \alpha_n) \neq 0$  if and only if  $\alpha_1, \dots, \alpha_n$  are linearly independent over  $\mathbb{Q}$ .

*Proof.* Note if  $\alpha_j$ 's are linearly dependent over  $\mathbb{Q}$ , then we have  $\sum_{j=1}^n a_j \alpha_j = 0$  for

some non-zero  $a_j \in \mathbb{Q}$ . Let  $v_i = \begin{bmatrix} \sigma_1(\alpha_i) \\ \vdots \\ \sigma_n(\alpha_i) \end{bmatrix}$ , then we have

$$\sum_{j=1}^n a_j v_j = \begin{bmatrix} \sigma_1 \left( \sum_{j=1}^n a_j \alpha_j \right) \\ \vdots \\ \sigma_n \left( \sum_{j=1}^n a_j \alpha_j \right) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Hence,  $a_1, \dots, a_n$  witnesses the linearly dependence of  $v_1, \dots, v_n$  and so the determinant must be 0.

Conversely, we suppose  $\text{disc}(\alpha_1, \dots, \alpha_n) = 0$  and we will show they are linear dependent. In particular, since  $\text{disc}(\alpha_1, \dots, \alpha_n) = 0$ , we must have the rows  $u_i$  of the matrix  $[T_{\mathbb{Q}}^K(\alpha_i \alpha_j)]_{i,j}$  are linear dependent. Hence, there exists  $a_1, \dots, a_n \in \mathbb{Q}$ , not all zero, so  $\sum_{i=1}^n a_i u_i = 0$ .

Now suppose  $\alpha_1, \dots, \alpha_n$  are linearly independent for a contradiction. Consider  $\alpha = \sum_{i=1}^n a_i \alpha_i$ , then we must have  $\alpha \neq 0$  because not all  $a_i$ 's are zero. Moreover, for all  $1 \leq j \leq n$ , by consider only the  $j$ th coordinate of  $\sum_i a_i u_i$ , we have  $T_{\mathbb{Q}}^K(\alpha \alpha_j) = 0$ . Since  $\{\alpha_j : 1 \leq j \leq n\}$  is a basis of  $K$  over  $\mathbb{Q}$ , we have  $\{\alpha \alpha_j : 1 \leq j \leq n\}$  is a basis as well. Therefore, we must have  $\forall \beta \in K$ , there exists  $b_1, \dots, b_n \in \mathbb{Q}$  so  $\beta = \sum_{i=1}^n b_i \alpha \alpha_i$ . Then, we have

$$T_{\mathbb{Q}}^K(\beta) = \sum_{j=1}^n b_j T(\alpha \alpha_j) = 0$$

In particular, when we take  $\beta = 1$ , we get a contradiction as  $T_{\mathbb{Q}}^K(1) = n \neq 0$ .  $\heartsuit$

**Proposition 2.5.6.** *Let  $K$  be number field of degree  $n$  over  $\mathbb{Q}$ . Let  $\{\alpha_i : 1 \leq i \leq n\}$  and  $\{\beta_i : 1 \leq i \leq n\}$  be two bases of  $K$  over  $\mathbb{Q}$ . Suppose  $\beta_k = \sum_{j=1}^n c_{kj} \alpha_j$  where  $c_{kj} \in \mathbb{Q}$ . Then, we have*

$$\text{disc}(\beta_1, \dots, \beta_n) = \text{Det}([c_{ij}])^2 \cdot \text{disc}(\alpha_1, \dots, \alpha_n)$$

*Proof.* Let  $\sigma_1, \dots, \sigma_n$  be all the embeddings of  $K$  to  $\mathbb{C}$  which fix  $\mathbb{Q}$ .

We have

$$\beta_k = [c_{k1} \quad \dots \quad c_{kn}] \cdot \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \Rightarrow \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

Therefore, we have

$$\begin{aligned}
\begin{bmatrix} \sigma_i(\beta_1) \\ \vdots \\ \sigma_i(\beta_n) \end{bmatrix} &= \begin{bmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{bmatrix} \begin{bmatrix} \sigma_i(\alpha_1) \\ \vdots \\ \sigma_i(\alpha_n) \end{bmatrix} \\
\Rightarrow \begin{bmatrix} \sigma_1(\beta_1) & \dots & \sigma_n(\beta_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \dots & \sigma_n(\beta_n) \end{bmatrix} &= \begin{bmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{bmatrix} \cdot \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_n(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{bmatrix} \\
\Rightarrow \left| \begin{bmatrix} \sigma_1(\beta_1) & \dots & \sigma_n(\beta_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \dots & \sigma_n(\beta_n) \end{bmatrix} \right|^2 &= \left| \begin{bmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{bmatrix} \right|^2 \cdot \left| \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_n(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{bmatrix} \right|^2 \\
\Rightarrow \text{disc}(\beta_1, \dots, \beta_n) &= \text{Det}([c_{ij}])^2 \cdot \text{disc}(\alpha_1, \dots, \alpha_n)
\end{aligned}$$

We note the last part is obtained by realizing the determinant of  $[a_{ij}]$  is equal to its transpose and hence the determinants of the matrices on the second line are effectively the same as what we defined for discriminants.  $\heartsuit$

**Theorem 2.5.7.** *Let  $[K : \mathbb{Q}] = n$  and  $K = \mathbb{Q}(\theta)$ . Then  $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$  is a basis of  $K$  over  $\mathbb{Q}$  and*

$$\text{disc}(1, \theta, \dots, \theta^{n-1}) := \text{disc}(\theta) = \left( \prod_{1 \leq i < j \leq n} (\sigma_i(\theta) - \sigma_j(\theta)) \right)^2$$

where  $\sigma_i$ 's are embeddings of  $K$  into  $\mathbb{C}$  fix  $\mathbb{Q}$ . In particular, we have  $\text{disc}(\theta)$  is non-zero and if we let  $f$  be the minimal polynomial of  $\theta$  then

$$\text{disc}(\theta) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^K(f'(\theta))$$

*Proof.* For the first assertion, we observe

$$\text{disc}(\theta) = \left| \begin{bmatrix} \sigma_1(1) & \dots & \sigma_1(\theta^{n-1}) \\ \sigma_2(1) & \dots & \sigma_2(\theta^{n-1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(1) & \dots & \sigma_n(\theta^{n-1}) \end{bmatrix} \right|^2 = \left| \begin{bmatrix} 1 & \sigma_1(\theta) & \dots & \sigma_1(\theta)^{n-1} \\ 1 & \sigma_1(\theta) & \dots & \sigma_2(\theta)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_1(\theta) & \dots & \sigma_n(\theta)^{n-1} \end{bmatrix} \right|^2$$

Observe the above determinant is the determinant of a Vandermonde matrix. Hence, we get

$$\text{disc}(\theta) = \left( \prod_{1 \leq i < j \leq n} (\sigma_i(\theta) - \sigma_j(\theta)) \right)^2$$

Clearly we have  $\text{disc}(\theta)$  is non-zero and hence it is an basis by Theorem 2.5.5.

Now for the final assertion. Let  $\theta = \sigma_1(\theta) = \theta_1, \dots, \sigma_n(\theta) = \theta_n$  be all the conjugates of  $\theta$  over  $\mathbb{Q}$ . Then, the minimal polynomial  $f(x)$  of  $\theta$  is equal

$$f(x) = (x - \theta_1) \dots (x - \theta_n) \Rightarrow f'(x) = \sum_{j=1}^n \prod_{i=1, i \neq j}^n (x - \theta_i)$$

Now, observe

$$N_{\mathbb{Q}}^K(f'(\theta)) = \prod_{k=1}^n \sigma_k(f'(\theta))$$

and observe  $f'(x) \in \mathbb{Q}[x]$  and so  $\sigma_k$  can pass through and we have  $\sigma_k(f'(\theta)) = f'(\sigma_k(\theta)) = f'(\theta_k)$ . Hence

$$N_{\mathbb{Q}}^K(f'(\theta)) = \prod_{k=1}^n f'(\theta_k) = \prod_{k=1}^n \left( \sum_{j=1}^n \prod_{i=1, i \neq j}^n (\theta_k - \theta_i) \right) = \prod_{k=1}^n \left( \prod_{i=1, i \neq k}^n (\theta_k - \theta_i) \right)$$

Then, observe  $(\theta_i - \theta_j)(\theta_j - \theta_i) = -(\theta_i - \theta_j)^2$  and hence we have

$$\begin{aligned} \text{disc}(\theta) &= \left( \prod_{1 \leq i < j \leq n} (\sigma_i(\theta) - \sigma_j(\theta)) \right)^2 \\ &= \left( \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right)^2 = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2 \\ &= \prod_{1 \leq i < j \leq n} (-1)(\theta_i - \theta_j)(\theta_j - \theta_i) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)(\theta_j - \theta_i) \quad \text{See the following for explanation} \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{k=1}^n \left( \prod_{i=1, i \neq k}^n (\theta_k - \theta_i) \right) \\ &= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^K(f'(\theta)) \end{aligned}$$

We note we have the line

$$(-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)(\theta_j - \theta_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{k=1}^n \left( \prod_{i=1, i \neq k}^n (\theta_k - \theta_i) \right)$$

because, if we consider the following



$$\begin{aligned}
\prod_{i < j} (\theta_i - \theta_j)(\theta_j - \theta_i) &= (\theta_n - \theta_{n-1})(\theta_n - \theta_{n-2})(\theta_n - \theta_{n-3}) \dots (\theta_n - \theta_1) \\
&\quad (\theta_{n-1} - \theta_n) (\theta_{n-1} - \theta_{n-2})(\theta_{n-1} - \theta_{n-3}) \dots (\theta_{n-1} - \theta_1) \\
&\quad (\theta_{n-2} - \theta_n) (\theta_{n-2} - \theta_{n-1}) (\theta_{n-2} - \theta_{n-3}) \dots (\theta_{n-2} - \theta_1) \\
&\quad \vdots \\
&\quad (\theta_1 - \theta_n) (\theta_1 - \theta_{n-1}) \dots (\theta_1 - \theta_2) \\
&= \prod_{k=1}^n \left( \prod_{\substack{i=1 \\ i \neq k}}^n (\theta_k - \theta_i) \right)
\end{aligned}$$

In the above, for  $1 \leq i < j \leq n$ , we have the blue part collects all the  $(\theta_i - \theta_j)$  and red part collects all the  $(\theta_j - \theta_i)$ , then if we look at the block of multiplications horizontally, we get our equality as desired.

Hence the proof follows. ♡

**Corollary 2.5.7.1.** *Let  $n$  be a positive integer and  $\zeta_n = e^{2\pi i/n}$ . Then in  $\mathbb{Q}(\zeta_n)$ , we have  $\text{disc}(\zeta_n)$  divides  $n^{\phi(n)}$ . Furthermore, if  $p$  is an odd prime, we have  $\text{disc}(\zeta_p) = (-1)^{\frac{p-1}{2}} p^{p-2}$ .*

*Proof.* Let  $\Phi_n(x)$  be the cyclotomic polynomial, then we have  $\Phi_n(x)$  is the minimal polynomial of  $\zeta_n$ . Observe we have the following factorization

$$x^n - 1 = \Phi_n(x)g(x), g(x) \in \mathbb{Z}[x]$$

Therefore, take derivative at both side, we get

$$nx^{n-1} = \Phi'_n(x)g(x) + \Phi_n(x)g'(x)$$

Now, plug in  $\zeta_n$ , we note  $\Phi_n(\zeta_n) = 0$  and hence we get

$$n\zeta_n^{n-1} = \Phi'_n(\zeta_n)g(\zeta_n) + 0 \cdot g'(\zeta_n) \Rightarrow n\zeta_n^{n-1} = \Phi'_n(\zeta_n)g(\zeta_n)$$

Now, observe  $\zeta_n^{n-1}$  is a unit as  $\zeta_n \cdot \zeta_n^{n-1} = 1$ . Therefore, we have  $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\zeta_n^{n-1}) = \pm 1$ . Thus, denote  $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}$  by  $N$ , we get

$$\begin{aligned}
N(n\zeta_n^{n-1}) &= n^{\phi(n)} \cdot N(\zeta_n^{n-1}) = N(\Phi'_n(\zeta_n)g(\zeta_n)) \\
&= N(\Phi'_n(\zeta_n)) \cdot N(g(\zeta_n)) \\
&= \text{disc}(\zeta_n) \cdot N(g(\zeta_n))
\end{aligned}$$

where  $\phi(n)$  is the Euler phi function. Therefore, we get

$$n^{\phi(n)} = \pm \text{disc}(\zeta_n) \cdot N(g(\zeta_n))$$

where  $N(g(\zeta_n))$  is an integer because  $\zeta_n$  is algebraic integer and  $g(x) \in \mathbb{Z}[x]$ . Hence we get our first assertion that  $\text{disc}(\zeta_n) \mid n^{\phi(n)}$ .

Now, let  $n = p$  where  $p$  is an odd prime number. Then we have  $x^p - 1 = \Phi_p(x)(x - 1)$  as  $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + 1$ . Therefore, taking derivative of  $x^p - 1 = \Phi_p(x)(x - 1)$  and plug in  $\zeta_p$  we obtain  $p\zeta_p^{p-1} = \Phi'_p(\zeta_p)(\zeta_p - 1)$  and multiply both side by  $\zeta_p$  we get

$$p = \zeta_p \Phi'_p(\zeta_p)(\zeta_p - 1)$$

Now take norm on both side, we get

$$N(p) = N(\zeta_p) \cdot N(\Phi'_p(\zeta_p)) \cdot N(\zeta_p - 1)$$

Let us compute term by term:

1. We have  $N(p) = p^{\phi(p)} = p^{p-1}$ .
2. For  $N(\zeta_p)$ , note  $N(\zeta_p) = \zeta_p \cdot \zeta_p^2 \dots \zeta_p^{p-1} = e^{\frac{2\pi i}{p} \cdot \frac{p(p-1)}{2}} = e^{(p-1)\pi i} = 1$  as  $p$  is odd.
3.  $N(\Phi'_p(\zeta_p)) = (-1)^{\frac{\phi(p)(\phi(p)-1)}{2}} \text{disc}(\zeta_p)$ . Now, note  $p$  is odd and we have  $\phi(p) = p - 1$ , we have  $(-1)^{\frac{\phi(p)(\phi(p)-1)}{2}} = (-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{p-2}{2}}$  because  $(-1)^{p-1}$  is just equal 1. Therefore, we get  $N(\Phi'_p(\zeta_p)) = (-1)^{\frac{p-2}{2}} \text{disc}(\zeta_p)$ .
4.  $N(\zeta_p - 1) = \prod_{i=1}^{p-1} \sigma_i(\zeta_p - 1)$  where  $\sigma_i$ 's are all the embeddings from  $\mathbb{Q}(\zeta_p)$  to  $\mathbb{C}$  fixes  $\mathbb{Q}$ . In particular, it sends  $\zeta_p$  to  $\zeta_p^i$ . Hence, we get  $N(\zeta_p - 1) = \prod_{i=1}^{p-1} (\zeta_p^i - 1) = (-1)^{p-1} \prod_{i=1}^{p-1} (1 - \zeta_p^i) = \Phi_p(1) = p$  as  $p$  is odd and we note  $\Phi_p(1) = (1 - \zeta_p)(1 - \zeta_p^2) \dots (1 - \zeta_p^{p-1}) = 1^{p-1} + \dots + 1^1 + 1 = p$ .

Therefore, we get

$$p^{p-1} = 1 \cdot (-1)^{\frac{p-2}{2}} \text{disc}(\zeta_p) \cdot p \Rightarrow \text{disc}(\zeta_p) = \frac{p^{p-1}}{(-1)^{\frac{p-2}{2}} p} = (-1)^{\frac{p-2}{2}} p^{p-2}$$

♡

## 2.6 Integral Bases

**Definition 2.6.1.** Let  $K$  be finite extension of  $\mathbb{Q}$ . A set of algebraic integers  $\{\alpha_1, \dots, \alpha_n\}$  is said to be an **integral basis** for  $K$  over  $\mathbb{Q}$  if every  $\gamma \in \mathcal{O}_K := \mathbb{A} \cap K$  has a unique representation of the form  $\gamma = \sum_{i=1}^n m_i \alpha_i$  with  $m_i \in \mathbb{Z}$ .

**Remark 2.6.2.** Note an integral basis  $\{\alpha_1, \dots, \alpha_n\}$  of  $K$  over  $\mathbb{Q}$  is indeed a basis of  $K$  over  $\mathbb{Q}$ . Given  $\theta \in K$ , by Theorem 2.1.7 there exists positive integer  $r$  such that  $r\theta \in \mathcal{O}_K$ . Therefore  $K$  is in the span of  $\{\alpha_1, \dots, \alpha_n\}$  and since the representations are unique, we get the linear independence.

**Theorem 2.6.3.** Let  $K$  be a number field, then  $K$  admits an integral basis.

*Proof.* Let  $\theta$  be an algebraic integer such that  $K = \mathbb{Q}(\theta)$ . Consider the set of all bases for  $K$  over  $\mathbb{Q}$  as a vector space, whose elements are algebraic integers. Observe this set is not empty because it contains the basis  $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$  where  $n = [K : \mathbb{Q}]$ . The discriminant of the bases in the set are integers since it consists of only algebraic integers. Hence the absolute values in the discriminants are non-zero positive integers as discriminants of bases are not zero.

Choose a basis  $\{\omega_1, \dots, \omega_n\}$  for which  $|\text{disc}(\omega_1, \dots, \omega_n)|$  is minimal, we will show it is an integral basis.

Suppose it is not an integral basis. Then there exists  $\gamma \in \mathbb{A} \cap K$  such that  $\gamma = \sum_{i=1}^n a_i \omega_i$  but with not all  $a_i$ 's are in  $\mathbb{Z}$ . Without loss of generality, suppose  $a_1$  is not integer. Then  $a_1 = a + r$  where  $a \in \mathbb{Z}$  and  $0 < r < 1$ .

Now, define  $\omega_1^* = \gamma - a\omega_1$  and  $\omega_i^* = \omega_i$  for  $2 \leq i \leq n$ . Then we note  $\{\omega_i^* : 1 \leq i \leq n\}$  forms a basis of  $K$  consists of algebraic integers. Then we get

$$\begin{aligned} \text{disc}(\omega_1^*, \dots, \omega_n^*) &= \begin{vmatrix} a_1 - a & a_2 & \dots & a_n \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{vmatrix}^2 \cdot \text{disc}(\omega_1, \dots, \omega_n) \\ &= (a_1 - a)^2 \cdot \text{disc}(\omega_1, \dots, \omega_n) = r^2 \cdot \text{disc}(\omega_1, \dots, \omega_n) \\ &< \text{disc}(\omega_1, \dots, \omega_n) \end{aligned}$$

This contradicts the minimality of  $\text{disc}(\omega_1, \dots, \omega_n)$  and hence proof follows.  $\heartsuit$

**Theorem 2.6.4.** *Let  $K$  be a number field. Then all integral bases for  $K$  over  $\mathbb{Q}$  have the same discriminant.*

*Proof.* Let  $\alpha = (\alpha_1, \dots, \alpha_n)$  and  $\beta = (\beta_1, \dots, \beta_n)$  be two integral basis. Then we have two integer matrices  $A, B \in M_n(\mathbb{Z})$  so that  $\alpha^T = A\beta^T$  and  $\beta^T = B\alpha^T$ . Then we have  $AB = I_n$  is the identity matrix and hence  $\det(A) \cdot \det(B) = 1$ . This forces  $\det(A)$  and  $\det(B)$  to be  $\pm 1$  as those are integer matrices.

Thus, by Proposition 2.5.6 we get  $\text{disc}(\alpha) = (\det(A))^2 \text{disc}(\beta) = \text{disc}(\beta)$ .  $\heartsuit$

**Definition 2.6.5.** Let  $K$  be a number field, then the **discriminant of  $K$**  is the discriminant of an integral basis of  $K$ .

**Example 2.6.6.** Let  $d$  be square-free integer, let us compute discriminant of  $\mathbb{Q}(\sqrt{d})$ .

If  $d \not\equiv 1 \pmod{4}$ , then  $\{1, \sqrt{d}\}$  is an integral basis and therefore we have

$$\text{disc}(\mathbb{Q}(\sqrt{d})) = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d$$

If  $d \equiv 1 \pmod{4}$  then  $\{1, \frac{1+\sqrt{d}}{2}\}$  is an integral basis and so we get

$$\text{disc}(\mathbb{Q}(\sqrt{d})) = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d$$

**Example 2.6.7.** Let  $K$  be a number field with  $[K : \mathbb{Q}] = n$  and  $\{\omega_1, \dots, \omega_n\} \subseteq \mathcal{O}_K$ . Then  $\text{disc}(\omega_1, \dots, \omega_n)$  is square-free number imply  $\text{disc}(\omega_1, \dots, \omega_n) = \text{disc}(K)$ .

Indeed, suppose  $\omega = (\omega_1, \dots, \omega_n)$  is not a integral basis. Then let  $\alpha = (\alpha_1, \dots, \alpha_n)$  be a integral basis. We have  $\omega^T = A \cdot \alpha^T$  where  $A \in M_n(\mathbb{Z})$  is an integer matrix. In particular, we would have  $\text{disc}(\omega) = |A|^2 \cdot \text{disc}(\alpha)$ . By definition of squarefree integer, we must have  $|A| = \pm 1$  and hence  $\text{disc}(\omega) = \text{disc}(K)$  as desired.

**Example 2.6.8.** Let  $K$  be a number field with  $[K : \mathbb{Q}] = n$ .

Then we let  $\{\theta_1, \theta_2, \theta_3, \dots, \theta_n\}$  be a basis of  $K$  with all elements in  $\mathcal{O}_K$ . Note this may not be an integral basis even they are all in  $\mathcal{O}_K$ . However, there always exists an integral basis by Theorem 2.6.3, say  $\{\alpha_1, \dots, \alpha_n\}$ . By the definition of integral basis, we would have

$$\begin{bmatrix} \theta_1 \\ \vdots \\ \theta_n \end{bmatrix} = A \cdot \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

Now, suppose  $\text{disc}(\theta_1, \dots, \theta_n)$  has the following prime factorization

$$\text{disc}(\theta_1, \dots, \theta_n) = \prod_{i=1}^m p_i^{k_i}$$

On the other hand, we would have

$$\text{disc}(\theta) = \det(A)^2 \cdot \text{disc}(K)$$

Hence, we have  $\text{disc}(K)$  must divide  $\prod_{i=1}^m p_i^{k_i}$ . In other word,  $\text{disc}(K)$  must be divisible by at least one of  $p_i$ 's.

Hence, if we can find a basis of  $K$  in  $\mathcal{O}_K$ , then  $\text{disc}(K)$  will be limited to a set of values. For example, let  $\theta$  be a root of the irreducible polynomial  $f(x) = x^3 + x^2 - 2x + 8$ , then we would have<sup>1</sup>  $\text{disc}(\theta) = -2012 = -4 \cdot 503$ . Therefore, let  $K = \mathbb{Q}(\theta)$ , then we must have  $\text{disc}(K)$  be in the set  $\{-4, -2, -503, -2012\}$ . Observe we keep the negative because  $\det(A)^2$  in our above argument is always positive while we have  $\det(A)^2 \cdot \text{disc}(K) = -2012$ . Also, we cannot have  $\text{disc}(K) = -2$  because  $2 \cdot 503$  is not a perfect square. Hence, we have  $\text{disc}(K) \in \{-4, -503, -2012\}$ .

**Definition 2.6.9.** Let  $K$  be a number field of degree  $n$  over  $\mathbb{Q}$ . Suppose that  $\lambda \in \mathcal{O}_K$  and  $\{1, \lambda, \lambda^2, \dots, \lambda^{n-1}\}$  is an integral basis of  $K$ . Then we say  $\{1, \lambda, \dots, \lambda^{n-1}\}$  is an *power basis*.

**Remark 2.6.10.** Not all number fields admits power bases. For an example, you have to wait until Example 2.8.7 when we introduce resultants.

<sup>1</sup>The calculation of this value  $\text{disc}(\theta)$  can be found in Example 2.8.7 using resultants

**Remark 2.6.11.** Next, we are going to prove that if  $p$  is prime, we have  $\mathcal{O}_{\mathbb{Z}[\zeta_{p^r}]} = \mathbb{Z}[\zeta_{p^r}]$  for any positive integer  $r$ .

**Theorem 2.6.12.** Let  $K$  be a number field of degree  $n$  and  $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathcal{O}_K$  a basis of  $K$  over  $\mathbb{Q}$ . Let  $d = \text{disc}(\alpha_1, \dots, \alpha_n)$ . Then every  $\alpha \in \mathcal{O}_K$  can be expressed in the form

$$\frac{m_1\alpha_1 + \dots + m_n\alpha_n}{d}$$

where  $m_i \in \mathbb{Z}$  and  $d \mid m_i^2$  for all  $1 \leq i \leq n$ .

*Proof.* Write  $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n$  with  $x_i \in \mathbb{Q}$ . Let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $K$  in  $\mathbb{C}$  which fix  $\mathbb{Q}$ . Consider the system of equations

$$\begin{cases} \sigma_1(\alpha) = x_1\sigma_1(\alpha_1) + \dots + x_n\sigma_1(\alpha_n) \\ \sigma_2(\alpha) = x_1\sigma_2(\alpha_1) + \dots + x_n\sigma_2(\alpha_n) \\ \vdots \\ \sigma_n(\alpha) = x_1\sigma_n(\alpha_1) + \dots + x_n\sigma_n(\alpha_n) \end{cases} \Rightarrow \begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Solving for  $x_j$  using Cramer's rule, we get  $x_j = \frac{Y_j}{\delta}$  where

$$\delta = \begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{vmatrix}$$

and  $Y_j$  is the determinant of the matrix in  $\delta$  with  $j$ th column changed to  $(\sigma_1(\alpha), \dots, \sigma_n(\alpha))^T$ , i.e. we have

$$Y_j = \begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_{j-1}) & \sigma_1(\alpha) & \sigma_1(\alpha_{j+1}) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_{j-1}) & \sigma_2(\alpha) & \sigma_2(\alpha_{j+1}) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_{j-1}) & \sigma_n(\alpha) & \sigma_n(\alpha_{j+1}) & \dots & \sigma_n(\alpha_n) \end{vmatrix}$$

We observe that both  $\delta$  and  $Y_j$  are algebraic integers and  $\delta^2 = d = \text{disc}(\alpha_1, \dots, \alpha_n)$ . Thus, we have  $dx_j = \delta Y_j \in \mathbb{A}$  where  $d \in \mathbb{Z}$  and  $x_j \in \mathbb{Q}$ . Hence we have  $dx_j \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$ . Therefore, let  $dx_j = m_j \in \mathbb{Z}$ , we finishes our first assertion and remain to show  $d \mid m_j^2$ .

Observe  $\frac{m_j^2}{d} = Y_j^2 \in \mathbb{A}$  and  $\frac{m_j^2}{d} \in \mathbb{Q}$ , we have  $\frac{m_j^2}{d} \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$  and thus  $d \mid m_j^2$  as desired.  $\heartsuit$

## 2.7 Structure Theorem of $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$

**Lemma 2.7.1.** For  $n \geq 3$ , we have  $\mathbb{Z}[1 - \zeta_n] = \mathbb{Z}[\zeta_n]$  and  $\text{disc}(1 - \zeta_n) = \text{disc}(\zeta_n)$ .

*Proof.* Observe  $1 \in \mathbb{Z}[1 - \zeta_n]$  and so  $-(1 - \zeta_n) + 1 \in \mathbb{Z}[1 - \zeta_n]$ , i.e.  $\zeta_n \in \mathbb{Z}[1 - \zeta_n]$ . On the other hand we have  $1 - \zeta_n \in \mathbb{Z}[\zeta_n]$ . Therefore,  $\mathbb{Z}[1 - \zeta_n] = \mathbb{Z}[\zeta_n]$  as desired.

On the other hand, observe  $\mathbb{Q}(\zeta_n) = \mathbb{Q}(1 - \zeta_n)$  with the same reasoning as above. In particular, let  $\sigma_1, \dots, \sigma_k$  be all the embeddings of  $\mathbb{Q}(\zeta_n)$  to  $\mathbb{C}$  fix  $\mathbb{Q}$  where  $k = \phi(n)$ . Then we have both  $\{1, \zeta_n, \dots, \zeta_n^{k-1}\}$  and  $\{1, 1 - \zeta_n, \dots, (1 - \zeta_n)^{k-1}\}$  are basis of  $\mathbb{Q}(\zeta_n)$ . Hence, we have

$$\begin{aligned} \text{disc}(\zeta_n) &= \left( \prod_{1 \leq i < j \leq k} (\sigma_i(\zeta_n) - \sigma_j(\zeta_n)) \right)^2 \\ &= \left( \prod_{1 \leq i < j \leq k} (-1)(1 - \sigma_i(\zeta_n) - 1 + \sigma_j(\zeta_n)) \right)^2 \\ &= \left( \prod_{1 \leq i < j \leq k} (-1) \left( \sigma_i(1) - \sigma_i(\zeta_n) - (\sigma_j(1) - \sigma_j(\zeta_n)) \right) \right)^2 \\ &= \left( \prod_{1 \leq i < j \leq k} (-1) \left( \sigma_i(1 - \zeta_n) - \sigma_j(1 - \zeta_n) \right) \right)^2 \\ &= \left( \prod_{1 \leq i < j \leq k} \left( \sigma_i(1 - \zeta_n) - \sigma_j(1 - \zeta_n) \right) \right)^2 = \text{disc}(1 - \zeta_n) \end{aligned}$$

♡

**Lemma 2.7.2.** For  $n \geq 1$  we have  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ . In particular, we have

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

*Proof.* For the first assertion we note  $a_0^n - 1 = 0$  imply  $a_0 = \zeta_n^k$  where  $0 \leq k \leq n$ . Hence  $a_0 = e^{\frac{2\pi i k}{n}} = e^{\frac{2\pi i t}{d}}$  where  $\gcd(t, d) = 1$  and  $d \mid n$ , i.e. we divide both numerator and denominator by  $\gcd(k, n)$ . Hence  $a_0 = \zeta_d^t$  is a root of  $\Phi_d(x)$  since  $\gcd(t, d) = 1$ . On the other hand, every root of  $\Phi_d(x)$  where  $d \mid n$  is clearly a root of  $x^n - 1$ . Thus the proof follows.

The second assertion follows trivially from the first assertion.

♡

**Lemma 2.7.3.** For  $p$  prime and  $r \geq 1$  we have

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}$$

*Proof.* We use induction. Observe if  $r = 1$  the case holds. Now suppose it holds for all values  $k$  such that  $k < r$ .

Let  $n = p^r$  and apply the lemma above we see  $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}$  with  $d \mid n$  if and only if  $d = p^k$  where  $k \leq r$ . Hence by induction hypothesis we get

$$\begin{aligned}\Phi_n(x) &= \frac{x^{p^r} - 1}{(x - 1) \left(\frac{x^{p^1} - 1}{x - 1}\right) \left(\frac{x^{p^2} - 1}{x^{p^1} - 1}\right) \cdots \left(\frac{x^{p^{r-1}} - 1}{x^{p^{r-2}} - 1}\right)} \\ &= \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}\end{aligned}$$

♡

**Lemma 2.7.4.** For  $n = p^r$  where  $p$  is prime and  $r > 0$ , we have

$$\Phi_n(1) = \prod_{p \nmid k, 1 \leq k \leq n} (1 - \zeta_n^k) = p$$

*Proof.* Since  $n = p^r$  we have  $\Phi_n(x)(x^{p^{r-1}} - 1) = x^n - 1$  with  $g(x) := x^{p^{r-1}} - 1$ . In particular, take derivative we get  $n x^{n-1} = \Phi'_n(x)g(x) + \Phi_n(x)g'(x)$  and so we have

$$n \cdot 1 = p^r = \Phi'_n(1) \cdot 0 + \Phi_n(1)g'(1)$$

Observe  $g'(x) = p^{r-1}x^{p^{r-1}-1}$  and so indeed we have

$$\Phi_n(1) = p$$

♡

**Theorem 2.7.5.** Let  $\zeta_n = e^{\frac{2\pi i}{n}}$  where  $n = p^r$  for some prime  $p$  and  $K = \mathbb{Q}(\zeta_n)$ . Then  $\mathcal{O}_K = \mathbb{A} \cap \mathbb{Q}(\zeta_n) = \mathbb{Z}[\zeta_n]$ , i.e.  $K$  has a power basis  $\{1, \zeta_n, \dots, \zeta_n^{\phi(n)-1}\}$ .

*Proof.* First observe  $\{1, \zeta_n, \dots, \zeta_n^{\phi(n)-1}\}$  is a basis of  $K$  as  $K = \mathbb{Q}(\zeta_n)$ . However, we have  $\text{disc}(\zeta_n) = \text{disc}(1 - \zeta_n)$  by Lemma 2.7.1 and so  $\{1, 1 - \zeta_n, \dots, (1 - \zeta_n)^{\phi(n)-1}\}$  is also a basis of  $K$ .

Let  $l = \phi(n)$ . By Theorem 2.6.12 we know every  $\alpha \in \mathcal{O}_K$  can be expressed in the form

$$\alpha = \frac{m_1 + m_2(1 - \zeta_n) + \dots + m_l(1 - \zeta_n)^{l-1}}{d}$$

where  $d = \text{disc}(\zeta_n) = \text{disc}(1 - \zeta_n)$  and  $m_1, \dots, m_l \in \mathbb{Z}$  with  $d \mid m_i^2$ . Also, we have  $\text{disc}(\zeta_n) \mid n^l = p^{rl}$  by Corollary 2.5.7.1. Thus we have  $d = \text{disc}(\zeta_n)$  is a power of prime  $p$ .

Now suppose for a contradiction we have  $\mathcal{O}_K \neq \mathbb{Z}[\zeta_n] = \mathbb{Z}[1 - \zeta_n]$ , then we can find  $\alpha \in \mathcal{O}_K$  for which not all  $m_i$  are divisible by  $d$  (because if every element's  $m_i$ 's are divisible by  $d$  then we get integer coefficients and so every element is in  $\mathbb{Z}[\zeta_n]$ ).

In other word, we have

$$\alpha' = \frac{m'_1 + m'_2(1 - \zeta_n) + \dots + m'_l(1 - \zeta_n)^{l-1}}{d}$$

with at least one  $m_i$  not divisible by  $d = p^T$  for some  $T$ . Then we can factor out all the common factors of  $p$  from numerator and denominator and get

$$\alpha' = \frac{m_1 + m_2(1 - \zeta_n) + \dots + m_l(1 - \zeta_n)^{l-1}}{p^t}$$

for some  $m_1, \dots, m_l$  and  $t$  where  $p \nmid \gcd(m_1, \dots, m_l)$ , i.e. we cannot factor out any more  $p$  from all of  $m_1, \dots, m_l$  at once.

Then, consider

$$\alpha'' := p^{t-1}\alpha' = \frac{m_1 + m_2(1 - \zeta_n) + \dots + m_l(1 - \zeta_n)^{l-1}}{p} \in \mathcal{O}_K$$

where we observe that we have at least one  $m_i$  that is not divisible by  $p$  because if all  $m_i$ 's are divisible by  $p$ , then we can still factor out a  $p$  from the top, which is a contradiction. Now, let  $i$  be the smallest in the sense that  $m_1, \dots, m_{i-1}$  are all divisible by  $p$  and  $m_i$  is not. Then we let

$$\alpha = \alpha'' - \frac{m_1 + m_2(1 - \zeta_n) + \dots + m_{i-1}(1 - \zeta_n)^{i-2}}{p} \in \mathcal{O}_K$$

Thus we have

$$\alpha = \frac{m_i(1 - \zeta_n)^{i-1} + \dots + m_l(1 - \zeta_n)^{l-1}}{p} \in \mathcal{O}_K, p \nmid m_i$$

Now, observe  $(1 - x)$  divides  $1 - x^k$  as we recall  $x^k - 1 = (x - 1)(1 + x + x^2 + \dots + x^{k-1})$  so we have  $1 - \zeta_n^k = (1 - \zeta_n)\beta_k$  where  $\beta_k = (1 + \zeta_n + \zeta_n^2 + \dots + \zeta_n^{k-1}) \in \mathbb{Z}[\zeta_n]$  and this works for all  $k$ . In particular, we would have

$$\prod_{p \nmid k, 1 \leq k \leq n} (1 - \zeta_n^k) = p = \prod_{p \nmid k, 1 \leq k \leq n} (1 - \zeta_n)\beta_k$$

Note we would have  $\phi(n) = l$  many copies of  $(1 - \zeta_n)$  multiply together and so by Lemma 2.7.4 we have

$$p = (1 - \zeta_n)^l \beta, \beta = \prod_k \beta_k \in \mathbb{Z}[\zeta_n] \Rightarrow \frac{p}{(1 - \zeta_n)^l} \in \mathbb{Z}[\zeta_n]$$

Therefore, we have

$$\frac{p}{(1 - \zeta_n)^l} \in \mathbb{Z}[\zeta_n] \Rightarrow \frac{p}{(1 - \zeta_n)^i} \in \mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_K$$

as we have  $(1 - \zeta_n)^{l-i} \in \mathbb{Z}[\zeta_n]$  and so  $(1 - \zeta_n)^{l-i} \cdot \frac{p}{(1 - \zeta_n)^l} = \frac{p}{(1 - \zeta_n)^i} \in \mathbb{Z}[\zeta_n]$ .

In particular, this imply

$$\begin{aligned} \frac{p\alpha}{(1 - \zeta_n)^i} &= \frac{m_i}{(1 - \zeta_n)} + \frac{m_{i+1}(1 - \zeta_n)^i}{(1 - \zeta_n)^i} + \frac{m_{i+2}(1 - \zeta_n)^{i+1}}{(1 - \zeta_n)^i} + \dots + \frac{m_l(1 - \zeta_n)^{l-1}}{(1 - \zeta_n)^i} \\ &= \frac{m_i}{1 - \zeta_n} + m_{i+1} + m_{i+1}(1 - \zeta_n) + \dots + m_l(1 - \zeta_n)^{l-1-i} \end{aligned}$$



Now, move the terms we get

$$\frac{m_i}{1 - \zeta_n} = \frac{p\alpha}{(1 - \zeta_n)^i} - (m_{i+1} + \dots + m_l(1 - \zeta_n)^{l-1-i}) \in \mathcal{O}_K$$

as both  $\frac{p\alpha}{(1 - \zeta_n)^i}$  and  $m_{i+1} + \dots + m_l(1 - \zeta_n)^{l-1-i}$  are elements of  $\mathcal{O}_K$ .

However, this imply

$$N_{\mathbb{Q}}^K\left(\frac{m_i}{1 - \zeta_n}\right) = \frac{N_{\mathbb{Q}}^K(m_i)}{N_{\mathbb{Q}}^K(1 - \zeta_n)} \in \mathbb{Z}$$

where  $N_{\mathbb{Q}}^K(1 - \zeta_n) = p$  by Lemma 2.7.4 as we recall  $N_{\mathbb{Q}}^K(1 - \zeta_n) = \prod \sigma_i(1 - \zeta_n) = \prod (1 - \sigma(\zeta_n))$  where  $\sigma_i$  are all the embeddings, namely  $\sigma(\zeta_n) = \zeta_n^i$  for  $i \nmid n$  which happens if and only if  $p$  does not divide  $i$ , i.e. we have  $N_{\mathbb{Q}}^K(1 - \zeta_n) = \prod_{p \nmid k, 1 \leq k \leq n} (1 - \zeta_n^k) = p$ .

Hence, we have  $N_{\mathbb{Q}}^K(m_i)$  is divisible by  $p$ , where  $m_i \in \mathbb{Z}$  so  $N_{\mathbb{Q}}^K(m_i) = m_i^l$ . Therefore, we have  $p \mid m_i^l$  and so  $p$  divides  $m_i$ . This is a contradiction and the proof follows.

♡

**Remark 2.7.6.** By the above theorem we could obtain in general that  $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$  where  $K = \mathbb{Q}(\zeta_n)$  for all  $n \in \mathbb{Z}_{\geq 1}$ . However, to do this, we need to define what a compositum is.

**Definition 2.7.7.** Let  $K$  and  $L$  be number fields. Define the *compositum field* (or *composition field*)  $KL$  of  $K$  and  $L$  as follows:

$$KL = \left\{ \sum_{i=1}^r \alpha_i \beta_i : r \in \mathbb{Z}_{\geq 1}, \alpha_i \in K, \beta_i \in L \right\}$$

**Definition 2.7.8.** Let  $\mathcal{O}_K, \mathcal{O}_L$  be ring of integers of  $K$  and  $L$ , respectively. Then we define

$$\mathcal{O}_K \mathcal{O}_L = \left\{ \sum_{i=1}^r \alpha_i \beta_i : r \in \mathbb{Z}_{\geq 1}, \alpha_i \in \mathcal{O}_K, \beta_i \in \mathcal{O}_L \right\}$$

**Remark 2.7.9.** Note  $\mathcal{O}_K \mathcal{O}_L \subseteq \mathcal{O}_{KL}$  by definition.

**Theorem 2.7.10.** Let  $K$  be a number field of degree  $n$  and  $L$  be of degree  $m$ , and  $d = \gcd(\text{disc}(K), \text{disc}(L))$ . Assume  $[KL : \mathbb{Q}] = nm$ , then we have

$$\mathcal{O}_{KL} \subseteq \frac{1}{d} \mathcal{O}_K \mathcal{O}_L$$

*Proof.* Let  $\alpha = (\alpha_1, \dots, \alpha_n)$  and  $\beta = (\beta_1, \dots, \beta_m)$  be integral bases of  $K$  and  $L$  respectively. Then  $\delta = \{\alpha_i \beta_j : 1 \leq i \leq n, 1 \leq j \leq m\}$  is a basis of  $\mathcal{O}_K \mathcal{O}_L$ . Thus, it is a basis of  $KL$  over  $\mathbb{Q}$  since the dimensions are equal while  $\mathcal{O}_K \mathcal{O}_L \subseteq KL$ .

Now, by Theorem 2.6.12 any  $\gamma \in \mathcal{O}_{KL}$  can be expressed in the form

$$\begin{aligned}\gamma &= \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \frac{M_{ij}}{\text{disc}(\delta)} \alpha_i \beta_j \\ \Rightarrow \gamma &= \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \frac{m_{ij}}{r} \alpha_i \beta_j, \quad \gcd(r, \gcd(\{m_{ij} : 1 \leq i \leq n, 1 \leq j \leq m\})) = 1\end{aligned}$$

where we obtained the second line by factor out common factors of numerator and denominator in the first line's expression.

We have to show  $r \mid d$  and it suffice to show  $r \mid \text{disc}(K)$  as  $r \mid \text{disc}(L)$  will follow by symmetry.

Let  $K = \mathbb{Q}(\theta)$  and  $L = \mathbb{Q}(\omega)$  with  $\theta_1, \dots, \theta_n$  (resp.  $\omega_1, \dots, \omega_m$ ) be the conjugates of  $\theta$  (resp.  $\omega$ ). Any embedding  $\sigma$  of  $KL$  into  $\mathbb{C}$  fix  $\mathbb{Q}$  is uniquely determined<sup>1</sup> by  $\sigma(\theta) = \theta_{i_\sigma}$  and  $\sigma(\omega) = \omega_{j_\sigma}$  where  $1 \leq i_\sigma \leq n$  and  $1 \leq j_\sigma \leq m$ . Since  $[KL : \mathbb{Q}] = nm$ , there is one-to-one correspondence between the embeddings of  $KL$  into  $\mathbb{C}$  fix  $\mathbb{Q}$  and the ordered pairs  $(i, j)$  where  $1 \leq i \leq n$ ,  $1 \leq j \leq m$ . In particular, we can find embeddings  $\sigma_1, \dots, \sigma_n$  of  $KL$  into  $\mathbb{C}$  fixing  $\mathbb{Q}$  such that

$$\sigma_k(\theta) = \theta_k, \sigma_i(\omega) = \omega$$

Viz, we have  $\sigma_i$ 's fix  $L$ .

Now consider

$$\sigma_k(\alpha) = \sum_{i,j} \frac{m_{ij}}{r} \sigma_k(\alpha_i) \beta_j$$

and we let

$$x_i = \sum_j \frac{m_{ij}}{r} \beta_j$$

and thus we obtain

$$\begin{bmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

Solve  $x_i$  using Cramer's rule, we obtain  $x_i = \frac{Y_i}{\Delta}$  where  $\Delta = \det([\sigma_k(\alpha_i)]_{k,i})$  and

$$\begin{array}{ccccc} \text{1th} & \dots & \text{ith} & \dots & \text{nth} \\ Y_i = & \left| \begin{array}{ccccc} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha) & \dots & \sigma_n(\alpha_n) \end{array} \right| \end{array}$$

---

<sup>1</sup>as we recall in the proof of Theorem 2.3.9

As before, we have  $\Delta, Y_i \in \mathbb{A}$  with  $\Delta^2 = \text{disc}(K) =: e$ . Then

$$ex_i = \Delta Y_i = \sum_{j=1}^m \frac{em_{ij}}{r} \beta_j \in \mathbb{A} \cap L = \mathcal{O}_L$$

Since  $\beta$  is an integral basis of  $L$  where  $ex_i \in \mathcal{O}_L$ , we must have  $em_{ij}/r \in \mathbb{Z}$  for all  $i, j$  by the definition of integral basis and so  $r \mid \gcd(em_{ij})$  where  $\gcd(em_{ij}) = e \cdot \gcd(m_{ij})$ . Since  $r \nmid \gcd(m_{ij})$  we have  $r \mid e = \text{disc}(K)$  and the proof follows.  $\heartsuit$

**Corollary 2.7.10.1.** *Let  $K, L$  be number fields with degree  $n$  and  $m$  respectively. Suppose  $\gcd(\text{disc}(K), \text{disc}(L)) = 1$  and  $[KL : \mathbb{Q}] = nm$ . Then we have  $\mathcal{O}_K \mathcal{O}_L = \mathcal{O}_{KL}$  and*

$$\text{disc}(KL) = \text{disc}(K)^m \text{disc}(L)^n$$

*Proof.* Note  $\mathcal{O}_K \mathcal{O}_L \subseteq \mathcal{O}_{KL}$  and by Theorem 2.7.10 we have  $\mathcal{O}_{KL} \subseteq \frac{1}{d} \mathcal{O}_K \mathcal{O}_L$  where  $d = \gcd(\text{disc}(K), \text{disc}(L))$ . Hence  $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$  as desired.

For the second claim, we note if  $\alpha = \{\alpha_1, \dots, \alpha_n\}$  is an integral basis of  $K$  and  $\beta = \{\beta_1, \dots, \beta_m\}$  is an integral basis of  $L$ , we have  $\delta = \{\alpha_i \beta_j : 1 \leq i \leq n, 1 \leq j \leq m\}$  is a basis of  $KL$ . However, since  $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$ , we have  $\delta$  is an integral basis. Hence we have  $\text{disc}(KL) = \text{disc}(\{\alpha_i \beta_j\})$  and we only need to compute  $\text{disc}(\{\alpha_i \beta_j\})$ . We first remark all the embeddings of  $KL$  to  $\mathbb{C}$  fixing  $\mathbb{Q}$  is obtained<sup>1</sup> by  $\sigma_i \tau_j$  where  $\sigma_i$ 's are embeddings of  $K$  to  $\mathbb{C}$  and  $\tau_j$ 's are embeddings of  $L$  to  $\mathbb{C}$ .

$$\begin{aligned} \text{Let } A &= \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{bmatrix} \text{ and } B \text{ for } \beta \text{ and } \tau_j\text{'s. Observe we have} \\ \text{disc}(\{\alpha_i \beta_j\}) &= \left| \begin{array}{cccccccccccc} \sigma_1 \tau_1(\alpha_1 \beta_1) & \dots & \sigma_1 \tau_1(\alpha_n \beta_1) & \sigma_1 \tau_1(\alpha_1 \beta_2) & \dots & \sigma_1 \tau_1(\alpha_n \beta_2) & \dots & \sigma_1 \tau_1(\alpha_1 \beta_n) & \dots & \sigma_1 \tau_1(\alpha_n \beta_n) \\ \sigma_2 \tau_1(\alpha_1 \beta_1) & \dots & \sigma_2 \tau_1(\alpha_n \beta_1) & \sigma_2 \tau_1(\alpha_1 \beta_2) & \dots & \sigma_2 \tau_1(\alpha_n \beta_2) & \dots & \sigma_2 \tau_1(\alpha_1 \beta_n) & \dots & \sigma_2 \tau_1(\alpha_n \beta_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_n \tau_1(\alpha_1 \beta_1) & \dots & \sigma_n \tau_1(\alpha_n \beta_1) & \sigma_n \tau_1(\alpha_1 \beta_2) & \dots & \sigma_n \tau_1(\alpha_n \beta_2) & \dots & \sigma_n \tau_1(\alpha_1 \beta_n) & \dots & \sigma_n \tau_1(\alpha_n \beta_n) \\ \sigma_1 \tau_2(\alpha_1 \beta_1) & \dots & \sigma_1 \tau_2(\alpha_n \beta_1) & \sigma_1 \tau_2(\alpha_1 \beta_2) & \dots & \sigma_1 \tau_2(\alpha_n \beta_2) & \dots & \sigma_1 \tau_2(\alpha_1 \beta_n) & \dots & \sigma_1 \tau_2(\alpha_n \beta_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_n \tau_m(\alpha_1 \beta_1) & \dots & \sigma_n \tau_m(\alpha_n \beta_1) & \sigma_n \tau_m(\alpha_1 \beta_2) & \dots & \sigma_n \tau_m(\alpha_n \beta_2) & \dots & \sigma_n \tau_m(\alpha_1 \beta_n) & \dots & \sigma_n \tau_m(\alpha_n \beta_n) \end{array} \right|^2 \\ &= \left| \begin{array}{ccc} \sigma_1(\alpha_1) \tau_1(\beta_1) & \dots & \sigma_1(\alpha_n) \tau_1(\beta_m) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) \tau_m(\beta_1) & \dots & \sigma_n(\alpha_n) \tau_m(\beta_m) \end{array} \right|^2 \\ &= \left| \begin{array}{cccc} \tau_1(\beta_1) A & \tau_1(\beta_2) A & \tau_1(\beta_3) A & \dots & \tau_1(\beta_m) A \\ \tau_2(\beta_1) A & \tau_2(\beta_2) A & \tau_2(\beta_3) A & \dots & \tau_2(\beta_m) A \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \tau_m(\beta_1) A & \tau_m(\beta_2) A & \tau_m(\beta_3) A & \dots & \tau_m(\beta_m) A \end{array} \right|^2, \quad \text{block matrix form} \\ &= \det(A \otimes B)^2, \quad \text{Kronecker product} \\ &= (\det(A))^m \cdot (\det(B))^n, \quad \text{standard property of Kronecker product} \\ &= \text{disc}(K)^m \cdot \text{disc}(L)^n \end{aligned}$$

<sup>1</sup>This is not rigorous saying, for more precisely formulation of the idea, go back to Theorem 2.3.9, i.e. we need to consider a normal cover and realize we can extend those  $\sigma_i$ 's and  $\tau_j$ 's.

♡

**Corollary 2.7.10.2.** *Let  $K_n$  be the  $n$ th cyclotomic field, i.e.  $K_n = \mathbb{Q}(\zeta_n)$ , then  $\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n]$ .*

*Proof.* We already have this claim if  $n = p^r$  for some prime  $p$ , as we recall Theorem 2.7.5.

We use induction on the value of  $n$ . Suppose it holds for all values less than  $n$ . Then suppose  $n$  is not a power of a prime, then we have  $n = n_1 n_2$  where  $n_1$  and  $n_2$  are coprime and  $n_1, n_2 < n$ . Hence by induction hypothesis, let  $K_1 = K_{n_1}$  and  $K_2 = K_{n_2}$  we have

$$\mathcal{O}_{K_1} = \mathbb{Z}[\zeta_{n_1}], \mathcal{O}_{K_2} = \mathbb{Z}[\zeta_{n_2}]$$

However,  $\text{disc}(K_1) \mid n_1^{\phi(n_1)}$  and  $\text{disc}(K_2) \mid n_2^{\phi(n_2)}$  and  $n_1, n_2$  are coprime, which imply  $\text{disc}(K_1)$  and  $\text{disc}(K_2)$  are coprime. Also note

$$[K_{n_1 n_2} : \mathbb{Q}] = \phi(n_1 n_2) = \phi(n_1) \phi(n_2) = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$$

Hence, we can apply Corollary 2.7.10.1 and obtain

$$\mathcal{O}_{K_{n_1 n_2}} = \mathcal{O}_{K_n} = \mathbb{Z}[\zeta_{n_1}] \mathbb{Z}[\zeta_{n_2}]$$

where  $\mathbb{Z}[\zeta_{n_1}] \mathbb{Z}[\zeta_{n_2}] = \mathbb{Z}[\zeta_{n_1 n_2}] = \mathbb{Z}[\zeta_n]$

♡

**Theorem 2.7.11.** *Let  $K$  be a number field of degree  $n$  with  $K = \mathbb{Q}(\lambda)$  where  $k \in \mathcal{O}_K$ . Then there is an integral basis*

$$\left\{1, \frac{f_1(\lambda)}{d_1}, \dots, \frac{f_{n-1}(\lambda)}{d_{n-1}}\right\}$$

where  $d_i \in \mathbb{Z}_{\geq 1}$  with  $d_1 \mid d_2 \mid \dots \mid d_{n-1}$  and  $f_i$ 's are monic polynomials of degree  $i$  in  $\mathbb{Z}[x]$ .

Furthermore, the  $d_i$ 's are uniquely determined by the following way: let  $d = \text{disc}(\lambda)$ , for each  $1 \leq q \leq n$  define  $\mathcal{O}_q \subseteq \mathcal{O}_K$  to be

$$\mathcal{O}_q = \left\{ \frac{1}{d} f(\lambda) : f \in \mathbb{Z}[x], f = 0 \text{ or } \deg(f) \leq q-1 \right\}$$

Then  $d_{q-1}$  is the smallest positive integer  $m$  such that  $m\mathcal{O}_q \subseteq \mathbb{Z}[\lambda]$ .

*Proof.* Note this proof is omitted in the original note. However, I will provide a sketch proof nonetheless.

First we recall a free abelian group of rank  $n$  is just a free  $\mathbb{Z}$ -module of rank  $n$ . Thus, observe if  $K$  has degree  $n$ , we have  $K$  is a subset of a free abelian group of rank  $n$  by consider a basis  $\{\alpha_1, \dots, \alpha_n\}$  and so  $K \subseteq \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$ . On the other

hand, by Theorem 2.6.12, we have  $\mathcal{O}_K \subseteq K$  where  $\mathcal{O}_K$  is a free abelian group of rank  $n$ . Hence we have  $K$  is a free abelian group of rank  $n$ .

Thus, for  $1 \leq i \leq n$  let  $F_i$  be the free abelian group of rank  $k$  generated by  $\frac{1}{d}, \frac{\lambda}{d}, \dots, \frac{\lambda^{k-1}}{d}$  and set  $K_i = F_i \cap K$ . Then we have  $K_1 = \mathbb{Z}$  and  $K_n = K$ . We will define the  $d_i$  and  $f_i$  so that for each  $1 \leq l \leq n$  we have

$$1, \frac{f_1(\lambda)}{d_1}, \dots, \frac{f_{l-1}(\lambda)}{d_{l-1}}$$

is a basis of  $R_k$  over  $\mathbb{Z}$ .

This holds for  $k = 1$  and assume it holds for all values less than  $k$ . We have to define  $f_k$  and  $d_k$  and show we get a basis for  $K_{l+1}$  by add  $\frac{f_k(\lambda)}{d_k}$  in the previous list.

Let  $\pi$  be the projection of  $F_{k+1} = \mathbb{Z} \frac{1}{d} \oplus \dots \oplus \mathbb{Z} \frac{\lambda^k}{d}$  on the last factor. Then  $\pi(K_{k+1})$  is a subgroup of  $\mathbb{Z} \frac{\lambda^k}{d}$ , which is an infinite cyclic group. Thus  $\pi(K_{k+1})$  is cyclic and so let  $\beta \in K_{k+1}$  such that  $\langle \beta \rangle = \pi(K_{k+1})$ . Then we see  $\{1, f_1(\lambda)/d_1, \dots, f_{k-1}(\lambda)/d_{k-1}, \beta\}$  is a basis over  $\mathbb{Z}$  for  $K_{k+1}$ .

We only need to show  $\beta$  has the desired form now. However, we have

$$\frac{\lambda^k}{d_{k-1}} = \pi\left(\frac{\lambda f_{k-1}(\lambda)}{d_{k-1}}\right)$$

and this is in  $\pi(K_{k+1})$ . Thus  $\lambda^k/d_{k-1} = m\pi(\beta)$  for some  $m \in \mathbb{Z}$ . Define  $d_k = md_{k-1}$  and so we have  $\pi(\beta) = \lambda^k/d_k$  which imply  $\beta = f_k(\lambda)/d_k$  for some  $f_k(\lambda) = \lambda^k + \text{lower degree terms}$ . Hence we only need to check  $f$  has integer coefficients. However, we note  $\frac{df_k}{d_k}$  must have integer coefficient and since  $f_k(\lambda)/d_{k-1} = m\beta$ , we have

$$\frac{f_k(\lambda) - \lambda f_{k-1}(\lambda)}{d_{k-1}} = \gamma \in K$$

and in particular  $\gamma \in K_k$ . Now use the basis for  $R_k$  we can write  $\gamma = g(\lambda)/d_{k-1}$  for some  $g \in \mathbb{Z}[x]$  with degree less than  $k$ . Therefore,  $f_k(x) - \lambda f_{k-1}(x)$  is equal  $g(x)$  and hence  $f_k(x) \in \mathbb{Z}[x]$ . Finally, observe by definition we would have  $d_k$  is the smallest positive integer so  $mK_{k+1} \subseteq \mathbb{Z}[\lambda]$ .  $\heartsuit$

**Theorem 2.7.12 (Stickelberger's Criterion).** *Let  $K$  be a number field of degree  $n$  and  $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ . Then*

$$\text{disc}(\alpha_1, \dots, \alpha_n) \equiv 0 \text{ or } 1 \pmod{4}$$

*In particular,  $\text{disc}(K)$  is either 0 or 1 when mod 4.*

*Proof.* Let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $K$  into  $\mathbb{C}$  fix  $\mathbb{Q}$ . Then let

$$d := \text{disc}(\alpha_1, \dots, \alpha_n) = \det([\sigma_i(\alpha_j)]_{i,j})^2$$

Observe  $\det([\sigma_i(\alpha_j)]_{i,j})$  is a sum of  $n!$  many terms and we recall one definition of determinants is the sum over all permutations in  $S_n$  of elements in the matrix,

i.e.  $\det(a_{ij}) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{i, \sigma(i)}$ . Thus, we let  $P$  be the sum of terms of  $\det([\sigma_i(\alpha_j)]_{i,j})$  correspond to even permutations and  $S$  be the sum terms correspond to odd permutations.

Then we have  $\det([\sigma_i(\alpha_j)]_{i,j}) = P - S$  by sign consideration and definition of determinants. Hence we have  $d = (P - S)^2 = (P + S)^2 - 4PS$ . If we can show  $P + S$  and  $PS$  are both integers, then and so when mod out by 4 we see  $d \equiv (P + S)^2 \pmod{4}$  where  $(P + S)^2$  only have two possibilities, i.e. 0 or 1 (because if  $P + S$  is even then  $(P + S)^2 \equiv 0 \pmod{4}$  and  $P + S$  odd then  $(P + S)^2 \equiv 1 \pmod{4}$ ).

Hence we will show  $P + S$  and  $PS$  are both integers.

First, we claim  $P + S$  and  $PS$  are algebraic integer. Observe

$$P + S = \sum_{\tau \in S_n} \prod_{i=1}^n \sigma_{\tau(i)}(\alpha_i), PS = \prod_{i=1}^n \prod_{\tau \in S_n} \sigma_{\tau(i)}(\alpha_i)$$

where we have<sup>1</sup>  $\sigma_i(\alpha_j) \in \mathbb{A}$  and so  $P + S$  and  $PS$  are a mix of sums and products of algebraic integers and hence are algebraic integers themselves.

Next we will show  $P + S$  and  $PS$  are both in the rational numbers. Consider a normal cover of  $K$ , say  $L$ . Then embeddings of  $K$  into  $\mathbb{C}$  fixing  $\mathbb{Q}$  extends to automorphisms of  $L$  fixing  $\mathbb{Q}$ . Also, observe for any  $\phi \in \text{Gal}(L/\mathbb{Q})$ , we have  $\phi \circ \sigma_i$  is an embedding of  $K$  into  $\mathbb{C}$  fixing  $\mathbb{Q}$  and since  $\phi$  is an automorphism (with inverse), we see  $\phi$  gives an permutation on the list  $\{\sigma_1, \dots, \sigma_n\}$  if we apply  $\phi$  to each  $\sigma_i$ . Say the permutation is  $\gamma$ . Therefore, we have

$$\begin{aligned} \phi(P + S) &= \sum_{\tau \in S_n} \prod_{i=1}^n \phi \circ \sigma_{\gamma \circ \tau}(\alpha_i) \\ &= P + S \end{aligned}$$

as we note  $\gamma \circ S_n = S_n$ . Similarly we see  $\phi(PS) = PS$  because we also took products over  $S_n$ . Hence we must have  $P + S, PS \in \mathbb{Q}$  by definition of  $\text{Gal}(L/\mathbb{Q})$ , i.e. automorphisms that only fix  $\mathbb{Q}$ . Thus we have  $P + S$  and  $PS$  are algebraic integers in  $\mathbb{Q}$ , i.e. they must be integers. Hence the proof follows.  $\heartsuit$

## 2.8 Resultants

---

<sup>1</sup>To see this is the case, let  $\sigma : K \rightarrow \mathbb{C}$  be embedding fixing  $\mathbb{Q}$ . Let  $\alpha \in \mathcal{O}_K$ , then  $f(\alpha) = 0$  where  $f(x) = x^n + m_{n-1}x^{n-1} + \dots + m_0$ . Hence we have  $f(\sigma(\alpha)) = \sigma(\alpha)^n + \dots + m_0 = \sigma(\alpha^n + m_{n-1}\alpha^{n-1} + \dots + m_0) = 0$

**Definition 2.8.1.** Let  $f(x), g(x) \in \mathbb{C}[x]$  with  $f(x) = \sum_{i=0}^n a_i x^i$  and  $g(x) = \sum_{i=0}^m b_i x^i$ . Then we define the **resultant** of  $f(x)$  and  $g(x)$ , denoted by  $R(f, g)$ , to be

$$R(f, g) := \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & 0 & \dots & a_0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \dots & a_n & a_{n-1} & a_{n-2} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & b_1 & b_0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & b_{m-2} & b_{m-3} & b_{m-4} & b_{m-5} & \dots & b_0 & 0 & 0 \\ 0 & 0 & 0 & \dots & b_{m-1} & b_{m-2} & b_{m-3} & b_{m-4} & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & b_m & b_{m-1} & b_{m-2} & b_{m-3} & \dots & b_2 & b_1 & b_0 \end{vmatrix}$$

**Example 2.8.2.**

1. Let  $f(x) = x^4 + 2x^3 + 3x^2 + 4x + 5$  and  $g(x) = 2x^3 + x^2 + 3x + 4$ , then we have

$$R(f, g) = \begin{vmatrix} 1 & 2 & 3 & 4 & 5 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 0 \\ 0 & 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 & 4 & 0 & 0 \\ 0 & 0 & 2 & 1 & 3 & 4 & 0 \\ 0 & 0 & 0 & 2 & 1 & 3 & 4 \end{vmatrix} = 15$$

2. Let  $f(x) = x^4$  and  $g(x) = x^3 - 1$ , then we would have

$$R(f, g) = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 \end{vmatrix} = (-1)^4$$

3. Let  $f(x) = x^n$  and  $g(x) = x^m - 1$ , then we would have

$$R(f, g) = \begin{vmatrix} I_m & 0 \\ C & -I_n \end{vmatrix} = (-1)^n$$

where  $C$  is a block matrix(try it by yourself and you will see).

**Remark 2.8.3.** Observe  $R(f, g)$  is homogeneous of degree  $m$  in  $a_i$ 's and degree  $n$  in  $b_j$ 's. What this means is the following: observe  $R(f, g)$  is a function based on  $m+n+2$  variables, i.e.  $R(f, g)$  varies as  $a_0, \dots, a_n, b_1, \dots, b_m$  varies. Then homogeneous in  $a_i$  of degree  $m$  means if we change  $a_0, \dots, a_n$  to  $ta_0, \dots, ta_n$ , i.e. we change  $f$  to  $tf$ , where  $t$  is any constant, then we get  $R(tf, g) = t^m R(f, g)$ . Similarly, we would have  $R(f, tg) = t^n R(f, g)$ .

**Remark 2.8.4.** The next proposition is actually what motivated the definition of resultant.

**Proposition 2.8.5.** *Let  $f, g \in \mathbb{C}[x]$ , then  $R(f, g) = 0$  if and only if  $f$  and  $g$  have non-constant common factor in  $\mathbb{C}$ .*

*Proof.* Let  $\deg(f) = n$  and  $\deg(g) = m$  with  $f(x) = \sum_{i=0}^n a_i x^i$  and  $g(x) = \sum_{i=0}^m b_i x^i$ . Note that  $f, g$  have a common root if and only if there exists  $h(x), k(x) \in \mathbb{C}[x]$  with  $h(x)f(x) = k(x)g(x)$  where  $\deg(h) \leq m-1$  and  $\deg(k) \leq n-1$ .

Now let  $h(x) = c_{m-1}x^{m-1} + \dots + c_0$  and  $k(x) = d_{n-1}x^{n-1} + \dots + d_0$ . Comparing coefficients on the both side of equation  $h(x)f(x) = k(x)g(x)$ , we have

$$\begin{aligned} a_0 c_0 &= b_0 d_0 \\ \vdots &= \vdots \\ a_n c_{m-3} + a_{n-1} c_{m-2} + a_{n-2} c_{m-1} &= b_m d_{n-3} + b_{m-1} d_{n-2} + b_{m-2} d_{n-1} \\ a_n c_{m-2} + a_{n-1} c_{m-1} &= b_m d_{n-2} + b_{m-1} d_{n-1} \\ a_n c_{m-1} &= b_m d_{n-1} \end{aligned}$$

with the  $k$ th row looks like

$$\sum_{i+j=k-1} a_i c_j = \sum_{i+j=k-1} b_m d_j$$

Thus move to the other side, we have

$$\begin{cases} a_n c_{m-1} - b_m d_{n-1} = 0 \\ a_n c_{m-2} + a_{n-1} c_{m-1} - b_m d_{n-2} - b_{m-1} d_{n-1} = 0 \\ \vdots \\ a_0 c_0 - b_0 d_0 = 0 \end{cases}$$

Make this into matrix form, we have

$$A \begin{bmatrix} c_{m-1} \\ c_{m-2} \\ c_{m-3} \\ \vdots \\ c_0 \\ -d_{n-1} \\ -d_{n-2} \\ \vdots \\ -d_0 \end{bmatrix} = 0, \text{ where } A := \begin{bmatrix} a_n & 0 & 0 & \dots & 0 & b_m & 0 & 0 & \dots & 0 \\ a_{n-1} & a_n & 0 & \dots & 0 & b_{m-1} & b_m & 0 & \dots & 0 \\ a_{n-2} & a_{n-1} & a_n & \dots & 0 & b_{m-2} & b_{m-1} & b_m & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_n & 0 & 0 & 0 & \dots & b_0 \end{bmatrix}$$

We want to find a non-trivial solution to the above system of equations in variables  $c_0, \dots, c_{m-1}$  and  $-d_0, \dots, -d_{n-1}$ . This is because once we find non-trivial solution, then  $h(x)$  and  $k(x)$  are non-constant polynomials and we see conversely



if we have  $h(x), k(x)$  are non-constant, then we can find non-trivial solution to the above system. Since we have  $m+n$  equations and  $m+n$  variables, we can find such a solution if and only if the above matrix  $A$  has determinant equal 0. However, note  $\det(A) = \det(A^T) = R(f, g)$  and so the proof follows.  $\heartsuit$

**Theorem 2.8.6.** Let  $f(x) = a_n x^n + \dots + a_0 = a_n \prod_{i=1}^n (x - \alpha_i)$  and  $g(x) = b_m x^m + \dots + b_0 = b_m \prod_{i=1}^m (x - \beta_i)$ . Define

$$S(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$$

Then we have

$$R(f, g) = S(f, g)$$

*Proof.* The coefficients  $a_0, \dots, a_{n-1}$  can be expressed<sup>1</sup> as  $a_n$  times an elementary symmetric function evaluating at the roots  $\alpha_1, \dots, \alpha_n$ . Similarly the coefficients  $b_1, \dots, b_{m-1}$  can be expressed as  $b_m$  times an elementary symmetric function evaluating at  $\beta_1, \dots, \beta_m$  as well.

Observe  $R(f, g)$  is homogeneous in the  $a_i$ 's of degree  $m$  and homogeneous in  $b_j$ 's of degree  $n$ . Hence,  $R(f, g)$  is  $a_n^m b_m^n$  times a symmetric function in  $m+n$  variables evaluated at  $(\alpha_1, \dots, \beta_m)$ .

Now we switch  $\alpha_i$ 's and  $\beta_j$ 's to be intermediates  $x_1, \dots, x_n, y_1, \dots, y_m$  with  $a_n, b_m$  constant for both  $R(f, g)$  and  $S(f, g)$ . We then get

$$R(f, g), S(f, g) \in \mathbb{C}[x_1, \dots, x_n, y_1, \dots, y_m]$$

Now, observe that for a polynomial  $p(x_1, \dots, x_n)$  over  $\mathbb{C}$ , if we have  $\forall \alpha \in \mathbb{C}, p = 0$  when we evaluate at  $i$ th place and  $j$ th place with  $\alpha$ , then we must have  $x_i - x_j \mid p$ .<sup>2</sup> Therefore, note we have  $x_i = y_j$  imply  $R(f, g) = 0$  by Proposition 2.8.5 as  $x_i = y_j$  imply  $f$  and  $g$  have a common factor<sup>3</sup>. Hence, by the observation we made above, we have  $x_i - y_j \mid R(f, g)$  in  $\mathbb{C}[x_1, \dots, y_m]$ . However, this would imply  $S(f, g)$  divides  $R(f, g)$  as  $\mathbb{C}[x_1, \dots, y_m]$  is a UFD and  $i, j$  are arbitrary in the argument. Viz, we have  $x_i - y_j \mid R(f, g)$  for all  $1 \leq i \leq n, 1 \leq j \leq m$  and at the same time by definition  $S(f, g)$  is just product of all the  $x_i - y_j$ 's.

---

<sup>1</sup>This is obtained by compare coefficients of  $\sum a_i x^i$  and  $a_n \prod (x - \alpha_i)$ . In particular what this says is that for all  $0 \leq i \leq n-1$ , we can find elementary symmetric function (if you do not know what elementary symmetric functions are, Google it.) in  $n$  vanish  $s(x_1, \dots, x_n)$  so that  $a_i = a_n s(\alpha_1, \dots, \alpha_n)$

<sup>2</sup>In other word, if  $x_i = x_j$  imply  $p(x_1, \dots, x_n) = 0$ , then  $x_i - x_j \mid p$ . One should try to prove this if he/she is not convinced. Here I will show this hold for  $\mathbb{C}[x, y]$  and inductively it will hold for all  $\mathbb{C}[x_1, \dots, x_n]$ . Say  $p(x, y) \in \mathbb{C}[x, y]$  with  $p(a, a) = 0$  for all  $a \in \mathbb{C}$ . Consider  $p(x, y) = \sum_{i=0}^n f_i(x) y^i$  as a polynomial in coefficients in  $\mathbb{C}[x]$  and intermediate  $y$ . Then we have  $p(x, x) = 0$  as  $p(a, a) = 0$  for all  $a \in \mathbb{C}$  and so  $x$  is a root of the polynomial  $p(x, y)$  in  $\mathbb{C}[x][y]$ , i.e.  $(y - x)$  divides  $p(x, y)$ .

<sup>3</sup>Namely, both of them are divisible by  $x - x_i$ .

Observe that  $g(x) = b_m \prod_{j=1}^m (x - y_j)$  and we get

$$S(f, g) = a_n^m \prod_{i=1}^n g(x_i) \quad (\text{Eq. 2.8.1})$$

and similarly we would have  $f(x) = a_n \prod (x - x_i) = a_n (-1)^n \prod (x_i - x)$  so

$$S(f, g) = (-1)^{nm} b_m^n \prod_{i=1}^n f(y_i)$$

From this two equations, we see  $S(f, g)$  is homogeneous of degree  $n$  in the  $y_j$ 's and homogeneous of degree  $m$  in the  $x_i$ 's. This means  $R(f, g)$  and  $S(f, g)$  have the same (total) degree with  $S(f, g)$  divides  $R(f, g)$  and this imply they only differ by a constant, say  $S(f, g) = cR(f, g)$  with  $c \in \mathbb{C}$  and this holds for all polynomials  $f$  and  $g$  with  $\deg(f) = n$  and  $\deg(g) = m$ .

Now consider  $f(x) = x^n$  and  $g(x) = x^m - 1$ . We have  $R(f, g) = 1 \cdot (-1)^n = (-1)^n$ . On the other hand, we have  $x = 0$  is all the roots of  $f(x)$  and  $g(x) = \prod_{i=1}^m (x - \zeta_m^i)$  is all the roots of  $g$ . Hence we would have, if we observe  $\prod_{j=1}^m \zeta_m^j = (-1)^{m+1}$ ,

$$\begin{aligned} S(f, g) &= (1)^m (1)^n \prod_{i=1}^n \prod_{j=1}^m (0 - \zeta_m^j) \\ &= ((-1)^m \prod_{j=1}^m \zeta_m^j)^n \\ &= ((-1)^m \cdot (-1)^{m+1})^n \\ &= (-1)^n \end{aligned}$$

Hence we must have  $S(f, g) = c \cdot R(f, g) = c \cdot (-1)^n = (-1)^n$  and so  $c = 1$ . The proof follows. ♡

**Corollary 2.8.6.1.** *Let  $\alpha$  be a root of an irreducible polynomial  $f(x)$  of degree  $n$  in  $\mathbb{Q}$ . Then*

$$\text{disc}(\alpha) = \text{disc}(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} R(f, f')$$

*Proof.* Let  $\alpha = \alpha_1, \dots, \alpha_n$  be all the conjugates of  $\alpha$  (in  $\mathbb{C}$ ), then  $f(x) = \prod (x - \alpha_i)$ . By Theorem 2.8.6 and equation Eq. 2.8.1 in the proof, we see

$$R(f, f') = S(f, f') = \prod_{i=1}^n f'(\alpha_i)$$

Now we invoke the theorem 2.5.7 to obtain (where  $K$  is the smallest field containing  $\alpha_1, \dots, \alpha_n$ )

$$\text{disc}(\alpha) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^K(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(\alpha_i)$$

where we observe we have the last line because embeddings from  $K$  to  $\mathbb{C}$  fixing  $\mathbb{Q}$  are exactly maps that send  $\alpha \rightarrow \alpha_i$  where  $1 \leq i \leq n$ . Hence we have

$$\text{disc}(\alpha) = (-1)^{\frac{n(n-1)}{2}} R(f, f')$$

as desired. ♡

**Example 2.8.7.** Let  $\theta$  be a root of  $f(x) = x^3 + x^2 - 2x + 8$ . Note  $f(x)$  is irreducible over  $\mathbb{Q}$  by the rational root test. Thus, we have  $f'(x) = 3x^2 + 2x - 2$  and so

$$\text{disc}(\theta) = (-1)^{3(3-1)/2} R(f, f') = (-1) \begin{vmatrix} 1 & 1 & -2 & 8 & 0 \\ 0 & 1 & 1 & -2 & 8 \\ 3 & 2 & -2 & 0 & 0 \\ 0 & 3 & 2 & -2 & 0 \\ 0 & 0 & 3 & 2 & -2 \end{vmatrix} = -2012 = -4 \cdot 503$$

Let  $K = \mathbb{Q}(\theta)$ , what is  $\text{disc}(K)$ ? Let us try to determine it. Recall from Example 2.6.8 we used integral basis argument (e.g.  $\det(A)^2 \cdot \text{disc}(K) = \text{disc}(\theta)$ ) to show  $\text{disc}(K) \in \{-4, -503, -2012\}$ , now we just have to nail it down.

First, we will show  $\alpha := \frac{\theta^2 + \theta}{2}$  is an algebraic integer in  $\mathcal{O}_K$ . If we have  $\alpha \in \mathcal{O}_K$ , then we would have

$$\begin{aligned} \text{disc}(1, \theta, \alpha) &= \text{disc}(1, \theta, \frac{\theta^2 + \theta}{2}) \\ &= \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1/2 & 1/2 \end{vmatrix}^2 \cdot \text{disc}(1, \theta, \theta^2), \quad \text{By Proposition 2.5.6} \\ &= \frac{\text{disc}(\theta)}{4} \end{aligned}$$

Videlicet we obtained another basis of  $K$  in  $\mathcal{O}_K$  with discriminant equal  $-503$ , and this would force  $\text{disc}(K)$  to divide  $\text{disc}(1, \theta, \alpha)$  and so  $\text{disc}(K) = -503$ .

First, we need to find the minimal polynomial of  $\alpha$ . Let  $\theta = \theta_1, \theta_2, \theta_3$  be all the conjugates of  $\theta$ . Then  $f(x) = \prod_{i=1}^3 (x - \theta_i)$  and

$$\alpha = \alpha_1 = \frac{\theta_1^2 + \theta_1}{2}, \alpha_2 = \frac{\theta_2^2 + \theta_2}{2}, \alpha_3 = \frac{\theta_3^2 + \theta_3}{2}$$

would be all the conjugates of  $\alpha$  over  $\mathbb{Q}$ , i.e. we obtained this by simply apply the embeddings  $\sigma_1, \dots, \sigma_3$  induced by  $\theta$  to  $\alpha_1$ . Hence, we would get

$$g(x) = (x - \alpha_1) \dots (x - \alpha_3) = x^3 - a_1 x^2 + a_2 x - a_3, a_1, a_2, a_3 \in \mathbb{Q}$$

is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ . We also know by comparing coefficients of  $(x - \theta_1) \dots (x - \theta_3) = x^3 + x^2 - 2x + 8$ , we would get

$$s_1 := \theta_1 + \theta_2 + \theta_3 = -1, s_2 = \theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3 = -2, s_3 = \theta_1\theta_2\theta_3 = -8$$

Thus, we have

$$\begin{aligned}
a_1 &= \alpha_1 + \alpha_2 + \alpha_3 \\
&= \frac{\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_1 + \theta_2 + \theta_3}{2} \\
&= \frac{s_1^2 - 2s_2 + s_1}{2} \\
&= 2
\end{aligned}$$

For  $a_2$ , we have<sup>1</sup>

$$\begin{aligned}
a_2 &= \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 \\
&= \left(\frac{\theta_1^2 + \theta_1}{2}\right)\left(\frac{\theta_2^2 + \theta_2}{2}\right) + \left(\frac{\theta_2^2 + \theta_2}{2}\right)\left(\frac{\theta_3^2 + \theta_3}{2}\right) + \left(\frac{\theta_1^2 + \theta_1}{2}\right)\left(\frac{\theta_3^2 + \theta_3}{2}\right) \\
&= \frac{1}{4} \left( \sum_{cyclic} \theta_i^2 \theta_{i+1}^2 + \theta_i^2 \theta_{i+1} + \theta_i \theta_{i+1}^2 + \theta_i \theta_{i+1} \right) \\
&= \frac{1}{4} \left( s_2^2 - 2 \sum_{cyclic} \theta_i^2 \theta_{i+1} \theta_{i+2} + \sum_{cyclic} ((\theta_i^2 \theta_{i+1} + \theta_i \theta_{i+1}^2) + \theta_i \theta_{i+1}) \right) \\
&= \frac{1}{4} \left( s_2^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3) + \sum_{cyclic} (\theta_i^2 \theta_{i+1} + \theta_i \theta_{i+1}^2) + s_2 \right) \\
&= \frac{1}{4} (s_2^2 - 2s_3s_1 + s_2 + s_1s_2 - 3s_3) \\
&= 3
\end{aligned}$$

Similarly, we would have

$$\begin{aligned}
a_3 &= \alpha_1\alpha_2\alpha_3 = \frac{1}{8} \prod_{i=1}^3 (\theta_i^2 + \theta_i) \\
&= \frac{1}{8} \theta_1\theta_2\theta_3 \prod_{i=1}^3 (1 + \theta_i) \\
&= \frac{1}{8} s_3 \cdot (-1)^3 f(-1) \\
&= 10
\end{aligned}$$

Therefore, all the conjugates of  $\alpha$  are in  $\mathbb{Z} \subseteq \mathbb{A} \cap K$ , we have  $disc(K) = -503$  as desired.

---

<sup>1</sup>**If you are confused by the following calculation, TRY BY YOURSELF AND IT SHOULD MAKE SENSE.** Note in the equations below, we have cyclic summand, denoted by  $\sum_{cyclic}$ . This basically means you sum over some cyclic indexing. In our case,  $i$  would go from 1 to 3, with the relation  $i + 1 = 1$  when  $i = 3$ . For example,  $\sum_{cyclic} x_i x_{i+1}$  in our case would be  $x_1 x_2 + x_2 x_3 + x_3 x_1$ .

Finally, we remark that  $K$  does not have any power basis. Given  $\lambda = a + b\theta + c\alpha \in \mathcal{O}_K$  be arbitrary, then we would have  $\lambda^2 = A + B\theta + C\alpha$  where  $A = a^2 - 2c^2 - 8bc$ ,  $B = -c^2 + 2ab + 2bc - b^2$  and  $C = 2b^2 + 2bc + c^2$ . Hence, we get

$$D := \begin{bmatrix} 1 & 0 & 0 \\ a & b & c \\ A & B & C \end{bmatrix} \Rightarrow \begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \end{bmatrix} = D \cdot \begin{bmatrix} 1 \\ \theta \\ \alpha \end{bmatrix} \Rightarrow \text{disc}(\lambda) = \det(D)^2 \cdot \text{disc}(1, \theta, \alpha)$$

However, note  $\det(D) = bC - Bc$  and so  $\det(D)^2 = (2b^3 - bc^2 + b^2c + 2c^3)^2$ . Hence, we get

$$\det(D)^2 \equiv (c(b^2 - b) - bc(c + 1)) \equiv 0 \pmod{2}$$

Now, suppose for a contradiction we have  $1, \lambda, \lambda^2$  is an integral basis, i.e. a power basis. Then we must have  $\text{disc}(\lambda) = \text{disc}(1, \theta, \alpha) = \text{disc}(K) = -503$ . However, in this case we would have

$$\text{disc}(\lambda) \equiv \det(D)^2 \cdot \text{disc}(1, \theta, \alpha) \pmod{2}$$

$$\Rightarrow -503 \equiv 0 \cdot (-503) \pmod{2}$$

This is a contradiction we desire.

## Chapter 3

### Dedekind Domains

莫唱阳关曲，泪湿当年金缕。  
离歌自古最消魂，闻歌更在消魂处。

南楼杨柳多情绪，不系行人住。  
人情却似飞絮，悠扬便逐春风去。

---

晏几道

## 3.1 Basic Definitions

**Definition 3.1.1.** Let  $f : A \rightarrow B$  be an  $A$ -algebra, then we say  $b \in B$  is **integral over**  $A$  if there exists monic polynomial  $f(x) \in A[x]$  so  $f(b) = 0$ .

**Example 3.1.2.** All algebraic integers are integral over  $\mathbb{Z}$  and  $\mathbb{Q}$ . In particular, we can define algebraic integers to be those elements that are integral over  $\mathbb{Z}$ .

In general, if  $A$  is a field and  $f : A \rightarrow B$  is an  $A$ -algebra, then  $b \in B$  is integral over  $A$  if and only if  $b$  is algebraic over  $A$ .

**Definition 3.1.3.** Let  $f : A \rightarrow B$  be an  $A$ -algebra, then we say  $B$  is **integral over**  $A$  if all elements of  $B$  is integral over  $A$ .

**Example 3.1.4.** Let  $K$  be a number field, then we have  $\mathcal{O}_K$  is integral over  $K$ .

**Proposition 3.1.5.** Let  $\phi : A \rightarrow B$  be an  $A$ -algebra and  $b \in B$ , then the following are equivalent:

1.  $b$  is integral over  $A$ .
2.  $A[b] := \{f(b) : f(x) \in A[x]\}$ , which is the  $A$ -subalgebra of  $B$  generated by  $b$ , is a finite  $A$ -algebra.
3. There is a finite  $A$ -subalgebra  $C \subseteq B$  such that  $b \in C$ .

*Proof.* Check my 446 Commutative Algebra Notes~ In particular, the proof is identical to the proof of Theorem 2.1.5.  $\heartsuit$

**Definition 3.1.6.** Let  $f : A \rightarrow B$  be an  $A$ -algebra, then we define the **integral closure** of  $B$  over  $A$  to be  $\overline{B} := \{b \in B : b \text{ is integral over } A\}$ .

**Definition 3.1.7.** Let  $A \subseteq B$  where  $A$  is a subring of  $B$ , then we say  $A$  is **integrally closed** in  $B$  if  $A$  is equal to the integral closure of  $A$ .

**Definition 3.1.8.** A **Dedekind domain** is an integral domain such that:

1. Every ideal is finitely generated.
2. Every non-zero prime ideal is maximal.
3.  $R$  is integrally closed in its field of fraction.

**Remark 3.1.9.** In other word, if  $R$  is integrally closed in its field of fraction, this means for all  $\alpha \in K := \text{Frac}(R)$  which is a root of a monic polynomial in  $R$ , we have  $\alpha \in R$ .

**Remark 3.1.10.** Let  $R$  be Dedekind domain, then the first condition is saying  $R$  is Noetherian. The second condition is saying  $R$  has Krull dimension 1.

**Example 3.1.11.**  $\mathbb{Z}$  is integrally closed over  $\mathbb{Q}$  as the only algebraic integers in  $\mathbb{Q}$  are  $\mathbb{Z}$ .

**Remark 3.1.12.** In the following of this section, we will show  $\mathcal{O}_K$  is a Dedekind domain for all number field  $K$ .

**Lemma 3.1.13.** Let  $K$  be a number field and  $I$  be a non-zero ideal in  $\mathcal{O}_K$ . Then there is a non-zero integer  $a \in I$ .

*Proof.* Since  $I$  is non-zero, let  $0 \neq \alpha \in I$ . Then consider  $\alpha = \alpha_1, \dots, \alpha_n$  be all the conjugates of  $\alpha$ . We have  $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = \prod_{i=1}^n \alpha_i = t \in \mathbb{Z} \setminus \{0\}$ . However, note  $\alpha_2, \dots, \alpha_n \in \mathbb{A}$  and  $\beta = \alpha_2 \dots \alpha_n = \frac{t}{\alpha} \in \mathbb{Q}(\alpha) \subseteq K$ , so we have  $\beta \in \mathcal{O}_K$ . In particular, then  $\alpha\beta = a \in I$  as desired.  $\heartsuit$

**Definition 3.1.14.** Let  $K$  be a number field and  $I$  an ideal in  $\mathcal{O}_K$ . A set of elements  $\{\alpha_1, \dots, \alpha_n\} \subseteq I$  is said to be an **integral basis for  $I$**  if every element of  $I$  can be written as a unique linear combination of  $\alpha_1, \dots, \alpha_n$  using integers<sup>1</sup>.

**Example 3.1.15.** Let  $K$  be a number field, then  $I = \mathcal{O}_K = \langle 1 \rangle$  is an ideal in  $\mathcal{O}_K$  with an integral basis (by Theorem 2.6.3).

**Theorem 3.1.16.** Let  $K$  be a number field,  $\omega_1, \dots, \omega_n$  be an integral basis for  $K$  and  $I$  an ideal in  $\mathcal{O}_K$ . Then there exists an integral basis  $\alpha_1, \dots, \alpha_n$  for  $I$  which determined by

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}$$

---

<sup>1</sup>This means  $I$  is in the span of  $\alpha_1, \dots, \alpha_n$  as  $\mathbb{Z}$ -module. Or in other word, the additive structure of  $I$  is  $I \cong \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$

where  $a_{ij} \in \mathbb{Z}$  and in particular  $a_{ii} \in \mathbb{Z}_{\geq 1}$  for  $1 \leq i \leq n, 1 \leq j \leq n$ .

*Proof.* By the Lemma 3.1.13, there exists a positive  $a \in I$ . Therefore we have  $a\omega_i \in I$  for  $1 \leq i \leq n$ . Now set  $\alpha_1 = a_{11}\omega_1$  where  $a_{11}$  is the smallest positive integer for which  $a_{11}\omega_1 \in I$ . Then we choose  $\alpha_2, \dots, \alpha_n$  so that

$$\alpha_i = \sum_{j=1}^n a_{ij}\omega_j$$

where  $a_{ii} \in \mathbb{Z}_{\geq 1}$  and  $a_{i1}, \dots, a_{i,i-1} \in \mathbb{Z}$  for which  $a_{ii}$  is minimal such that  $\alpha_i \in I$ .

Now we claim  $\alpha_1, \dots, \alpha_n$  is an integral basis for  $I$ . It is obvious that  $\{\alpha_1, \dots, \alpha_n\}$  is a basis for  $K$  over  $\mathbb{Q}$  since  $\det(A) \neq 0$  where  $A = \begin{bmatrix} a_{11} & \dots & 0 \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$ . Thus, it is enough to show that every element  $\alpha \in I$  can be written as integer linear combinations. Since  $\{\omega_1, \dots, \omega_n\}$  is an integral basis for  $K$ , we have  $\alpha = \sum_{i=1}^n c_i\omega_i$  where  $c_i \in \mathbb{Z}$ .

Note  $c_n$  is divisible by  $a_{nn}$  by minimality of  $a_{nn}$ . Indeed, if this is not the case, then  $c_n = qa_{nn} + r$  with  $0 < r < a_{nn}$  and then  $\alpha - q\alpha_n = (c_1 - qa_{n1})\omega_1 + \dots + r\omega_n \in I$ , i.e.  $a_{nn}$  is not the smallest integer so  $\sum_{i=1}^n a_{ni}\omega_i \in I$ . This is a contradiction. So we must have  $a_{nn} \mid c_n$ .

Therefore, say  $c_n = q_n a_{nn}$  where  $q_n \in \mathbb{Z}$ . Then we have

$$\begin{aligned} \alpha - q_n \alpha_n &= (c_1 - q_n a_{n1})\omega_1 + \dots + (c_{n-1} - q_n a_{n,n-1})\omega_{n-1} \\ &:= d_1\omega_1 + \dots + d_{n-1}\omega_{n-1} \in I \end{aligned}$$

Again, by minimality of  $a_{n-1,n-1}$ , we have  $a_{n-1,n-1}$  divides  $d_{n-1}$ , say  $d_{n-1} = q_{n-1}a_{n-1,n-1}$  and so

$$\alpha - q_n \alpha_n - q_{n-1} \alpha_{n-1} = d'_1\omega_1 + \dots + d'_{n-2}\omega_{n-2} \in I$$

Thus inductively we see in the end we get

$$\alpha = q_1\alpha_1 + \dots + q_n\alpha_n, q_1, \dots, q_n \in \mathbb{Z}$$

This establish the proof of our theorem. ♡

**Theorem 3.1.17.** *Let  $K$  be a number field and  $\mathcal{O}_K$  the ring of integers of  $K$ . Then  $\mathcal{O}_K$  is a Dedekind domain.*

*Proof.* We need to check three conditions in the definition. The first condition is done due to Theorem 3.1.16.

Now let  $P$  be a non-zero prime ideal. We will show  $\mathcal{O}_K/P$  is a field by show  $\mathcal{O}_K/P$  is in fact finite, then finite integral domain (due to  $P$  is prime) would imply  $\mathcal{O}_K/P$  is actually a field. By the Lemma 3.1.13, there is a positive integer  $a \in P$ .



Let  $\omega_1, \dots, \omega_n$  be an integral basis for  $\mathcal{O}_K$ . Then every  $\alpha \in \mathcal{O}_K$  is an integer linear combination of  $\omega_1, \dots, \omega_n$ , i.e.  $\alpha = \sum_{i=1}^n z_i \omega_i$ . Therefore, we have

$$|\mathcal{O}_K/P| \leq a^n$$

because for each  $z_i$  we only have at most  $a$  possibilities to choose from<sup>1</sup>.

Finally, let  $\gamma = \alpha/\beta$  such that  $f(\gamma) = 0$  for some monic  $f(x) \in \mathcal{O}[x]$ , say  $f(x) = x^m + \sum_{i=0}^{m-1} \alpha_i x^i$  with  $\alpha_i \in \mathcal{O}_K$  of degree  $d_i$  for  $0 \leq i \leq m-1$ . Also, we let  $d_m = m$ . We will show  $\gamma \in \mathbb{A}$ . Observe the  $\mathbb{Z}$  module (this is also a subring of  $\mathbb{C}$ )  $M := \mathbb{Z}[\alpha_0, \dots, \alpha_{m-1}, \gamma]$  is finitely generated with generators  $\{\gamma^{j_n} \cdot \prod_{i=0}^{n-1} \alpha_i^{j_i} : 0 \leq j_i \leq d_i, 1 \leq i \leq n\}$ . Thus we have  $\gamma \in M$  and so  $\gamma \in \mathbb{A}$  by Theorem 2.1.5 as  $\gamma$  is in some finitely generated subring.  $\heartsuit$

## 3.2 Ideal Classes

**Definition 3.2.1.** Let  $R$  be a commutative ring with unity and  $\mathcal{I}$  be the set of all ideals of  $R$ . Define an equivalence relation  $\sim$  on  $\mathcal{I}$  as follows:  $A, B \in \mathcal{I}$ , we have

$$A \sim B \Leftrightarrow \exists \alpha, \beta \in R, \{\alpha, \beta\} \neq \{0\}, \alpha A = \beta B$$

**Definition 3.2.2.** Let  $R$  be a commutative ring and  $\mathcal{I}$  be the set of ideals. Then for  $A \in \mathcal{I}$ , the **ideal class** of  $A$ , denoted by  $[A]$ , is the equivalence class of  $A$  under the above equivalence relation. We let the **ideal classes of  $R$** , denoted by  $\mathcal{C}_R$ , be the set of non-trivial equivalence classes of  $\mathcal{I}/\sim$ , i.e.

$$\mathcal{C}_R := \{[A] : A \neq \langle 0 \rangle, A \in \mathcal{I}\}$$

**Proposition 3.2.3.** Let  $R$  be an integral domain. Then the set of non-trivial principal ideals forms a single equivalence class in  $\mathcal{C}_R$ .

*Proof.* Let  $I$  be an ideal of  $R$  and  $\alpha, \beta \in R, \alpha, \beta \neq 0$  such that  $\alpha I = \langle \alpha \rangle I = \langle \beta \rangle$ , we will show  $I$  is principal. Since  $\beta \in \langle \alpha \rangle I$ , we have  $\alpha \gamma = \beta$  where  $\gamma \in I$ . We claim  $I = \langle \gamma \rangle$ . Indeed, take  $\mu \in I$  be arbitrary, we have  $v \in R$  so  $\alpha \mu = v \beta$  and so

$$\alpha \mu = v \beta \Rightarrow \alpha(\mu - v\gamma) = 0 \Rightarrow \mu = v\gamma \Rightarrow \mu \in \langle \gamma \rangle$$

$\heartsuit$

**Remark 3.2.4.** The first goal of this section is to show  $\mathcal{C}_R$  forms a group. We already see by Proposition 3.2.3,  $[\langle a \rangle]$  is the identity element in  $\mathcal{C}_R$  where  $a \neq 0$ . Also, associativity is obvious, so the only thing left to check is existence of the inverses.

**Definition 3.2.5.** Let  $R$  be a commutative ring, we say  $R$  is **Noetherian** if every ascending chain of ideals stabilizes, i.e. if  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ , then there exists  $n \geq 1$  so that for all  $m \geq n$  we have  $I_n = I_m$ .

---

<sup>1</sup>Once  $z_i = a$ , then  $z_i \omega_i$  goes back to 0 as  $z_i \omega_i \in P$  now and so  $z_i \omega_i + P = 0 + P$

**Theorem 3.2.6.** *Let  $R$  be a commutative ring, the following are equivalent:*

1. *Every ideal in  $R$  is finitely generated.*
2.  *$R$  is Noetherian.*
3. *Every non-empty set of ideals in  $R$  has a maximal element.*

*Proof.* ( $2 \Leftrightarrow 1$ ): Given  $I_1 \subseteq I_2 \subseteq \dots$ , let  $I = \bigcup_{i \geq 0} I_i$ , this is an ideal of  $R$  because we have a chain of containment. By assumption  $I = \langle a_1, \dots, a_l \rangle$  for  $a_1, \dots, a_l \in R$ . Thus,  $a_1, \dots, a_l \in I_n$  for some  $n > 0$ . Hence  $I = \langle a_1, \dots, a_l \rangle \subseteq I_n$  and  $I_n \subseteq I$ . This imply  $I_n = I_{n+1} = I_{n+2} = \dots$

( $\neg 1 \Rightarrow \neg 2$ ): Suppose  $I$  is an ideal that is not finitely generated. Choose  $a_0 \in I, a_1 \in I \setminus \langle a_0 \rangle$  and inductively  $I_n = I \setminus \langle a_0, \dots, a_{n-1} \rangle$ . Then we get an ascending chain of proper containment, which imply  $R$  is not Noetherian.

( $2 \Rightarrow 3$ ) Say  $R$  is Noetherian. Let  $S$  be a non-empty set of ideals in  $R$ , then  $(S, \subseteq)$  is a poset. Pick  $I_1 \in S$ , if  $I_1$  is maximal then we are done. If  $I_1$  is not, then there exists  $I_2$  so  $I_1 \subsetneq I_2$ . Inductively doing so we see either it stops at one point, i.e. we get a maximal element, or we end up with an proper ascending chain, which contradicts Noetherianity.  $\heartsuit$

**Lemma 3.2.7.** *Let  $R$  be a Noetherian. Every non-zero ideal of  $R$  contains a non-zero product of prime ideals.*

*Proof.* Let  $S$  be the set of non-zero ideals in  $R$  which do not contain a product of prime ideals. If  $S$  is non-empty, then we can find a maximal element  $M$  in  $S$ .

Note this  $M$  is not prime, so there exists  $r, s \in R \setminus M$  with  $rs \in M$  as  $R/M$  is not an integral domain. Then consider  $M_1 = M + \langle r \rangle$  and  $M_2 = M + \langle s \rangle$ . Since  $M$  is maximal in  $S$  and  $M \subsetneq M_1$  and  $M \subsetneq M_2$ , we get  $M_1, M_2$  contains product of prime ideals. However, note

$$M_1 M_2 = (M + \langle r \rangle)(M + \langle s \rangle) = M \cdot M + r \cdot M + s \cdot M + \langle rs \rangle \subseteq M$$

Thus  $M$  contains a product of prime ideals, a contradiction. Thus we must have  $S$  is empty, i.e. every non-zero ideal of  $R$  contains non-zero product of prime ideals.  $\heartsuit$

**Lemma 3.2.8.** *Let  $R$  be a Dedekind domain and  $K$  be the field of fraction of  $R$ . Let  $I$  be proper ideal of  $R$ , then there is an element  $\gamma \in K \setminus R$  such that  $\gamma I \subseteq R$ .*

*Proof.* If  $I = \langle 0 \rangle$  then pick any element  $\gamma \in K \setminus R$  would suffice. Thus we assume  $I \neq \langle 0 \rangle$ .

Thus, there is  $0 \neq \alpha \in I$  and since  $I$  is proper,  $\alpha$  is not a unit. Thus, we have  $\frac{1}{\alpha} \notin R$ , i.e.  $\frac{1}{\alpha} \in K \setminus R$ . By Lemma 3.2.7,  $\langle \alpha \rangle$  contains a product of prime ideals, say  $\mathcal{P}_1, \dots, \mathcal{P}_r \subseteq \langle \alpha \rangle$  with  $\mathcal{P}_1, \dots, \mathcal{P}_r$  prime. Choose such a product with  $r$  minimal.

Let  $S$  be the set of proper ideals which contains  $I$ . The set  $S$  is not empty because  $I \in S$ . By Theorem 3.2.6, we note  $S$  contains maximal element  $M$ . In particular this  $M$  is actually a maximal ideal and so  $M$  is prime ideal of  $R$ .

Now we know  $M \supseteq I \supseteq \langle \alpha \rangle \supseteq \mathcal{P}_1 \dots \mathcal{P}_r$ , we claim there is a prime ideal  $\mathcal{P}_i$  such that  $M \supseteq \mathcal{P}_i$ . This is by the prime-ness of  $\mathcal{M}$ , i.e. we have  $\mathcal{P}_1 \dots \mathcal{P}_r \subseteq M$  imply  $\mathcal{P}_1 \subseteq M$  or  $\mathcal{P}_2 \dots \mathcal{P}_r \subseteq M$  and inductively we must have some  $\mathcal{P}_i \subseteq M$ . WLOG, we may assume  $\mathcal{P}_1 \subseteq M$ .

Then we have  $M = \mathcal{P}_1$  because  $R$  is a Dedekind domain, i.e. every prime is maximal. Now if  $r = 1$ , then we have  $\mathcal{P}_1 \subseteq \langle \alpha \rangle \subseteq I \subseteq M = \mathcal{P}_1$  and so  $\langle \alpha \rangle = I = \mathcal{P}_1 = M$ . Now take  $\gamma = \frac{1}{\alpha}$ , we have

$$\gamma I = \frac{1}{\alpha} \langle \alpha \rangle = R \subseteq R$$

If  $r > 1$ , then note  $\mathcal{P}_2, \dots, \mathcal{P}_r$  is not contained in  $\langle \alpha \rangle$  since  $r$  is minimal and we have  $\mathcal{P}_1 \dots \mathcal{P}_r \subseteq \langle \alpha \rangle \subseteq I \subseteq \mathcal{P}_1$ , i.e. if  $\mathcal{P}_2 \dots \mathcal{P}_r \subseteq \langle \alpha \rangle$  then we can replace  $\mathcal{P}_1 \dots \mathcal{P}_r$  with  $\mathcal{P}_2 \dots \mathcal{P}_r$ . Thus we can choose an element  $\beta \in \mathcal{P}_2 \dots \mathcal{P}_r$  such that  $\beta \notin \langle \alpha \rangle$  and let  $\gamma = \frac{\beta}{\alpha}$ . Then  $\gamma \in K \setminus R$  and we have

$$\gamma I = \frac{\beta}{\alpha} I \subseteq \frac{\beta}{\alpha} \mathcal{P}_1 \subseteq \frac{\langle \beta \rangle \mathcal{P}_1}{\alpha} \subseteq \frac{\mathcal{P}_1 \dots \mathcal{P}_r}{\alpha} \subseteq \frac{\langle \alpha \rangle}{\alpha} = R$$

♡

**Theorem 3.2.9.** *Let  $R$  be a Dedekind domain and  $I$  be a non-zero ideal of  $R$ . Then there exists a non-zero ideal  $J$  such that  $IJ$  is principal.*

*Proof.* If  $I$  is the zero ideal then the result is immediate. Thus we may assume  $I$  is non-zero with  $0 \neq \alpha \in I$ . Consider the subset  $J$  of  $R$  defined as follows

$$J = \{\beta \in R : \beta I \subseteq \langle \alpha \rangle\}$$

It is easy to check  $J$  is indeed a non-zero ideal and it is clear from the definition we have  $IJ \subseteq \langle \alpha \rangle$ . Thus it suffice to show  $\langle \alpha \rangle \subseteq IJ$ . Therefore, consider the set

$$A = \frac{1}{\alpha} IJ = \{\beta \in K : \beta \alpha \in IJ\}$$

This is contained in  $R$  since  $IJ \subseteq \langle \alpha \rangle$  and it is easy to see  $A$  is an ideal. If  $A = R$ , then  $IJ = \langle \alpha \rangle$  as desired. Thus, we may assume  $A$  is proper. Therefore, by Lemma 3.2.8, there exists  $\gamma \in \text{Frac}(R) \setminus R$  such that  $\gamma A \subseteq R$ . We will show  $\gamma \in R$  to get a contradiction. To do this, it suffice to show  $\gamma$  is integral over  $R$  since  $R$  is Dedekind domain and hence integrally closed.

Observe  $A$  contains  $J$  since  $\alpha \in I$ , thus

$$\gamma J \subseteq \gamma A \subseteq R$$

Since  $\gamma A \subseteq R$  we see

$$\gamma \left( \frac{1}{\alpha} IJ \right) \subseteq R \Rightarrow (\gamma J) I \subseteq \langle \alpha \rangle \Rightarrow \gamma J \subseteq J$$

The last inclusion follows from definition of  $J$ . The ideal  $J$  is finitely generated additive group (thus finite subalgebra) and hence by invoke Proposition 3.1.5 or apply a proof similar to the proof of theorem 2.1.5 we obtain  $\gamma \in J$  imply  $\gamma$  is integral over  $R$ .  $\heartsuit$

**Corollary 3.2.9.1.** *The ideal class in a Dedekind domain forms a group, and it is called the **ideal class group**, denoted by  $\mathcal{C}_R$ .*

*Proof.* Theorem 3.2.9 imply every ideal has an inverse (we have ideal  $J$  so that  $IJ$  is principal, which is the identity in  $\mathcal{C}_K$ ) and thereform  $\mathcal{C}_K$  is indeed a group.  $\heartsuit$

### 3.3 Prime Decomposition

**Proposition 3.3.1.** *Let  $A, B, C$  be ideals with  $C \neq \langle 0 \rangle$  in Dedekind domain  $R$ . Then  $AC = BC$  imply  $A = B$ .*

*Proof.* We can find non-zero ideal  $J$  so  $JC = CJ = \langle c \rangle$  for some non-zero  $c \in R$ . Thus  $AC = BC$  imply  $ACJ = BCJ$  imply  $\langle c \rangle A = \langle c \rangle B$  and so  $A = B$  as  $R$  is integral domain.  $\heartsuit$

**Proposition 3.3.2.** *If  $A$  and  $B$  are ideals in a Dedekind domain  $R$ , then  $A \supseteq B$  if and only if  $A \mid B$ , i.e. there exists ideal  $C$  so  $B = AC$ .*

*Proof.* Suppose  $A \mid B$ , then  $AC = B$  and so  $B \subseteq A$  as  $AC \subseteq A \cap C$  and so  $B \subseteq A \cap C \subseteq A$ .

Conversely, suppose  $A \supseteq B$  and fix  $J$  such that  $AJ = \langle a \rangle$  for some  $0 \neq a \in R$ . Let  $C = \frac{1}{a}JB$  and we have  $C = \frac{1}{a}JB \subseteq \frac{1}{a}JA \subseteq \frac{1}{a}\langle a \rangle = R$  and so  $C$  is actually an ideal of  $R$ . Thus we have

$$AC = A \frac{1}{a}JB = \left(\frac{1}{a}JA\right)B = \left(\frac{1}{a}\langle a \rangle\right)B = RB = B$$

$\heartsuit$

**Theorem 3.3.3.** *Every non-zero proper ideal in a Dedekind domain  $R$  has a unique factorization into prime ideals, up to reordering.*

*Proof.* First we show every ideal is representable as a product of prime ideals. Let  $S$  be the set of non-zero proper ideals which cannot be written as a product of prime ideals. If  $S$  is non-empty, then there exists a maximal element  $M$  in  $S$ . Then  $M$  is contained in a maximal ideal  $P$  of  $R$ . Observe since  $M \in S$ , we must have  $M \neq P$  so  $M \subsetneq P$ . Now by Proposition 3.3.2, we have a proper ideal  $C$  so that  $M = PC$ . Since  $M \in S$  we must have  $C$  is not a product of prime ideals and so  $C \in S$ . However, note  $M \subsetneq C$  as  $M \subsetneq P$  and this contradicts the maximality of  $M$ .

Thus, every proper ideal can be written as a product of prime ideals. We will now show uniqueness. Suppose  $P_1 \dots P_r = Q_1 \dots Q_s$  where  $P_i$ 's and  $Q_j$ 's are prime ideals. Since  $P_1$  is a prime ideal and  $P_1 \supseteq Q_1 \dots Q_s$  we must have  $P_1 \supseteq Q_j$  for some  $1 \leq j \leq s$ . WLOG, say  $P_1 \supseteq Q_1$ . However, note  $Q_1$  is prime and so  $Q_1$  is maximal, we must have  $Q_1 = P_1$ . Doing this inductively we see  $r = s$  and  $P_i = Q_i$  as desired.  $\heartsuit$

**Corollary 3.3.3.1.** *Let  $K$  be a number field, then every ideal in the ring of integers has a unique factorization into product of prime ideals, up to a reordering.*

*Proof.* Recall ring of integers is an Dedekind domain by Theorem 3.1.17 and so by Theorem 3.3.3, we have our desired claim.  $\heartsuit$

**Remark 3.3.4.** We also could also prove this theorem using commutative algebra. Namely, let  $R$  be Dedekind domain, then  $R$  is Noetherian, hence every ideal in  $R$  is decomposable using primary decomposition. In particular, this primary decomposition is unique and we only need to show those primary ideals can be further factored into prime ideals.

Indeed, we can use the integrally closed property to ensure that every primary ideal is a power of a prime ideal and thus we get the unique factorization into prime ideals as desired.

**Remark 3.3.5.** The following are not in the original note.

**Lemma 3.3.6.** *Let  $R$  be a Dedekind domain and  $P$  a prime ideal of  $R$ . Then every ideal in  $R/P^k$  is generated by one element.*

*Proof.* Now, let  $I/P^k$  be any proper ideal in  $R/P^k$ , by correspondence theorem, we have  $P^k \subsetneq I \subsetneq R$ . In particular, observe since  $P^k \subseteq I$  we must have  $I$  divides  $P^k$ , i.e.  $IC = P^k$  for some ideal  $C$ . However, by unique prime factorization of Dedekind domains, this imply  $I = P^i$  for  $1 \leq i \leq k$ , this classifies all ideals in  $R/P^k$ .

Now, suppose if  $P = P^2$ , then we have  $P = P^n$  for all  $n \geq 1$  and in particular this imply  $R/P^k$  is  $R/P$  which is a field, i.e. every ideal is indeed generated by one elements. Then, suppose  $P \neq P^2$  and so we can find  $\alpha \in P \setminus P^2$ . In light of this, we observe  $\langle \alpha \rangle \subseteq P$  and on the other hand, we have  $\langle \alpha \rangle \not\subseteq P^i$  for  $1 < i \leq k$ . Now,  $\langle \alpha \rangle/P^k$  is an ideal in  $R/P^k$  while it is not equal any of  $P^i/P^k$  for all  $1 < i \leq k$  and so we have  $\langle \alpha \rangle/P^k = P/P^k$ , i.e.  $P/P^k$  is generated by one single element in  $R/P^k$ . Hence  $P^i/P^k = \langle \alpha^i \rangle/P^k$  and the proof follows.  $\heartsuit$

**Corollary 3.3.6.1.** *Let  $R$  be a Dedekind domain and  $I$  a proper ideal of  $R$ , then  $R/I$  is a principal ideal ring (every ideal is generated by one element).*

*Proof.* Note  $I$  admits a prime factorization, say  $I = \prod_{i=1}^n P_i^{q_i}$ . Now, let  $P_i^{q_i}$  and  $P_j^{q_j}$  be arbitrary with  $i \neq j$ , we have  $P_i^{q_i} + P_j^{q_j} \subseteq R$ . Now, observe we can find

$x \in P_i$  and  $y \in P_j$  so  $x + y = 1 \in R$  as  $P_i$  and  $P_j$  are disjoint maximal ideals hence comaximal. Thus we have  $(x + y)^{q_i + q_j - 1} = 1$  is an element of  $P_i^{q_i} + P_j^{q_j}$ , i.e. they are comaximal as well. Hence we can use Chinese Remainder Theorem to conclude

$$R/I \cong \bigoplus_{i=1}^n R/P_i^{q_i}$$

Now observe if  $R = A \oplus B$  with both  $A$  and  $B$  being principal ideal ring, then we have  $R$  is principal ideal ring. Indeed, let  $I$  be an ideal of  $R$ , then  $I = I_1 \oplus I_2$  where  $I_1 \in A$  and  $I_2 \in B$ , then  $I = \langle \alpha \rangle \oplus \langle \beta \rangle = \langle (\alpha, \beta) \rangle$ . Thus inductively we see  $R/I$  is indeed principal ideal ring as we apply Lemma 3.3.6 to each  $R/P_i^{q_i}$ .  $\heartsuit$

**Theorem 3.3.7.** *Let  $I$  be a non-zero ideal in a Dedekind domain  $R$ , and  $0 \neq \alpha \in I$ . Then there exists  $\beta \in I$  such that  $I = \langle \alpha, \beta \rangle$ .*

*Proof.* Note the proof is not included in the original note.

First, observe by Lemma 3.3.6.1, we have  $R/\langle \alpha \rangle$  is a principal generated ring and  $I/\langle \alpha \rangle$  is an principal ideal. Viz, either we have  $I/\langle \alpha \rangle = 0$ , i.e.  $I = \langle \alpha \rangle$ , or we have  $I/\langle \alpha \rangle = \langle \beta + \langle \alpha \rangle \rangle$  for some  $\beta \notin \langle \alpha \rangle$ . Thus we have  $I = \langle \alpha \rangle + \langle \beta \rangle = \langle \alpha, \beta \rangle$  as desired.

$\heartsuit$

## Chapter 4

### Ideals In Ring of Integers

春未老，风细柳斜斜。试上超然台上看，半壕春水一城花。烟雨暗千家。  
寒食后，酒醒却咨嗟。休对故人思故国，且将新火试新茶。诗酒趁年华。

苏轼

#### 4.1 Splitting Primes in $\mathcal{O}_K$

**Proposition 4.1.1.** *Let  $K$  be a number field and  $P$  a prime ideal of  $\mathcal{O}_K$ . Then there exists a unique prime number  $p \in \mathbb{Z}_{\geq 1}$  such that  $P \mid \langle p \rangle \in \mathcal{O}_K$ .*

*Proof.* By Lemma 3.1.13, there exists positive integer  $a$  such that  $a \in P$ . Then let  $a = p_1 \cdots p_l$  be the prime factorization (into integers) of  $a$  and by primeness of  $P$  we have some  $1 \leq j \leq l$  so that  $p_j \in P$ . In particular, if this is the case then  $P \mid \langle p_j \rangle$ . We are left to show uniqueness. Suppose there exists  $P \mid \langle p \rangle$  and  $P \mid \langle q \rangle$  where both  $p$  and  $q$  are primes and  $p \neq q$ . Then we have  $ap + bq = 1$  as  $\gcd(p, q) = 1$ . Thus we have  $P \mid \langle ap + bq \rangle = 1$  and so  $P \mid R$ , i.e.  $P = R$ , which contradicts the fact  $P$  is a proper ideal.  $\heartsuit$

**Corollary 4.1.1.1.** *Let  $K$  be a number field and  $P$  a prime ideal in  $\mathcal{O}_K$ . Then  $P \cap \mathbb{Z} = p\mathbb{Z}$  for some prime integer numbers.*

*Proof.* By Proposition 4.1.1, we have  $p \in \mathbb{Z}_{\geq 1}$  such that  $P \mid \langle p \rangle$ . Then we observe  $P \cap \mathbb{Z}$  is a proper ideal of  $\mathbb{Z}$ . Since  $p \in P \cap \mathbb{Z}$  we have  $P \cap \mathbb{Z} \supseteq p\mathbb{Z}$ . However, observe

$p\mathbb{Z}$  is a maximal ideal in  $\mathbb{Z}$  so we must have  $P \cap \mathbb{Z} = p\mathbb{Z}$ .  $\heartsuit$

**Corollary 4.1.1.2.** *Let  $K$  be a number field and  $P$  a prime ideal of  $\mathcal{O}_K$  and  $P \cap \mathbb{Z} = p\mathbb{Z}$  for some prime integers  $p \in \mathbb{Z}$ . Then  $P$  appears in the prime decomposition of  $p\mathcal{O}_K = \langle p \rangle := \{kp : k \in \mathcal{O}_K\} \subseteq \mathcal{O}_K$ .*

*Proof.* Observe we have  $P \supseteq \langle p \rangle$  so we have  $P \mid \langle p \rangle$ . Thus the proof follows.  $\heartsuit$

**Example 4.1.2.** Let  $K = \mathbb{Q}(\sqrt{-5})$ . Then  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$  as we recall Corollary 2.7.10.2. Then we observe  $\langle 2 \rangle$  is not a prime ideal in  $\mathcal{O}_K$  because  $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in \langle 2 \rangle$  but both  $1 + \sqrt{-5}$  and  $1 - \sqrt{-5}$  are not in  $\langle 2 \rangle$  as we observe  $\langle 2 \rangle = 2 \cdot \mathcal{O}_K$  so  $\langle 2 \rangle = \{2a + 2b\sqrt{-5} : a, b \in \mathbb{Z}\}$  and  $1 \neq 2a$  for some  $a \in \mathbb{Z}$ .

Now, what is the prime factorization of  $\langle 2 \rangle$ ? Suppose  $P \mid \langle 2 \rangle$ , then we have  $2 \in P$  and by Theorem 3.3.7, we can find  $\alpha \in \mathbb{Z}[\sqrt{-5}]$  so  $P = \langle 2, \alpha \rangle$ . Now, observe we must have  $\mathbb{Z}[\sqrt{-5}]/P \cong (\mathbb{Z}[\sqrt{-5}]/\langle 2 \rangle)/\langle \alpha + \langle 2 \rangle \rangle$ , i.e. we can quotient out 2 first, then quotient the quotient ring with the image of  $\alpha$  in  $\mathbb{Z}[\sqrt{-5}]/\langle 2 \rangle$  and obtain the same ring. Hence, we consider the set  $S$  of representatives of the quotient ring  $\mathbb{Z}[\sqrt{-5}]/\langle 2 \rangle$ , i.e.

$$S = \{0, 1, \sqrt{-5}, 1 + \sqrt{-5}\}$$

and we know  $\alpha \in S$ .

Observe if  $\alpha = \sqrt{-5}$  then  $-\alpha^2 - 2 \cdot 2 = 1 \in P$  and so  $P = \mathbb{Z}[\sqrt{-5}]$ , a contradiction. Similarly we cannot have  $\alpha = 1$ . If  $\alpha = 0$  then  $P = \langle 2 \rangle$ , which is not a prime, contradiction. Hence we must have  $\alpha = 1 + \sqrt{-5}$  is the only possibility. Therefore, if  $P$  is a prime factor of  $\langle 2 \rangle$ , then  $P = \langle 2, 1 + \sqrt{-5} \rangle$ . Now we only need to compute the power of  $P$ . Observe

$$P^2 = \langle 2, \alpha \rangle \langle 2, \alpha \rangle = \langle 4, 2\alpha, 2\alpha, \alpha^2 \rangle = \langle 4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-4} \rangle = \langle 2 \rangle$$

Thus, we have the prime factorization of  $\langle 2 \rangle$  in  $\mathcal{O}_K$  is  $\langle 2 \rangle = \langle 1 + \sqrt{-5}, 2 \rangle^2$ .

**Definition 4.1.3.** Let  $K$  be a number field and  $p$  a prime number in  $\mathbb{Z}_{\geq 1}$ . Then the ideal  $\langle p \rangle = p\mathcal{O}_K$  can be factored as a product of prime ideals in  $\mathcal{O}_K$ , say  $\langle p \rangle = \prod_{i=1}^n P_i^{k_i}$ . Then we say:

1. If  $P$  appears in the prime factorization of  $\langle p \rangle$ , then  $P$  **lies over**  $p$ .
2. Let  $P$  lies over  $p$ , say  $P = P_i$ , then the exponent  $k_i$  is called the **ramification index of  $P$** , denoted<sup>1</sup> by  $e(P|p)$ . If for  $p \in \mathbb{Z}_{\geq 1}$ , there exists at least one prime ideal  $P \leq \mathcal{O}_K$  such that  $e(P|p) \geq 2$ , then we say  $p$  **ramifies in  $K$**  and otherwise say  $p$  **unramifies in  $K$**  (or unramified over  $K$ ).
3. Let  $P$  be a prime lies over  $p$ . Then the inclusion  $\phi : \mathbb{Z} \rightarrow \mathcal{O}_K$  induces a homomorphism<sup>2</sup>  $\pi : \mathbb{Z} \rightarrow \mathcal{O}_K/P$  whose kernel is  $p\mathbb{Z}$ . Therefore, we have an embedding<sup>3</sup> induced by  $\pi$  from  $\mathbb{Z}/p\mathbb{Z} \rightarrow \mathcal{O}_K/P$ , where we observe both  $\mathbb{Z}/p\mathbb{Z}$  and  $\mathcal{O}_K/P$  are fields, i.e. we get a field extension. The finite field  $\mathcal{O}_K/P$

---

<sup>1</sup>Note this does not make sense if  $P$  does not lie over  $p$

<sup>2</sup>Namely, the homomorphism is  $z \mapsto z + P$

<sup>3</sup>Namely, the embedding is  $z + p\mathbb{Z} \mapsto z + P$



with characteristic  $p$  is called a **residue field**. The degree of  $\mathcal{O}_K/P$  over the finite field  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  is called the **inertial degree of  $P$  over  $p$** , denoted by  $f(P|p)$ .

**Example 4.1.4.** Let  $K = \mathbb{Q}(\sqrt{-5})$  and  $p = 2$ , we have

1. The only prime lies over 2 is  $P = \langle 2, 1 + \sqrt{-5} \rangle$ .
2. The ramification index  $e(P|p)$  is 2 as  $\langle 2 \rangle = P^2$ . Thus  $\langle 2 \rangle$  ramifies in  $K$ .
3. The residue field  $\mathcal{O}_K/P$  is equal  $\mathbb{F}_2$  itself and so the inertial degree  $f(P|p)$  is 1.

**Theorem 4.1.5.** Let  $K$  be a number field and  $D$  the discriminant of  $K$ . If  $p$  is a prime in  $\mathbb{Z}$  and  $p \nmid D$ . Then  $p$  is unramified over  $K$ .

*Proof.* Let  $P$  be a prime ideal of  $\mathcal{O}_K$  lying over  $p$  such that  $e(P|p) > 1$ . Let  $\langle p \rangle = PI$  with  $I$  divisible by all prime ideals lying over  $p$ , i.e. since  $\langle p \rangle = P^{e(P|p)} \cdot \prod_{i=1}^n P_i^{e(P_i|p)}$ , then we just let  $I = P^{e(P|p)-1} \prod_{i=1}^n P_i^{e(P_i|p)}$ .

Let  $\sigma_1, \dots, \sigma_n$  be all the embeddings of  $K$  in  $\mathbb{C}$  which fix  $\mathbb{Q}$  and extend all  $\sigma_i$  to automorphisms of some normal extension  $L$  of  $K$ . Let  $\omega_1, \dots, \omega_n$  be an integral basis for  $\mathcal{O}_K$  and now we will replace one  $\omega_i$  by a suitable new element which makes  $p$  divide  $\text{disc}(K)$  and this will prove our theorem as  $p$  is ramified over  $K$  would imply  $p \mid \text{disc}(K)$ .

Take any  $\omega \in I \setminus \langle p \rangle$ , then  $\omega$  is in every prime ideal of  $\mathcal{O}_K$  lying over  $p$  but not in  $\langle p \rangle$ . Let  $\omega = \sum_{i=1}^n m_i \omega_i$  with  $m_i \in \mathbb{Z}$ , we can find  $m_j$  such that  $p \nmid m_j$  since  $\omega \notin \langle p \rangle$ . WLOG, assume  $p \nmid m_1$  and we set

$$d = \text{disc}(\omega, \omega_2, \dots, \omega_n)$$

Then we have

$$d = m_1^2 D$$

by basic linear algebra and since  $p \nmid m_1$ , it suffice to show  $p \mid d$  and we would have  $p \mid D$  as desired.

Recall  $\omega$  is in every prime ideal of  $\mathcal{O}_K$  lies over  $p$  and it follows that  $\omega$  is in every prime ideal of  $\mathcal{O}_L$  that lies over  $p$ . To see this<sup>1</sup>, observe if  $Q \leq \mathcal{O}_L$  is prime, then we would have  $Q \cap \mathcal{O}_K$  is still prime ideal and it contains  $\langle p \rangle$ . Hence  $Q \cap \mathcal{O}_K$  is a prime ideal in  $\mathcal{O}_K$  lies over  $p$ , i.e.  $\omega \in Q \cap \mathcal{O}_K \subseteq Q$  as desired.

Now, fix any prime ideal  $Q$  of  $\mathcal{O}_L$  lying over  $p$ , we claim  $\sigma(\omega) \in Q$  for all automorphisms  $\sigma$  of  $L$ . To see this, observe  $\sigma^{-1}(Q)$  is a prime ideal of  $\sigma^{-1}(\mathcal{O}_L)$  as  $\sigma^{-1}(\mathcal{O}_L)/\sigma^{-1}(Q) \cong \mathcal{O}_L/Q \cong \mathbb{F}_{p^{f(Q|p)}}$  is a finite field (we actual see it is a maximal ideal). Since  $L$  is normal over  $\mathbb{Q}$  we have<sup>2</sup>  $\sigma^{-1}(\mathcal{O}_L) = \mathcal{O}_L$ . Thus, we have  $\sigma^{-1}(Q)$  is

<sup>1</sup>A quick way to observe this is by saying prime ideal contraction is still prime

<sup>2</sup>Observe this claim does not require  $L$  to be normal. As long as  $\sigma : L \rightarrow L$  is a automorphism, we would have  $\sigma$  fix  $\mathbb{Q}$  and so  $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$  as  $f(\alpha) = 0$  imply  $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$  with  $\alpha \in \mathcal{O}_L$  and  $f(x) \in \mathbb{Z}[x]$ . Then because  $\mathcal{O}_L$  is finitely generated as it admits a integral basis, we have  $\sigma(\mathcal{O}_L)$  actually equal  $\mathcal{O}_L$  by dimension consideration

a prime ideal in  $\mathcal{O}_L$  which lies over  $p$  as  $\sigma$  fix the element  $p$ , i.e.  $p \in \sigma^{-1}(Q)$ . Since  $\omega$  is in every prime ideal of  $\mathcal{O}_L$  lying over  $p$ , we have  $\omega \in \sigma^{-1}(Q)$  and so  $\sigma(\omega) \in Q$ .

Thus, we have  $\sigma_i(\omega) \in Q$  for all  $1 \leq i \leq n$  and by definition, we know  $\text{disc}(\omega, \omega_2, \dots, \omega_n) \in Q$ . However, at the same time observe  $D, m_1^2$  are both in  $\mathbb{Z}$  so  $d$  is in  $\mathbb{Z}$ . Therefore,  $d \in Q \cap \mathbb{Z}$  and now we claim  $Q \cap \mathbb{Z} = p\mathbb{Z}$ . Indeed,  $\mathbb{Z} \cap Q$  is a proper ideal which contains  $p\mathbb{Z}$  where  $p\mathbb{Z}$  is a maximal ideal in  $\mathbb{Z}$ , i.e.  $Q \cap \mathbb{Z} = p\mathbb{Z}$ . Hence  $d \in p\mathbb{Z}$  and so  $p \mid d$  as desired. The proof follows.  $\heartsuit$

**Remark 4.1.6.** Suppose

$$\langle p \rangle = P_1^{e_1} \dots P_r^{e_r}$$

Then we can show  $p^k \mid \text{disc}(K)$  where

$$k = \sum_{i=1}^r (e(P_i|p) - 1)f(P_i|p)$$

**Example 4.1.7.** Let  $K = \mathbb{Q}(\sqrt{-5})$ , we have  $\text{disc}(K) = -20$ . Thus, the possible ramified primes are 2 and 5 as we have ramified imply  $p \mid \text{disc}(K)$  by Theorem 4.1.5. We already seen  $\langle 2 \rangle = \langle 2, 1 + \sqrt{-5} \rangle^2$  and observe  $\langle 5 \rangle = \langle \sqrt{-5} \rangle^2$  and so both of them are ramified.

**Remark 4.1.8.** Note the converse of Theorem 4.1.5 is also true, i.e.  $p \mid \text{disc}(K)$  then  $p$  is ramified in  $K$ .

## 4.2 Norm on Ideals

**Definition 4.2.1.** Let  $K$  be a number field and  $\mathcal{I}$  an ideal of  $\mathcal{O}_K$ . Then we define the norm of  $\mathcal{I}$  to be the number of the cosets modulo  $\mathcal{I}$  in  $\mathcal{O}_K$ , i.e.

$$N(\mathcal{I}) := N_{\mathbb{Q}}^K(\mathcal{I}) := \|\mathcal{I}\| := |\mathcal{O}_K/\mathcal{I}|$$

**Theorem 4.2.2.** Let  $K$  be a number field and  $\mathcal{I} \leq \mathcal{O}_K$ . Let  $\{\alpha_1, \dots, \alpha_n\}$  be an integral basis for  $\mathcal{I}$ , then

$$N(\mathcal{I}) = \left( \frac{\text{disc}(\alpha_1, \dots, \alpha_n)}{\text{disc}(K)} \right)^{\frac{1}{2}}$$

*Proof.* Let  $D = \text{disc}(K)$ . First we observe every integral basis for  $\mathcal{I}$  has the same discriminant. Now let  $\{\omega_1, \dots, \omega_n\}$  be an integral basis of  $\mathcal{O}_K$  and  $\{\alpha_1, \dots, \alpha_n\}$  be an integral basis for  $\mathcal{I}$  given by Theorem 3.1.16 of the lower triangular form. Viz, we

have

$$\begin{aligned}
\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} &= \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix} \\
\Rightarrow \text{disc}(\alpha_1, \dots, \alpha_n) &= \begin{vmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}^2 \cdot \text{disc}(\omega_1, \dots, \omega_n) \\
\Rightarrow \frac{\text{disc}(\alpha_1, \dots, \alpha_n)}{D} &= \left( \prod_{i=1}^n a_{ii} \right)^2 \\
\Rightarrow \left| \frac{\text{disc}(\alpha_1, \dots, \alpha_n)}{D} \right|^{1/2} &= a_{11} \dots a_{nn}
\end{aligned}$$

Thus, it suffice to prove  $N(\mathcal{I}) = a_{11} \dots a_{nn}$ .

First, we show that if

$$\sum r_i \omega_i \equiv \sum s_i \omega_i \pmod{\mathcal{I}} \quad (\text{Eq. 4.2.1})$$

with  $0 \leq r_i, s_i < a_{ii}$  for  $i = 1, \dots, n$ , then  $r_i = s_i$  for all  $1 \leq i \leq n$ . Note this will imply  $N(\mathcal{I}) \geq a_{11} \dots a_{nn}$ .

Assume the claim in Equation [Eq. 4.2.1](#), then we have

$$(r_1 - s_1)\omega_1 + \dots + (r_n - s_n)\omega_n \in \mathcal{I}$$

Recall from the proof of Theorem [3.1.16](#) that  $a_{nn}$  is the smallest positive integer occurring as the coefficient of  $\omega_n$  in a linear combination of  $\omega_1, \dots, \omega_n$  which is in  $\mathcal{I}$ , therefore, we have  $a_{nn} \mid (r_n - s_n)$ . Indeed, note  $\sum (r_i - s_i)\omega_i = \sum k_i \alpha_i$  with  $k_i \in \mathbb{Z}$  by definition of  $\alpha_i$ 's. Therefore we have

$$\sum (r_i - s_i)\omega_i = k_1 a_{11} \omega_1 + (k_2 a_{21} + k_2 a_{22})\omega_2 + \dots + (k_n a_{n1} + \dots + k_n a_{nn})\omega_n$$

and by uniqueness of the representation, we must have  $k_n a_{nn} = r_n - s_n$ , i.e.  $a_{nn} \mid r_n - s_n$  and so  $r_n = s_n$  as  $0 \leq r_n, s_n < a_{nn}$ .

Inductively we could deduce that  $a_{ii} \mid r_i - s_i$  for all  $i$  and then  $r_i = s_i$  for all  $i$ . Thus  $N(\mathcal{I}) \geq a_{11} \dots a_{nn}$ .

Now let  $\gamma \in \mathcal{O}_K$  so  $\gamma = b_1 \omega_1 + \dots + b_n \omega_n$  with  $b_1, \dots, b_n \in \mathbb{Z}$ . Then there exists  $q_n, r_n \in \mathbb{Z}$  with  $0 \leq r_n < a_{nn}$  such that  $b_n = q_n a_{nn} + r_n$ . Then

$$\gamma \equiv \gamma - q_n \alpha_n \equiv \sum (b_i - q_n a_{ni}) \omega_i \equiv c_1 \omega_1 + \dots + c_{n-1} \omega_{n-1} + r_n \omega_n \pmod{\mathcal{I}}$$

with  $c_i = b_i - q_n a_{ni}$  for  $i = 1, \dots, n-1$ . By repeating the process, there exists  $r_1, \dots, r_n \in \mathbb{Z}$  with  $0 \leq r_i < a_{ii}$  for all  $i$  such that

$$\gamma \equiv r_1 \omega_1 + \dots + r_n \omega_n \pmod{\mathcal{I}}$$

Thus  $N(\mathcal{I}) \leq a_{11} \dots a_{nn}$  and the proof follows. ♡

**Theorem 4.2.3.** Let  $K$  be a number field and  $\mathcal{I}$  an ideal of  $\mathcal{O}_K$ . Suppose  $\mathcal{I} = \langle \alpha \rangle$  then  $N(\mathcal{I}) = |N_{\mathbb{Q}}^K(\alpha)|$ .

*Proof.* Observe if  $\{\omega_1, \dots, \omega_n\}$  is an integral basis of  $K$  then  $\{\alpha\omega_1, \dots, \alpha\omega_n\}$  is an integral basis of  $\mathcal{I}$ . Let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $K$  in  $\mathbb{C}$  fixing  $\mathbb{Q}$ , then we have

$$\begin{aligned} \text{disc}(\alpha\omega_1, \dots, \alpha\omega_n) &= \begin{vmatrix} \sigma_1(\alpha\omega_1) & \dots & \sigma_1(\alpha\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha\omega_1) & \dots & \sigma_n(\alpha\omega_n) \end{vmatrix}^2 = \begin{vmatrix} \sigma_1(\alpha)\sigma_1(\omega_1) & \dots & \sigma_1(\alpha)\sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha)\sigma_n(\omega_1) & \dots & \sigma_n(\alpha)\sigma_n(\omega_n) \end{vmatrix}^2 \\ &= \left( \begin{vmatrix} \sigma_1(\alpha) & 0 & \dots & 0 \\ 0 & \sigma_2(\alpha) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n(\alpha) \end{vmatrix} \cdot \underbrace{\begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_n) \end{vmatrix}}_{= \text{disc}(K)^{1/2}} \right)^2 \\ &= N_{\mathbb{Q}}^K(\alpha)^2 \cdot \text{disc}(K) \end{aligned}$$

Now use Theorem 4.2.2, we have

$$\begin{aligned} N(\mathcal{I}) &= \left( \frac{N_{\mathbb{Q}}^K(\alpha)^2 \cdot \text{disc}(K)}{\text{disc}(K)} \right)^{\frac{1}{2}} \\ &= |N_{\mathbb{Q}}^K(\alpha)| \end{aligned}$$

♡

**Proposition 4.2.4.** Let  $K$  be a number field and  $\mathcal{I} \leq \mathcal{O}_K$  an ideal of  $\mathcal{O}_K$ , then  $N(\mathcal{I}) \in \mathcal{I}$ .

*Proof.* Let  $\{\alpha_i : 1 \leq i \leq N(\mathcal{I})\}$  be a complete set of representatives of the cosets, then  $\{1 + \alpha_i : 1 \leq i \leq N(\mathcal{I})\}$  is also a complete set of representatives. Hence we have

$$\sum \alpha_i \equiv \sum (1 + \alpha_i) \pmod{\mathcal{I}} \Rightarrow N(\mathcal{I}) \equiv 0 \pmod{\mathcal{I}} \Rightarrow N(\mathcal{I}) \in \mathcal{I}$$

♡

### 4.3 Norms and Indices

**Definition 4.3.1.** Let  $K$  be a number field and  $\mathcal{B}, \mathcal{C}$  be two ideals in  $\mathcal{O}_K$ . Then

1. We say an ideal  $\mathcal{D}$  in  $\mathcal{O}_K$  is the **greatest common divisor** of  $\mathcal{B}$  and  $\mathcal{C}$ , denoted by  $\gcd(\mathcal{B}, \mathcal{C})$ , if  $\mathcal{D} \mid \mathcal{B}, \mathcal{D} \mid \mathcal{C}$ , and  $\mathcal{E} \mid \mathcal{B}, \mathcal{E} \mid \mathcal{C} \Rightarrow \mathcal{D} \mid \mathcal{E}$  for all ideals  $\mathcal{E} \leq \mathcal{O}_K$ .

2. We say an ideal  $\mathcal{F}$  of  $\mathcal{O}_K$  is the **least common multiple** of  $\mathcal{B}$  and  $\mathcal{C}$ , denoted by  $lcm(\mathcal{B}, \mathcal{C})$ , if  $\mathcal{B} \mid \mathcal{F}, \mathcal{C} \mid \mathcal{F}$ , and  $\mathcal{B} \mid \mathcal{G}, \mathcal{C} \mid \mathcal{G} \Rightarrow \mathcal{F} \mid \mathcal{G}$  for all ideals  $\mathcal{G} \leq \mathcal{O}_K$ .

**Definition 4.3.2.** We say two ideals in  $\mathcal{O}_K$ ,  $\mathcal{B}, \mathcal{C} \leq \mathcal{O}_K$ , are **relatively prime** if  $gcd(\mathcal{B}, \mathcal{C}) = \langle 1 \rangle = \mathcal{O}_K$ .

**Remark 4.3.3.** By the unique prime factorization on ideals, we have  $gcd(\mathcal{B}, \mathcal{C}) = \mathcal{B} + \mathcal{C}$  and  $lcm(\mathcal{B}, \mathcal{C}) = \mathcal{B} \cap \mathcal{C}$ . Indeed, say  $\mathcal{B} = \mathcal{P}_1^{b_1} \dots \mathcal{P}_r^{b_r}$  and  $\mathcal{C} = \mathcal{Q}_1^{c_1} \dots \mathcal{Q}_k^{c_k}$  where  $\mathcal{P}_i, \mathcal{Q}_i$  are all prime ideals with  $\mathcal{P}_i = \mathcal{Q}_i$  for  $i = 1, \dots, l$  where  $l \leq \min(r, k)$ , then we should have

$$gcd(\mathcal{B}, \mathcal{C}) = \mathcal{P}_1^{\min(c_1, b_1)} \dots \mathcal{P}_l^{\min(c_l, b_l)}$$

and similarly we should have  $lcm(\mathcal{B}, \mathcal{C})$  be the product of all distinct primes in the list  $\{\mathcal{P}_i\} \cup \{\mathcal{Q}_j\}$  to the power of  $\max(c_i, b_i)$ .

**Theorem 4.3.4 (Chinese Remainder Theorem).** Assume  $I_1, \dots, I_n$  are pairwise co-maximal (or coprime, or relatively prime) ideals in a commutative ring  $R$  with unity. Then

$$R/(I_1 \cap I_2 \cap \dots \cap I_n) \cong R/I_1 \times \dots \times R/I_n$$

is an isomorphism via the projection map.

*Proof.* Omitted. ♡

**Theorem 4.3.5.** Let  $K$  be a number field and  $\mathcal{I}$  and  $\mathcal{J}$  are ideals of  $\mathcal{O}_K$ . Then

$$N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$$

*Proof.* We will do this in three steps:

1. Show the case when  $\mathcal{I}, \mathcal{J}$  are relatively prime.
2. Show  $N(\mathcal{P}^m) = N(\mathcal{P})^m$  where  $\mathcal{P}$  is a prime ideal.
3. Then Step 1 and Step 2 would imply  $N(\mathcal{P}_1^{m_1} \dots \mathcal{P}_r^{m_r}) = N(\mathcal{P}_1)^{m_1} \dots N(\mathcal{P}_r)^{m_r}$  and the result would follow from unique prime factorization of ideals.

Suppose  $\mathcal{I}$  and  $\mathcal{J}$  are relatively prime, then  $\mathcal{I} + \mathcal{J} = \mathcal{O}_K$  and  $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$ . Then by the Chinese Remainder Theorem we have

$$\mathcal{O}_K/\mathcal{I} \cap \mathcal{J} = \mathcal{O}_K/\mathcal{I}\mathcal{J} \cong \mathcal{O}_K/\mathcal{I} \times \mathcal{O}_K/\mathcal{J}$$

Hence we would have  $N(\mathcal{I}\mathcal{J}) = |\mathcal{O}_K/\mathcal{I}\mathcal{J}| = |\mathcal{O}_K/\mathcal{I}| \cdot |\mathcal{O}_K/\mathcal{J}| = N(\mathcal{I})N(\mathcal{J})$ . This finishes Step 1.

Now suppose  $\mathcal{P}$  is a prime and let  $m \geq 1$ , and consider the chain of ideals

$$\mathcal{O}_K \supseteq \mathcal{P} \supseteq \mathcal{P}^2 \supseteq \dots \supseteq \mathcal{P}^m$$

Now, by third isomorphism theorem, we would have  $\mathcal{O}/\mathcal{P}^m \cong (\mathcal{O}_K/\mathcal{P}^{m-1})/(\mathcal{P}^{m-1}/\mathcal{P}^m)$  and so if we can show  $N(\mathcal{P}) = |\mathcal{P}^{k-1}/\mathcal{P}^k|$  for all possible value of  $k$ , we would have  $N(\mathcal{P}^m) = |\mathcal{O}_K/\mathcal{P}^m| = |\mathcal{O}_K/\mathcal{P}^{m-1}| \cdot N(\mathcal{P})$  and then induction would follow as  $N(\mathcal{P}^m) = |\mathcal{O}_K/\mathcal{P}^{m-2}| \cdot N(\mathcal{P})^2$  and so on and finally obtain  $N(\mathcal{P}^m) = N(\mathcal{P})^m$ .

Now, we claim there is an isomorphism of groups from  $\mathcal{O}_K/\mathcal{P}$  to  $\mathcal{P}^k/\mathcal{P}^{k+1}$  and this would imply  $N(\mathcal{P}) = |\mathcal{P}^{k-1}/\mathcal{P}^k|$  and proof follows.

Note  $\mathcal{P}^k \supsetneq \mathcal{P}^{k+1}$  by the unique factorization, we can find  $\alpha \in \mathcal{P}^k \setminus \mathcal{P}^{k+1}$ . Then we have  $\mathcal{P}^{k+1} \subseteq \langle \alpha, \mathcal{P}^{k+1} \rangle \subseteq \mathcal{P}^k$ . By Proposition 3.3.2 and unique factorization, we must have  $\langle \alpha, \mathcal{P}^{k+1} \rangle = \mathcal{P}^k$ . Indeed, note by Proposition 3.3.2 we have  $\mathcal{P}^k \mid \langle \alpha, \mathcal{P}^{k+1} \rangle$  and  $\langle \alpha, \mathcal{P}^{k+1} \rangle \mid \mathcal{P}^{k+1}$ . Hence  $A\mathcal{P}^k = \langle \alpha, \mathcal{P}^{k+1} \rangle$  and  $B\langle \alpha, \mathcal{P}^{k+1} \rangle = \mathcal{P}^{k+1}$  for some ideals  $A, B$ . Now  $\mathcal{P}^{k+1} = AB\langle \alpha, \mathcal{P}^{k+1} \rangle$  and by unique factorization we would have  $AB = \mathcal{P}$ . Therefore, by Proposition 3.3.2 we have  $A \mid \mathcal{P}$  and  $B \mid \mathcal{P}$ , i.e.  $\mathcal{P} \subseteq A$  and  $\mathcal{P} \subseteq B$  and so by maximality of  $\mathcal{P}$  (recall we are in Dedekind domain) we have  $A, B$  are either  $\mathcal{P}$  or  $\mathcal{O}_K$ . Thus we have either  $A\mathcal{P}^k = \mathcal{O}_K\mathcal{P}^k = \langle \alpha, \mathcal{P}^{k+1} \rangle$ , which is what we desired, or  $A = \mathcal{P}$  and so  $\mathcal{P}^{k+1} = \langle \alpha, \mathcal{P}^{k+1} \rangle$ . However the latter case would imply  $\alpha \in \mathcal{P}^{k+1}$ , a contradiction. Thus  $\langle \alpha, \mathcal{P}^{k+1} \rangle = \mathcal{P}^k$ .

Next, we consider the prime decomposition of the principal ideal  $\langle \alpha \rangle$  and we get

$$\langle \alpha \rangle = \mathcal{Q}_1^{n_1} \dots \mathcal{Q}_l^{n_l} \mathcal{P}^n$$

for some  $n_1, \dots, n_l \geq 1$  and  $n \geq 0$ . Since  $\alpha \in \mathcal{P}^k$ , we have  $\langle \alpha \rangle \subseteq \mathcal{P}^k$  and so by Proposition 3.3.2 and unique factorization we have  $n \geq k$ . On the other hand we have  $n < k + 1$  because  $\alpha \notin \mathcal{P}^{k+1}$  and so

$$\langle \alpha \rangle = \prod \mathcal{Q}_i^{n_i} \cdot \mathcal{P}^k$$

Define a map  $\phi$  from  $\mathcal{O}_K$  to  $\mathcal{P}^k/\mathcal{P}^{k+1}$  by

$$\phi(\gamma) = \gamma\alpha + \mathcal{P}^{k+1}$$

for all  $\gamma \in \mathcal{O}_K$ . Then it is clearly a homomorphism and surjective as  $\langle \alpha, \mathcal{P}^{k+1} \rangle = \mathcal{P}^k$ . Thus, suppose  $\gamma \in \text{Ker}(\phi)$ , we have  $\gamma\alpha \in \mathcal{P}^{k+1}$  by definition. Observe

$$\alpha\mathcal{O}_K \cap \mathcal{P}^{k+1} = \text{lcm}(\langle \alpha \rangle, \mathcal{P}^{k+1}) = \text{lcm}(\mathcal{Q}_1^{m_1} \dots \mathcal{Q}_l^{m_l} \mathcal{P}^k, \mathcal{P}^{k+1}) = \prod \mathcal{Q}_i^{m_i} \cdot \mathcal{P}^{k+1} = \alpha\mathcal{P}$$

This imply  $\text{Ker}(\phi) = \mathcal{P}$  and so we have an isomorphism from  $\mathcal{O}_K/\text{Ker}(\phi) = \mathcal{O}_K/\mathcal{P}$  to  $\mathcal{P}^k/\mathcal{P}^{k+1}$  and the proof of the theorem follows.

♡

**Corollary 4.3.5.1.** *If  $N(\mathcal{I})$  is a prime number, then  $\mathcal{I}$  is a prime ideal.*

*Proof.* Say  $\mathcal{I} = AB$  where  $A, B$  are two ideals. Then we have  $N(\mathcal{I}) = N(A) \cdot N(B)$  and so  $N(A) = 1$  or  $N(B) = 1$  as  $N(\mathcal{I})$  is a prime number. WLOG, say  $N(A) = 1$ .

Then we have  $|\mathcal{O}_K/A| = 1$  and so  $A = \mathcal{O}_K$ , hence  $B$  must equal  $\mathcal{I}$  and so in particular  $B \subseteq \mathcal{I}$ . Therefore the proof follows.

♡

**Remark 4.3.6.** If  $\mathcal{P}$  is a prime ideal lies over  $p$  and the degree of  $K$  is  $n$ , then  $N(\mathcal{P}) \mid p^n$  and hence  $N(\mathcal{P}) = p^f$  with  $1 \leq f \leq n$ .

**Theorem 4.3.7.** Let  $K$  be a number field of degree  $n$  and  $p$  a prime number in  $\mathbb{Z}$ . Suppose  $\mathcal{P}_1, \dots, \mathcal{P}_r$  are all the primes lying over  $p$  and  $f_i = f(\mathcal{P}_i|p)$  be the inertial degree and  $e_i = e(\mathcal{P}_i|p)$  be the ramification index. Viz, we have

$$p\mathcal{O}_K = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}$$

Then, we have

$$n = \sum_{i=1}^r e_i f_i$$

*Proof.* Note  $N(\langle p \rangle) = |N_{\mathbb{Q}}^K(p)| = p^n$  by Theorem 4.2.3. On the other hand, we have

$$N(\langle p \rangle) = N\left(\prod_{i=1}^r \mathcal{P}_i^{e_i}\right) = \prod_{i=1}^r N(\mathcal{P}_i)^{e_i}$$

In particular, we observe  $f_i = [\mathcal{O}_K/\mathcal{P}_i : \mathbb{F}_p]$  and so  $N(\mathcal{P}_i) = p^{f_i}$ . Therefore, we get

$$N(\langle p \rangle) = p^{\sum_{i=1}^r e_i f_i} = p^n \Rightarrow n = \sum_{i=1}^r e_i f_i$$

♡

**Example 4.3.8.** Let  $K = \mathbb{Q}(\sqrt{-5})$  and  $p = 2$ . Then  $\langle 2 \rangle = \langle 2, 1 + \sqrt{-5} \rangle^2$  and so  $n = 2 = ef = 2f$  and hence  $f = 1$ . This tell us  $\mathbb{Z}[\sqrt{-5}]/\langle 2, 1 + \sqrt{-5} \rangle \cong \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ .

**Example 4.3.9.** Let  $K = \mathbb{Q}(\sqrt{d})$  where  $d$  is squarefree, note the degree of extension in this case is always 2. Let  $p$  be a prime in  $\mathbb{Z}$ . By Theorem 4.3.7, there are only three possibilities of the principal ideal  $\langle \alpha \rangle$  in  $\mathcal{O}_K$ . Namely

$$\langle p \rangle = \begin{cases} \mathcal{P}^2, & e(\mathcal{P}|p) = 2, f(\mathcal{P}|p) = 1 \\ \mathcal{P}, & e(\mathcal{P}|p) = 1, f(\mathcal{P}|p) = 2 \\ \mathcal{P}_1 \mathcal{P}_2, & e(\mathcal{P}_i|p) = f(\mathcal{P}_i|p) = 1 \end{cases}$$

By a finer argument, we obtain the following theorem.

**Theorem 4.3.10.** Let  $d$  be a squarefree integer and  $K = \mathbb{Q}(\sqrt{d})$ . Let  $p$  be a prime number in  $\mathbb{Z}$ . Then

1. If  $p \mid d$ , then  $\langle p \rangle = \langle p, \sqrt{d} \rangle^2$ .
2. If  $p = 2$ , and  $2 \nmid d$ , then

$$\langle 2 \rangle = \begin{cases} \langle 2, 1 + \sqrt{d} \rangle^2, & \text{if } d \equiv 3 \pmod{4} \\ \langle 2, \frac{1+\sqrt{d}}{2} \rangle \langle 2, \frac{1-\sqrt{d}}{2} \rangle, & \text{if } d \equiv 1 \pmod{8} \\ \text{prime ideal}, & \text{if } d \equiv 5 \pmod{8} \end{cases}$$

3. If  $p$  is odd, and  $p \nmid d$ , then

$$\langle p \rangle = \begin{cases} \langle p, n + \sqrt{d} \rangle \langle p, n - \sqrt{d} \rangle, & \text{if } \exists n \text{ so } d \equiv n^2 \pmod{p} \\ \text{prime ideal}, & \text{if } \forall n \in \mathbb{Z}, d \not\equiv n^2 \pmod{p} \end{cases}$$

*Proof.* First, assume  $p \mid d$ , i.e.  $d = bp$  for some  $b \in \mathbb{Z}$ . We first show  $\langle p, \sqrt{d} \rangle$  is prime and then show  $\langle p \rangle = \langle p, \sqrt{d} \rangle^2$ . Suppose  $d \not\equiv 1 \pmod{4}$  first. Observe  $\mathcal{O}_K / \langle p, \sqrt{d} \rangle = \mathbb{Z}[\sqrt{d}] / \langle p, \sqrt{d} \rangle \cong \mathbb{Z} / \langle p \rangle \cong \mathbb{F}_p$ , which is an integral domain, hence  $\langle p, \sqrt{d} \rangle$  is prime as desired. Then suppose  $d \equiv 1 \pmod{4}$  and in this case we have  $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ . In particular, note in this case we have  $\sqrt{d} = 2\alpha - 1$  where  $\alpha = \frac{1+\sqrt{d}}{2}$ . Hence we have (note  $x^2 - x + \frac{1-d}{4} = (2x-1)(\frac{1}{2}x - \frac{1}{4}) - \frac{d}{4}$ )

$$\begin{aligned} \mathcal{O}_K / \langle p, \sqrt{d} \rangle &= \mathbb{Z}[\alpha] / \langle p, 2\alpha - 1 \rangle \\ &\cong \mathbb{Z}[x] / \langle p, 2x - 1, x^2 - x + \frac{1-d}{4} \rangle \\ &\cong \mathbb{F}_p[x] / \langle 2x - 1, x^2 - x + \frac{1-d}{4} \rangle \\ &\cong \mathbb{F}_p[\frac{1}{2}] / \langle -\frac{d}{4} \rangle \\ &\cong \mathbb{F}_p[\frac{1}{2}] \end{aligned}$$

We get  $\frac{1}{2}$  in the middle is because  $\mathbb{F}_p[x] / \langle ax - b \rangle \cong \mathbb{F}_p[\frac{b}{a}]$  with the identification  $f(x) \mapsto f(\frac{b}{a})$ . In particular it is not hard to see  $\mathbb{F}_p[\frac{1}{2}]$  is indeed integral domain as

$$\mathbb{F}_p[\frac{1}{2}] = \{ \sum_{i=0}^m a_i (\frac{1}{2})^i : m \in \mathbb{N}, \quad \forall i, a_i \in \mathbb{Z}_p, \quad 1 \leq i \leq m \Rightarrow 2 \nmid a_i \}$$

Note we can assume the non-divisibility by 2 because if  $2 \mid a_i$  then we can always cancel the 2 in that term. In particular if  $(\sum_{i=0}^n a_i (1/2)^i)(\sum_{j=0}^m b_j (1/2)^j) = 0$  then

$$f(x) = (\sum_{i=0}^n a_i x^i)(\sum_{j=0}^m b_j x^j) = a_n b_m x^{n+m} + \dots$$

has a root  $1/2$ . Thus by rational root test we must have  $2 \mid a_n b_m$  imply  $2 \mid a_n$  or  $2 \mid b_m$ , which is a contradiction by our assumption. This shows that ring is integral domain and so  $\langle p, \sqrt{d} \rangle$  is prime ideal.

Next, note  $\langle p, \sqrt{d} \rangle^2 = \langle p^2, p\sqrt{d}, d \rangle = \langle p^2, p\sqrt{d}, bp \rangle = \langle p \rangle \langle p, \sqrt{d}, b \rangle$ . On the other hand, note  $d$  is squarefree and  $d = bp$  so we must have  $\gcd(b, p) = 1$ . Thus  $\mathcal{O}_K = \langle 1 \rangle = \langle p, b \rangle \subseteq \langle p, \sqrt{d}, b \rangle$ , i.e.  $\langle p, \sqrt{d} \rangle^2 = \langle p \rangle \cdot \mathcal{O}_K = \langle p \rangle$ . This finishes our first claim.

Now suppose  $p = 2$  and  $2 \nmid d$ . Let  $P$  be a prime ideal that divides  $\langle 2 \rangle$ . Then  $\langle 2 \rangle \subseteq P$  and so  $2 \in P$  by Proposition 3.3.2. Then by Theorem 3.3.7 we have  $P = \langle 2, \alpha \rangle$ . Now  $\mathcal{O}_K / P$  is an integral domain. Now, recall by Corollary 2.1.4.2, we have either  $\mathcal{O}_K = \{r + s\sqrt{d} : r, s \in \mathbb{Z}\}$  or  $\mathcal{O}_K = \{\frac{a+b\sqrt{d}}{2} : a \equiv b \pmod{2}\}$ . In particular, since  $2 \nmid d$ , we have  $d \equiv 3 \pmod{4}$  then  $\mathcal{O}_K = \{r + s\sqrt{d} : r, s \in \mathbb{Z}\}$  and otherwise  $\mathcal{O}_K = \{\frac{a+b\sqrt{d}}{2} : a \equiv b \pmod{2}\}$ .

First, let  $d \equiv 3 \pmod{4}$ , then the representatives in  $\mathcal{O}_K / \langle 2 \rangle$  are  $\{0, 1, \sqrt{d}, 1 + \sqrt{d}\}$ . Then we must have  $\alpha + \langle 2 \rangle \in \{\langle 2 \rangle, 1 + \langle 2 \rangle, \sqrt{d} + \langle 2 \rangle, (1 + \sqrt{d}) + \langle 2 \rangle\}$ . However,  $\alpha$  cannot be 1 as that imply  $P = \mathcal{O}_K$ . Also  $\alpha$  cannot be 0 because that will imply



$P = \langle 2, 0 \rangle = \langle 2 \rangle$  is a prime, but  $(1 + \sqrt{d})(1 - \sqrt{d}) \in \langle 2 \rangle$  while both of them are not in  $\langle 2 \rangle$ , i.e. it is not a prime. Next, observe  $(\sqrt{d} + \langle 2 \rangle)^2 = d + \langle 2 \rangle = 1 + \langle 2 \rangle$  as  $2 \nmid d$ , i.e.  $P = \mathcal{O}_K$ , a contradiction. Hence, the only possibilities for a prime ideal to divide 2 is  $P = \langle 2, 1 + \sqrt{d} \rangle$ . Thus, by Theorem 4.3.7, we must have  $\langle 2 \rangle = P^2$  where  $P = \langle 2, 1 + \sqrt{d} \rangle$ . This finishes the first part of second claim.

Now suppose  $d \equiv 1 \pmod{4}$  and then  $\mathcal{O}_K = \{\frac{a+b\sqrt{d}}{2} : a \equiv b \pmod{2}\}$ . Then, we have the set of representatives to be<sup>1</sup>  $\{0, 1, \sqrt{d}, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}\}$ . In particular, suppose  $d \equiv 5 \pmod{8}$ , then  $\mathcal{O}_K/\langle 2 \rangle$  contains those representatives and it is a computational matter to check those elements actually form an integral domain module 2, i.e.  $\langle 2 \rangle$  is a prime when  $d \equiv 5 \pmod{8}$ . This is the second part of our second claim done.

Therefore, the only case left is  $d \equiv 1 \pmod{8}$ . In this case, a similar argument could show that  $\alpha$  is either  $(1 + \sqrt{d})/2$  or  $(1 - \sqrt{d})/2$  and so we only have two possible prime ideals that divides  $\langle 2 \rangle$ . Namely,  $\langle 2, (1 + \sqrt{d})/2 \rangle$  or  $\langle 2, (1 - \sqrt{d})/2 \rangle$ . However, note  $\langle 2 \rangle \subseteq \langle 2, \frac{1+\sqrt{d}}{2} \rangle$  and  $\langle 2 \rangle \subseteq \langle 2, \frac{1-\sqrt{d}}{2} \rangle$  at the same time, so both of the two primes divide  $\langle 2 \rangle$ , i.e. we must have

$$\langle 2 \rangle = \langle 2, \frac{1 + \sqrt{d}}{2} \rangle \langle 2, \frac{1 - \sqrt{d}}{2} \rangle$$

This finishes the last part of our second claim.

Now suppose  $p$  is odd and  $p \nmid d$ . In particular, if  $d \equiv n^2 \pmod{p}$  for some  $n \in \mathbb{Z}$ , then we have  $d = kp + n^2$ . In this case, we first show  $\langle p, n + \sqrt{d} \rangle$  is prime (note  $\langle p, n - \sqrt{d} \rangle$  is similar). If  $d \not\equiv 1 \pmod{4}$  then  $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ . In this case, let  $f(x) = x^2 - d$  be the minimal polynomial of  $\sqrt{d}$  we have (note  $x^2 - d \equiv (x+n)(x-n) \pmod{p}$  as  $d \equiv n^2 \pmod{p}$ )

$$\mathbb{Z}[\sqrt{d}]/\langle p, n + \sqrt{d} \rangle \cong \mathbb{F}_p[x]/\langle x + n, x^2 - d \rangle = \mathbb{F}_p[x]/\langle x + n \rangle \langle x - n \rangle \cong \mathbb{F}_p \times \mathbb{F}_p$$

where the last step is by Chinese remainder theorem. This establishes the primeness. Thus, we have  $\langle p, n + \sqrt{d} \rangle \langle p, n - \sqrt{d} \rangle = \langle p^2, p(n + \sqrt{d}), p(n - \sqrt{d}), -kp \rangle = \langle p \rangle \langle p, n + \sqrt{d}, n - \sqrt{d}, k \rangle = \langle p \rangle$  as  $\langle p, n + \sqrt{d}, n - \sqrt{d}, k \rangle = \mathcal{O}_K$  as  $2n \in \langle p, n + \sqrt{d}, n - \sqrt{d}, k \rangle$  where we must have  $\gcd(p, 2n) = \gcd(p, n) = 1$  for otherwise  $d \equiv 0 \pmod{p} \Rightarrow p \mid d$ , which is a contradiction.

Thus the only thing left to check is when  $d \not\equiv n^2 \pmod{p}$  for all  $n \in \mathbb{Z}$ , we have  $\langle p \rangle$  is a prime ideal. In this case, let  $f(x)$  be the minimal polynomial of  $\alpha$  where  $\mathbb{Z}[\alpha] = \mathcal{O}_K$ . We then have  $\mathbb{Z}[\alpha]/\langle p \rangle \cong \mathbb{Z}[x]/\langle f(x), p \rangle \cong \mathbb{F}_p[x]/\langle f(x) \rangle$ . If  $f(x)$  is irreducible in  $\mathbb{F}_p[x]$  then clearly  $\mathbb{Z}[\alpha]/\langle p \rangle \cong \mathbb{F}_p[x]/\langle f \rangle$  is field and so  $\langle p \rangle$  is prime. Conversely, if  $\langle p \rangle$  is prime, then  $f(x)$  must be irreducible mod  $p$ . Therefore, suppose  $p$  is not a prime ideal, we must have  $f(x)$  is reducible mod  $p$ , i.e.  $f(x) = (x-a)(x-b)$

---

<sup>1</sup>Indeed, note  $\langle 2 \rangle = 2\mathcal{O}_K = \{a + b\sqrt{d} : a \equiv b \pmod{2}\}$ . Thus, take any element in  $\mathcal{O}_K$ , say  $(r + s\sqrt{d})/2$ . If  $r \equiv s \equiv 0 \pmod{2}$ , then  $(r + s\sqrt{d})/2 = c + d\sqrt{d}$ . Now if  $c$  is odd and  $d$  is even then we can categorize this element either in the equivalence class of 1 or 0. If  $c$  is even and  $d$  is odd then it is in the class  $\sqrt{d}$  or 0. If both are still even then it is in 0. Then, if  $r \equiv s \equiv 1 \pmod{2}$ , the only two possibilities are  $(1 \pm \sqrt{d})/2$ .

$(\text{mod } p)$ . However, if  $a \not\equiv b \pmod{p}$  then we get

$$\begin{aligned}\mathbb{F}_p[x]/\langle f(x) \rangle &\cong \mathbb{Z}_p[x]/\langle x-a \rangle \langle x-b \rangle \\ &\cong \mathbb{Z}_p[x]/\langle x-a \rangle \times \mathbb{Z}_p[x]/\langle x-b \rangle \\ &\cong \mathbb{F}_p \times \mathbb{F}_p\end{aligned}$$

This is an integral domain and so contradict the fact  $p$  is not prime. Therefore  $a \equiv b \pmod{p}$ . Hence we get  $f(x) \equiv (x-a)^2 \equiv x^2 - 2ax + a^2 \equiv x^2 - d \pmod{p}$  or  $f(x) \equiv x^2 - 2ax + a^2 \equiv x^2 - x + \frac{1-d}{4} \pmod{p}$ . In the first case, we are forced to have  $-2ax \equiv 0$  and  $a^2 \equiv d \pmod{p}$  as desired. In the second case, we are forced to have  $-2ax \equiv -x \pmod{p} \Rightarrow 2a \equiv 1 \pmod{p}$  and  $1-d \equiv 4a^2 \pmod{p}$ . Thus we get  $d \equiv 0 \pmod{p}$ , which is a contradiction. In all cases, we have  $p$  is not prime imply  $n^2 \equiv d \pmod{p}$  and hence we are done.

♡

## Chapter 5

# Ideal Class Group

一片春愁待酒浇。江上舟摇，楼上帘招。秋娘渡与泰娘桥，风又飘飘，雨又萧萧。  
何日归家洗客袍？银字笙调，心字香烧。流光容易把人抛，红了樱桃，绿了芭蕉。

蒋捷

## 5.1 Finiteness of Ideal Class Group

**Remark 5.1.1.** Recall the ideal class group,  $\mathcal{C}_R$ , is defined by  $\mathfrak{I}/\sim$  where  $\mathfrak{I}$  is the set of ideals of a Dedekind domain  $R$  and  $\sim$  is defined by  $A \sim B$  if and only if  $\alpha A = \beta B$  for some elements  $\alpha, \beta \in R$ . If you need a full review on this, consider Section 3.2.

**Remark 5.1.2.**

1. The multiplication of  $\mathcal{C}_R$  is defined by  $[A] \cdot [B] = [AB]$  where  $[A]$ ,  $[B]$  and  $[AB]$  are equivalence classes.
2. The identity element of  $\mathcal{C}_R$  is the class of principal ideals, the proof to show it forms a single equivalence class is Proposition 3.2.3.
3. The existence of inverse is Theorem 3.2.9 and Corollary 3.2.9.1.

**Theorem 5.1.3.** *Let  $K$  be a number field. There exists a constant  $c_0$ , depending on  $K$ , such that every non-zero ideal  $\mathcal{I}$  of  $\mathcal{O}_K$  contain a non-zero element  $\alpha$  such that*

$$|N_{\mathbb{Q}}^K(\alpha)| \leq c_0 N(\mathcal{I})$$

*Proof.* Let  $(\alpha_1, \dots, \alpha_n)$  be an integral basis of  $K$  and  $\sigma_1, \dots, \sigma_n$  be all the embeddings of  $K$  in  $\mathbb{C}$  fix  $\mathbb{Q}$  where  $n$  is the degree of  $K$ . We will show the following value works:

$$c_0 = \prod_{j=1}^n \left( \sum_{i=1}^n |\sigma_i(\alpha_j)| \right)$$

For any ideal  $\mathcal{I}$ , let  $m$  be the unique positive integer satisfying

$$m^n \leq N(\mathcal{I}) < (m+1)^n$$

and consider the  $(m+1)^n$  members of  $\mathcal{O}_K$  of the form

$$0 \leq m_j \leq m, m_j \in \mathbb{Z}, \sum_{j=1}^n m_j \alpha_j$$

Two of these must congruent modulo  $\mathcal{I}$  since there are more than  $N(\mathcal{I})$  of them. Taking the difference, we obtain a non-zero member of  $\mathcal{I}$  having the form

$$\alpha = \sum_{j=1}^n a_j \alpha_j, a_j \in \mathbb{Z}, |a_j| \leq m$$

Finally, we have

$$|N_{\mathbb{Q}}^K(\alpha)| = \prod_{i=1}^n |\sigma_i(\alpha)| \leq \prod_{i=1}^n \left( \sum_{j=1}^n |a_j| |\sigma_i(\alpha_j)| \right) \leq m^n c_0 \leq c_0 N(\mathcal{I})$$

♡

**Lemma 5.1.4.** *Given a value  $m \in \mathbb{Z}_{\geq 1}$ , there are only finitely many ideals  $\mathcal{I}$  such that  $N(\mathcal{I}) = m$ .*

*Proof.* First, observe by Proposition 4.2.4, we know  $N(\mathcal{I}) \in \mathcal{I}$  for any ideal  $\mathcal{I}$ . Therefore, consider  $\langle m \rangle = m\mathcal{O}_K$  and its prime factorization, for any ideal  $\mathcal{I}$ , we have  $N(\mathcal{I}) = m$  imply  $m \in \mathcal{I}$  imply  $\langle m \rangle \subseteq \mathcal{I}$  and now by Proposition 3.3.2, this happens if and only if  $\mathcal{I} \mid \langle m \rangle$ . The proof of the result follows as now if  $N(\mathcal{I}) = m$  then we must have  $\mathcal{I}$  of the form  $\prod_{i=1}^k P_i^{k_i}$  with  $0 \leq k_i \leq e(P_i | \langle m \rangle)$  and  $P_i$  are all the prime factors of  $\langle m \rangle$  and there are only finitely many possibilities for this expression, i.e. finitely many possible ideal for  $N(\mathcal{I}) = m$ . ♡

**Theorem 5.1.5.** *Let  $K$  be a number field, then the ideal class group  $\mathcal{C}_K$  of  $\mathcal{O}_K$  is finite.*

*Proof.* We will show that every ideal class of  $\mathcal{O}_K$  contains an ideal of  $\mathcal{O}_K$  of the norm at most  $c_0$  where  $c_0$  is from last Theorem 5.1.3. Then the result follows by Lemma 5.1.4 as we can just enumerate over all possible value  $m$  with  $1 \leq m \leq c_0$  and for each  $m$  there are only finitely many ideals.

Let  $\mathcal{I}$  be an ideal of  $\mathcal{O}_K$ , there is an ideal  $\mathcal{A}$  of  $\mathcal{O}_K$  such that  $[\mathcal{I}\mathcal{A}] = [1]$ . By Theorem 5.1.3, there is an element  $0 \neq \alpha \in \mathcal{A}$  such that  $|N_{\mathbb{Q}}^K(\alpha)| \leq c_0 N(\mathcal{A})$  where  $N_{\mathbb{Q}}^K(\alpha) = N(\langle \alpha \rangle)$ .

Since  $\alpha \in \mathcal{A}$  we have  $\langle \alpha \rangle \subseteq \mathcal{A}$  and so  $\mathcal{A} \mid \langle \alpha \rangle$  by Proposition 3.3.2, i.e. there exists ideal  $\mathcal{B}$  so  $\mathcal{B}\mathcal{A} = \langle \alpha \rangle$ . In particular since  $\alpha \neq 0$  we have  $[\mathcal{B}\mathcal{A}] = [1]$ . Thus we have

$$[\mathcal{I}][\mathcal{A}] = [\mathcal{B}][\mathcal{A}] = 1 \Rightarrow [\mathcal{I}] = [\mathcal{B}]$$

Viz,  $\mathcal{I}$  and  $\mathcal{B}$  are in the same equivalence class. Next, observe

$$N(\mathcal{B})N(\mathcal{A}) = N(\mathcal{B}\mathcal{A}) = N(\langle \alpha \rangle) \leq c_0 N(\mathcal{A}) \Rightarrow N(\mathcal{B}) \leq c_0$$

this finishes the claim and so the proof follows.  $\heartsuit$

**Definition 5.1.6.** Let  $K$  be a number field, the number of ideal classes, denoted by  $h_K$ , is a finite number called **class number** of  $K$ . In other word,  $h_K = |\mathcal{C}_K|$ .

**Remark 5.1.7.** Hilbert conjectured and Furtivangler proved the following: let  $K$  be a number field, then there exists an extension  $H$  of  $K$  such that

1.  $[H : K] = h_K$ .
2.  $H$  is normal over  $K$ .
3. The ideal class group of  $K$  is isomorphic to the Galois group of  $H$  over  $K$ .
4. Every ideal of  $\mathcal{O}_K$  becomes a principal ideal of  $\mathcal{O}_H$ .
5. Every prime ideal  $\mathcal{P}$  of  $\mathcal{O}_K$  decomposes into the products of  $h_K/f$  many prime ideals in  $\mathcal{O}_H$  where  $f = |[P]|$  is the order of  $[P]$  in the ideal class group of  $\mathcal{O}_K$ .

This  $H$  is unique and it is called **Hilbert class field** of  $K$ .

**Example 5.1.8.** Let  $K = \mathbb{Q}(\sqrt{2})$  and  $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ . Taking the integral basis  $\{1, \sqrt{2}\}$ , we have

$$c_0 = \prod_{j=1}^2 \left( \sum_{i=1}^2 |\sigma_i(\alpha_j)| \right) = (|1| + |\sqrt{2}|)(|1| + |-\sqrt{2}|) = (1 + \sqrt{2})^2 \approx 5.828$$

as  $c_0$  defined in Theorem 5.1.3. Therefore, any ideal class contains an ideal  $\mathcal{J}$  with  $N(\mathcal{J}) \leq 5$ . The possible prime divisors of  $\mathcal{J}$  are necessarily among primes lying over 2, 3 or 5. So let us factor  $\langle 2 \rangle$ ,  $\langle 3 \rangle$  and  $\langle 5 \rangle$ .

By Theorem 4.3.10, we have

$$\langle 2 \rangle = \langle \sqrt{2} \rangle^2, \langle 3 \rangle = \langle 3 \rangle, \langle 5 \rangle = \langle 5 \rangle$$

are the prime factorizations. This shows that the only ideals  $\mathcal{J}$  with  $N(\mathcal{J}) \leq 5$  are  $\langle 1 \rangle$ ,  $\langle \sqrt{2} \rangle$ ,  $\langle 2 \rangle$  and so  $h_K = 1$  and all ideals in  $\mathcal{O}_K$  are principal.

**Example 5.1.9.** Let  $K = \mathbb{Q}(\sqrt{-5})$  and  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ . Taking integral basis  $\{1, \sqrt{-5}\}$ , we have

$$c_0 = (1 + |\sqrt{-5}|)(1 + |-\sqrt{-5}|) = (1 + \sqrt{5})^2 \approx 10.472$$

Therefore, any ideal class contains an ideal  $\mathcal{J}$  with  $N(\mathcal{J}) \leq 10$ . The possible prime divisors of  $\mathcal{J}$  are necessarily among primes lying over 2, 3, 5 and 7. By Theorem 4.3.10 again, we have the prime factorization to be

$$\begin{cases} \langle 2 \rangle &= \langle 2, 1 + \sqrt{-5} \rangle^2 = \mathcal{P}^2 \\ \langle 3 \rangle &= \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle = \mathcal{Q}_1 \mathcal{Q}_2 \\ \langle 5 \rangle &= \langle \sqrt{-5} \rangle^2 \\ \langle 7 \rangle &= \langle 7, 3 + \sqrt{-5} \rangle \langle 7, 3 - \sqrt{-5} \rangle = \mathcal{R}_1 \mathcal{R}_2 \end{cases}$$

It is easy to see that  $\mathcal{P}$  is principal. Indeed, say  $\mathcal{P} = \langle \alpha \rangle$  for some  $\alpha$ , then  $|N_{\mathbb{Q}}^K(\alpha)| = N(\mathcal{P}) = 2$ , i.e. this is because  $N(\langle 2 \rangle) = |N_{\mathbb{Q}}^K(2)| = 4$  while we also have  $N(\langle 2 \rangle) = N(\mathcal{P})^2$ , i.e.  $N(\mathcal{P}) = 2$ . Therefore, we would have  $N_{\mathbb{Q}}^K(\alpha) = \pm 2$ . Suppose  $\alpha = a + b\sqrt{-5}$  where  $a, b$  are some coefficients. Then we have

$$N_{\mathbb{Q}}^K(\alpha) = \pm 2 \Leftrightarrow a^2 + 5b^2 = \pm 2$$

which contains no integer solutions. Similarly, the prime factors of 3 and 7 are non-principal.

Let us now study the relations between those primes. Consider  $\beta = 1 + \sqrt{-5}$ . Since  $N(\beta) = 6 = 2 \cdot 3$ , the principal ideal  $\langle \beta \rangle$  can be factorize into a product of two primes, say

$$\langle \beta \rangle = \mathcal{P} \mathcal{Q}_i$$

Then we have

$$[\mathcal{P}][\mathcal{Q}_i] = [1]$$

On the other hand,  $\langle 3 \rangle = \mathcal{Q}_1 \mathcal{Q}_2$  so  $[\mathcal{Q}_1][\mathcal{Q}_2] = [1]$ . Similarly since  $\mathcal{P}^2 = \langle 2 \rangle$  we have  $[\mathcal{P}][\mathcal{P}] = [1]$ . Then

$$[\mathcal{P}][\mathcal{Q}_i] = [\mathcal{Q}_1][\mathcal{Q}_2] = [\mathcal{P}][\mathcal{P}] = [1] \Rightarrow [\mathcal{P}] = [\mathcal{Q}_1] = [\mathcal{Q}_2]$$

Similarly, by consider  $\gamma = 3 + \sqrt{-5}$  whose norm is 14, we get  $[\mathcal{P}] = [\mathcal{R}_1] = [\mathcal{R}_2]$  and so all non-principal prime ideals are in the same ideal class, i.e. the class number is 2.

**Remark 5.1.10.** It can be shown that  $c_0$  can be taken to be  $\sqrt{|disc(K)|}$ .

## 5.2 The Lattices

**Definition 5.2.1.** A subset (or subgroup)  $\Lambda$  of  $\mathbb{R}^m$  is called a **lattice** in  $\mathbb{R}^m$  if there are  $n$   $\mathbb{R}$ -linearly independent vectors  $\alpha_1, \dots, \alpha_n \in \mathbb{R}^m$  where  $n \leq m$ , such that every element  $\gamma \in \Lambda$  can be uniquely represented in the form

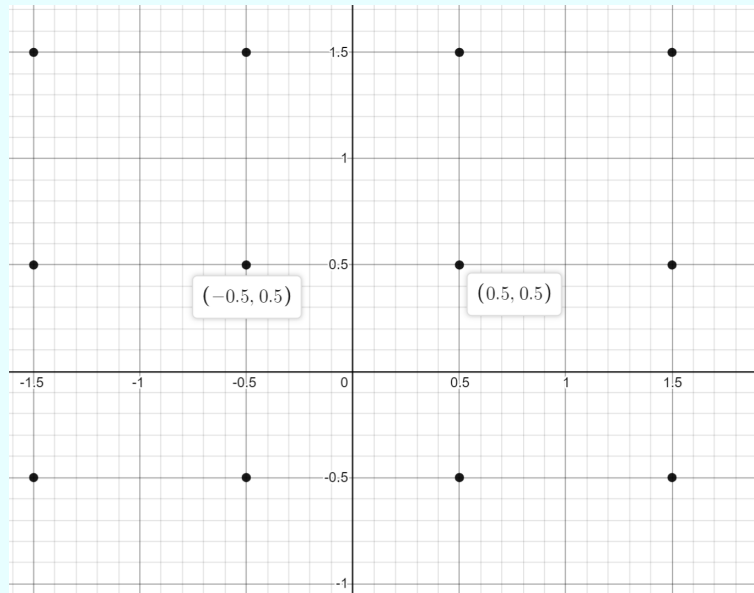
$$u_1 \alpha_1 + \dots + u_n \alpha_n$$

where for all  $i = 1, \dots, n$  we have  $u_i \in \mathbb{Z}$ . Then  $\alpha_1, \dots, \alpha_n$  are called a **basis** of  $\Lambda$  and  $n$  is the dimension of the lattice  $\Lambda$ .

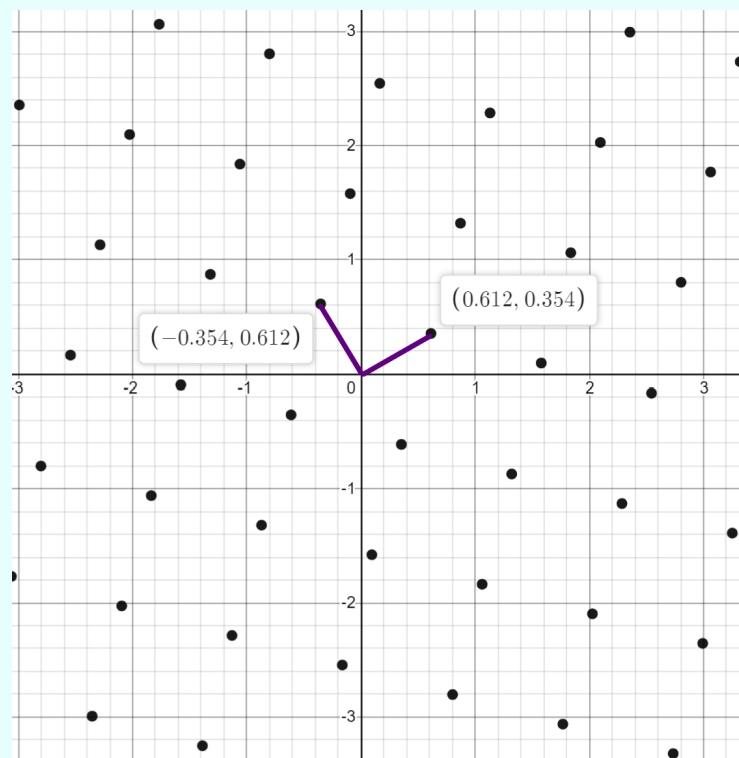
**Remark 5.2.2.** Note the basis  $\alpha_1, \dots, \alpha_n$  is not uniquely determined. In addition, in the case  $n = m$ , we call  $d(\Lambda)$ , the determinant of  $\Lambda$ , to be  $|\det(\alpha_1, \dots, \alpha_n)|$  where  $\{\alpha_i : 1 \leq i \leq n\}$  is a basis of  $\Lambda$ .

**Example 5.2.3.** Here we give some visualization of lattices in  $\mathbb{R}^2$ .

The first one is a lattice spanned by  $(\frac{1}{2}, \frac{1}{2})$  and  $(-\frac{1}{2}, \frac{1}{2})$  where black dots are the lattice elements:



The second one is a lattice spanned by the two elements  $(\frac{\sqrt{6}}{4}, \frac{\sqrt{2}}{4})$  and  $(\frac{-\sqrt{2}}{4}, \frac{\sqrt{6}}{4})$ :



**Example 5.2.4.** Consider the dimension  $n$  lattice

$$\Lambda_0 = \left\{ \sum_{i=1}^n u_i e_i : u_i \in \mathbb{Z} \right\} \subseteq \mathbb{R}^n$$

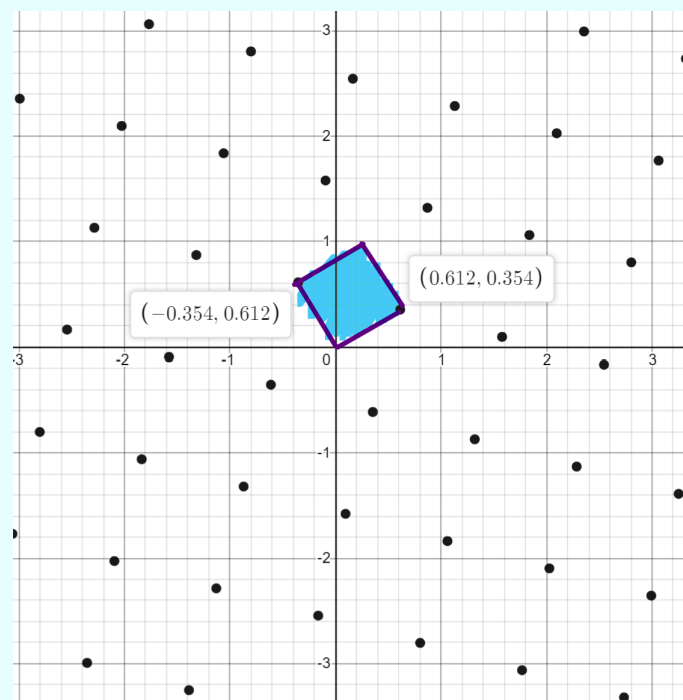
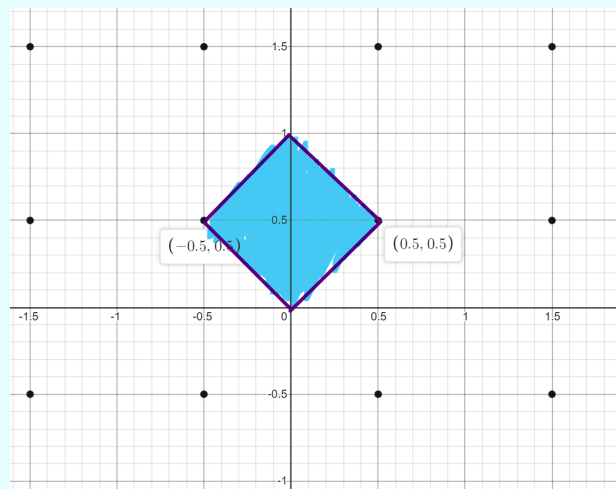
where  $e_1, \dots, e_n$  are standard basis. Then  $d(\Lambda_0) = 1$ .

**Definition 5.2.5.** Let  $\Lambda$  be a lattice in  $\mathbb{R}^m$ . A *fundamental parallelotope* for  $\Lambda$  is a subset of  $\mathbb{R}^m$  of the form

$$\{u_1 \alpha_1 + \dots + u_n \alpha_n : 0 \leq u_i < 1\}$$

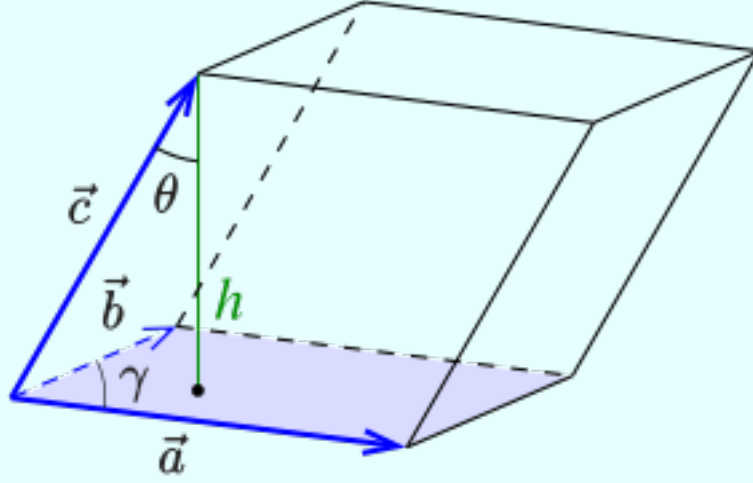
where  $\{\alpha_1, \dots, \alpha_n\}$  is any basis for  $\Lambda$ .

**Example 5.2.6.** In our previous Example 5.2.3, we have the following to be examples of fundamental parallelotopes (note change a basis will result the fundamental parallelotope to change):





Lastly, we give an illustration of what a fundamental parallelotope may look like in  $\mathbb{R}^3$ :



**Remark 5.2.7.** Note it is a well-known that the  $n$ -dimensional volume of such a parallelotope is the absolute value of the determinant by taking the rows  $\alpha_1, \dots, \alpha_n$ .

**Lemma 5.2.8.** Let  $\Gamma$  be an additive subgroup of  $\mathbb{R}^m$  with the property that any bounded subset of  $\mathbb{R}^m$  contains only finitely many element of  $\Gamma$ . Then  $\Gamma$  is a lattice of  $\mathbb{R}^m$ .

*Proof.* We use induction on  $m$ . If  $\Gamma = \{0\}$  then we are done. Thus, we assume  $\Gamma \neq \{0\}$ .

Now suppose  $m = 1$ , i.e.  $\Gamma \subseteq \mathbb{R}$ . Let  $\lambda$  be the smallest positive real number in  $\Gamma$ , i.e. this is because we assumed that any bounded subset of  $\mathbb{R}$  contains only finitely many elements of  $\Gamma$ . Now let  $\beta \in \Gamma$  be arbitrary, then either  $\beta$  or  $-\beta$  is positive, say  $\beta$ . We claim  $\beta/\lambda =: a$  is a positive integer. Consider

$$0 \leq \beta - [a]\lambda = (a - [a])\lambda < \lambda$$

and  $\beta - [a]\lambda \in \Gamma$ . Thus by minimality of  $\lambda$  we have  $(a - [a])\lambda = 0$  and so  $a = [a] \in \mathbb{Z}$  where here  $[a]$  means the floor of  $a$ . Therefore, all elements in  $\Gamma$  are the multiple of  $\lambda$  and the base case is done.

Now, suppose it holds for values less than  $m$ . We will establish the case for  $\mathbb{R}^m$ . Let  $\{v_1, \dots, v_k\}$  be a maximal linearly independence subset of  $\Gamma$ , i.e. we would have  $\Gamma \subseteq \mathbb{R}v_1 + \dots + \mathbb{R}v_k$ . Let  $V$  be the subspace of  $\mathbb{R}^m$  spanned by  $\{v_1, \dots, v_{k-1}\}$  and  $\Gamma_0 = V \cap \Gamma$ . Then by induction hypothesis we have  $\Gamma_0$  is a lattice of  $V$ , which is isomorphic to  $\mathbb{R}^{m-1}$ . Therefore, we have a linearly independence subset  $\{w_1, \dots, w_{k-1}\} \subseteq \Gamma$  such that  $\Gamma_0 = \mathbb{Z}w_1 + \dots + \mathbb{Z}w_{k-1}$ . Evidently,  $V$  is spanned by  $\{w_1, \dots, w_{k-1}, v_k\}$ .

Now let

$$T = \left\{ \sum_{i=1}^{k-1} a_i w_i + a_k v_k : \forall 1 \leq i \leq k-1, 0 \leq a_i < 1, \text{ and } 0 \leq a_k \leq 1 \right\}$$

and observe  $T$  is bounded hence finite. Therefore, we can choose an element  $w_k \in T$  with smallest non-zero coefficient  $a_k$  of  $v_k$ , say  $w_k = \sum_{i=1}^{k-1} b_i w_i + b_k v_k$ . Since  $b_k \neq 0$ , we have  $\{w_1, \dots, w_k\}$  is linearly independent. Moreover, for any  $\gamma \in \Gamma$ , without loss of generality, we may assume

$$\gamma = c_1 w_1 + \dots + c_{k-1} w_{k-1} + c_k w_k = d_1 w_1 + \dots + d_{k-1} w_{k-1} + d_k v_k$$

for some coefficients  $c_i$  and  $d_i$ . Consider

$$\begin{aligned} \gamma' &= \gamma - ([d_1]w_1 + \dots + [d_k]v_k) \\ &= ((d_1 - [d_1])w_1 + \dots + (d_{k-1} - [d_{k-1}])w_{k-1} + (d_k - [d_k])v_k) \in T \end{aligned}$$

Observe the coefficient  $d_k - [d_k]$  is smaller than  $b_k$  and so by minimality of  $b_k$  we have  $d_k = 0$  and then  $c_k = 0$ . Therefore,  $\gamma \in \Gamma_0$  and so  $c_1, \dots, c_{k-1} \in \mathbb{Z}$ , i.e.

$$\Gamma = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_k$$

and the proof follows. ♡

**Definition 5.2.9.** Let  $K$  be a number field. Let  $\sigma$  be an embedding of  $K$  in  $\mathbb{C}$ . If  $\sigma(K)$  contained in  $\mathbb{R}$ , we say  $\sigma$  is a **real embedding**. If it is not, we say  $\sigma$  is a **complex embedding**.

**Example 5.2.10.** Let  $K = \mathbb{Q}(\sqrt[3]{2})$ . Then  $K$  has one real embedding  $\sigma_1$  that sends  $\sqrt[3]{2}$  to  $\sqrt[3]{2}$ . We have two complex embeddings  $\sigma_i$  that sends  $\sqrt[3]{2}$  to  $\zeta_3^i \sqrt[3]{2}$  where  $i = 1, 2$ .

**Remark 5.2.11.** Let  $K$  be a number field, and  $\sigma$  be a complex embedding, then  $\bar{\sigma}$  is also a complex embedding which is different to  $\sigma$ . In particular,

$$\operatorname{Re}(\sigma) = \frac{\sigma + \bar{\sigma}}{2}, \operatorname{Im}(\sigma) = \frac{\sigma - \bar{\sigma}}{2i}$$

where  $\operatorname{Re}$  and  $\operatorname{Im}$  means the real and imaginary part respectively<sup>1</sup>. Also, note if  $K$  has  $r$  real embedding and  $2s$  complex embeddings, then

$$n = r + 2s$$

where  $n$  is the degree of  $K$ .

**Definition 5.2.12.** Let  $K$  be a number field with  $r$  real embeddings and  $2s$  complex embeddings. Then the **signature** of  $K$  is the two tuple  $(r, s)$ .

**Example 5.2.13.** Let  $K$  be a number field of degree  $n$ , say  $\sigma_1, \dots, \sigma_r$  the real embeddings of  $K$ , and  $\tau_1, \bar{\tau}_1, \dots, \tau_s, \bar{\tau}_s$  be the complex embeddings of  $K$ . We know  $n = r + 2s$ , define a map  $v$  from  $K$  to  $\mathbb{R}^n$  as follows

$$\forall \alpha \in K, v(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re}(\tau_1(\alpha)), \operatorname{Im}(\tau_1(\alpha)), \dots, \operatorname{Re}(\tau_s(\alpha)), \operatorname{Im}(\tau_s(\alpha)))$$

It is easy to see that  $v$  is an additive homomorphism with trivial kernel and hence an embedding.

---

<sup>1</sup>E.g., say  $\alpha = 2 + 4i$ , then  $\operatorname{Re}(\alpha) = 2$  and  $\operatorname{Im}(\alpha) = 4$

**Proposition 5.2.14.** Let  $K$  be a number field of degree  $n$  and  $v$  be the map defined by above remark. Let  $\Lambda_{\mathcal{O}_K} = \Lambda_K$  be the image of  $\mathcal{O}_K$  in  $\mathbb{R}^n$  by  $v$ . Then  $\Lambda_K$  is an  $n$ -dimensional lattice in  $\mathbb{R}^n$ , whose determinant is

$$d(\Lambda_K) = \frac{1}{2^s} \sqrt{|\text{disc}(K)|}$$

*Proof.* Let  $\omega_1, \dots, \omega_n$  be an integral basis of  $K$ . Therefore,  $v(\omega_1), \dots, v(\omega_n)$  generates  $\Lambda_K$  over  $\mathbb{Z}$ . We need to show that  $v(\omega_1), \dots, v(\omega_n)$  are linearly independent.

From the  $n \times n$  matrix  $M$  whose  $i$ th row consists of  $v(\omega_i)$ , i.e.

$$M = \begin{bmatrix} \sigma_1(\omega_1) & \dots & \sigma_r(\omega_1) & \text{Re}(\tau_1(\omega_1)) & \text{Im}(\tau_1(\omega_1)) & \dots & \text{Re}(\tau_s(\omega_1)) & \text{Im}(\tau_s(\omega_1)) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\omega_n) & \dots & \sigma_r(\omega_n) & \text{Re}(\tau_1(\omega_n)) & \text{Im}(\tau_1(\omega_n)) & \dots & \text{Re}(\tau_s(\omega_n)) & \text{Im}(\tau_s(\omega_n)) \end{bmatrix}$$

where  $\sigma_1, \dots, \sigma_r$  are the real embeddings and  $\tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$  are complex embeddings of  $K$ . Then

$$\begin{aligned} \det(M) &= \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_r(\omega_1) & \dots & \text{Re}(\tau_s(\omega_1)) & \text{Im}(\tau_s(\omega_1)) \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\omega_n) & \dots & \sigma_r(\omega_n) & \dots & \text{Re}(\tau_s(\omega_n)) & \text{Im}(\tau_s(\omega_n)) \end{vmatrix} \\ &= (-1)^s \frac{1}{(2i)^s} \begin{vmatrix} \sigma_1(\omega_1) & \dots & \sigma_r(\omega_1) & \tau_1(\omega_1) & \overline{\tau_1}(\omega_1) & \dots & \tau_s(\omega_1) & \overline{\tau_s}(\omega_1) \\ \sigma_1(\omega_2) & \dots & \sigma_r(\omega_2) & \tau_1(\omega_2) & \overline{\tau_1}(\omega_2) & \dots & \tau_s(\omega_2) & \overline{\tau_s}(\omega_2) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\omega_n) & \dots & \sigma_r(\omega_n) & \tau_1(\omega_n) & \overline{\tau_1}(\omega_n) & \dots & \tau_s(\omega_n) & \overline{\tau_s}(\omega_n) \end{vmatrix} \\ &= \pm (-1)^s \frac{1}{(2i)^s} \sqrt{|\text{disc}(K)|} \neq 0 \end{aligned}$$

Therefore,  $\{v(\omega_i) : 1 \leq i \leq n\}$  is linearly independent over  $\mathbb{R}$  and

$$d(\Lambda_K) = |\det(M)| = \frac{1}{2^s} \sqrt{|\text{disc}(K)|}$$

♡

## 5.3 The Unit Theorem

**Definition 5.3.1.** A subset  $S$  of  $\mathbb{R}^n$  is **symmetric** about the origin if  $x \in S$  imply  $-x \in S$ .

**Definition 5.3.2.** A subset  $S$  of  $\mathbb{R}^n$  is **convex** if  $x, y \in S$  then  $\lambda x + (1 - \lambda)y \in S$  for all  $0 \leq \lambda \leq 1$ .

**Lemma 5.3.3 (Minkowski's Lemma).** *Let  $\Lambda$  be an  $n$ -dimensional lattice in  $\mathbb{R}^n$ , let  $S$  be convex, symmetric and measurable subset in  $\mathbb{R}^n$ , such that*

$$\mu(S) > 2^n d(\Lambda)$$

*where  $\mu$  is the Lebesgue measure of  $S$ . Then  $S$  contains some non-zero point of  $\Lambda$ . Also, if  $S$  is compact, then the strict inequality can be weakened to  $\geq$ .*

*Proof.* Let  $F$  be a fundamental parallelotope for  $\Lambda$ . Then  $\mathbb{R}^n$  is the disjoint union of translates  $x + F$  where  $x \in \Lambda$ . It follows that

$$\frac{1}{2}S = \left\{ \frac{1}{2}s \in \mathbb{R}^n : s \in S \right\} = \bigcup_{x \in \Lambda} \left( \left( \frac{1}{2}S \right) \cap (x + F) \right)$$

where the latter union is a disjoint union.

Assume the strict inequality, we have

$$\begin{aligned} d(\Lambda) &= \mu(F) < \frac{1}{2^n} \mu(S) \\ &= \mu\left(\frac{1}{2}S\right) = \sum_{x \in \Lambda} \mu\left(\left(\frac{1}{2}S\right) \cap (x + F)\right) \\ &= \sum_{x \in \Lambda} \mu\left(\left(\frac{1}{2}S - x\right) \cap F\right) \end{aligned}$$

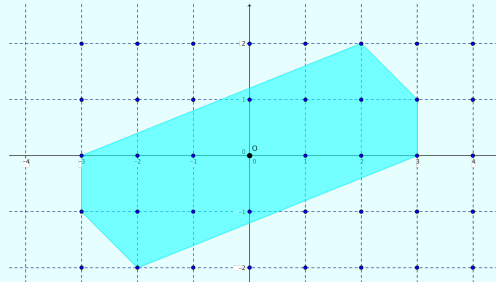
Note the last line is obtained because Lebesgue measure of a set is invariant under translation. The above shows that  $(\frac{1}{2}S - x) \cap F$  cannot be all pairwise disjoint as that would imply the measure equal 0. Therefore, there are two points  $x, y \in \Lambda$  with  $x \neq y$  such that  $(\frac{1}{2}S - x) \cap (\frac{1}{2}S - y) \neq \emptyset$  and so there exists  $s_1, s_2 \in S$  such that

$$\frac{1}{2}s_1 - x = \frac{1}{2}s_2 - y \Rightarrow x - y = \frac{1}{2}(s_1 - s_2) \in S$$

Viz,  $x - y$  is a non-zero element contained in  $S$ . This finishes the proof of the first assertion.

Now we suppose  $S$  is compact, and we know in  $\mathbb{R}^n$  this is the same as closed and bounded. For each  $m \in \mathbb{Z}_{\geq 1}$ , the first part shows the set  $(1 + \frac{1}{m})S$  contains some non-zero point  $x_m$  of  $\Lambda$ . Thus the set  $\{x_m : m \geq 1\}$  are bounded as  $m \rightarrow \infty$  since they are all in  $2S$ . However, there are only finitely many  $x$  in  $\Lambda$  contained in  $2S$  and so one of  $x_m$  is in  $(1 + \frac{1}{m})S$  infinitely many  $m$ , hence in the closure of  $S$ , which is  $S$  as  $S$  is closed. Thus the proof follows.  $\heartsuit$

**Example 5.3.4.** Below is a set satisfying Minkowski's lemma for  $\mathbb{R}^2$ :



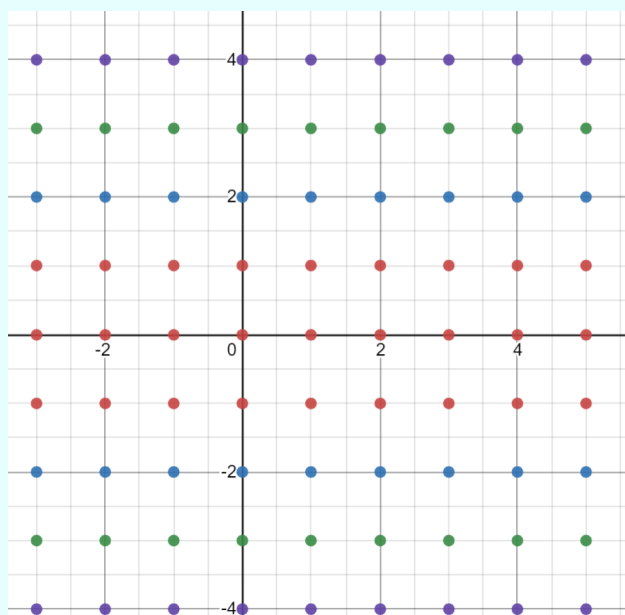
In particular, the way to think of this lemma is that if we have  $S$  has volume large enough, it contains a lattice point of our like.

**Definition 5.3.5.** Let  $K$  be a number field of degree  $n$  with  $r$  real embeddings and  $2s$  complex embeddings. Define a map from  $\mathcal{O}_K \setminus \{0\}$  to  $\mathbb{R}^{r+s}$ , denoted by  $\log$ , by the following: for all  $\alpha \in \mathcal{O}_K \setminus \{0\}$  with  $v(\alpha) = (a_1, \dots, a_n)$ , we have

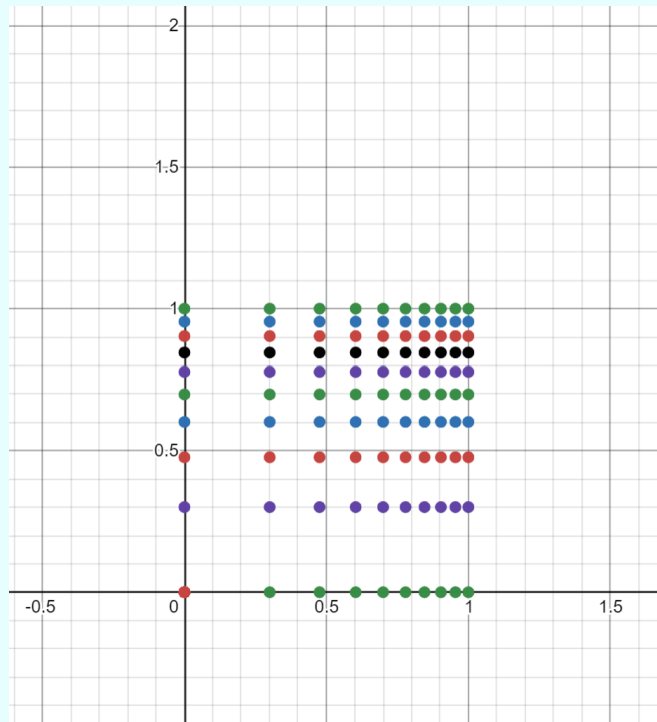
$$\log(\alpha) = (\log |a_1|, \dots, \log |a_r|, \log(a_{r+1}^2 + a_{r+2}^2), \dots, \log(a_{n-1}^2 + a_n^2))$$

**Example 5.3.6.** Let's try to have an intuitive feeling about the logarithmic embedding.

Below is an integer lattice (with 100 points plotted in total but we only showed a part of it):

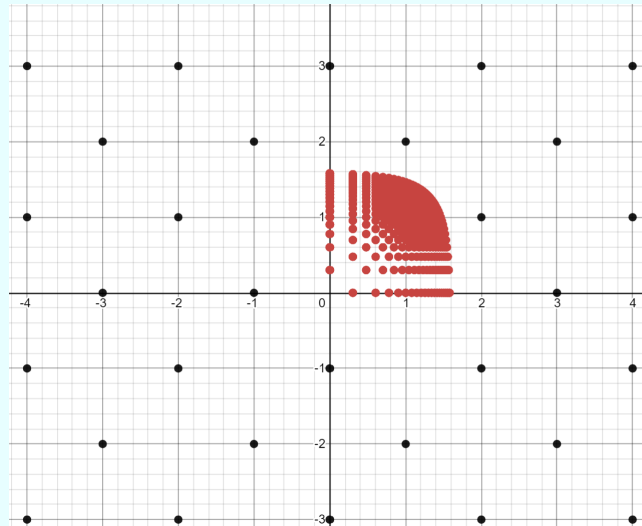


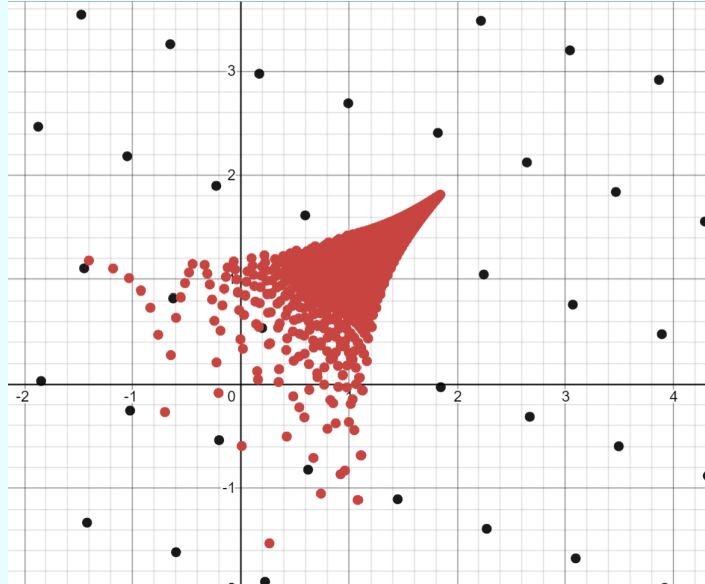
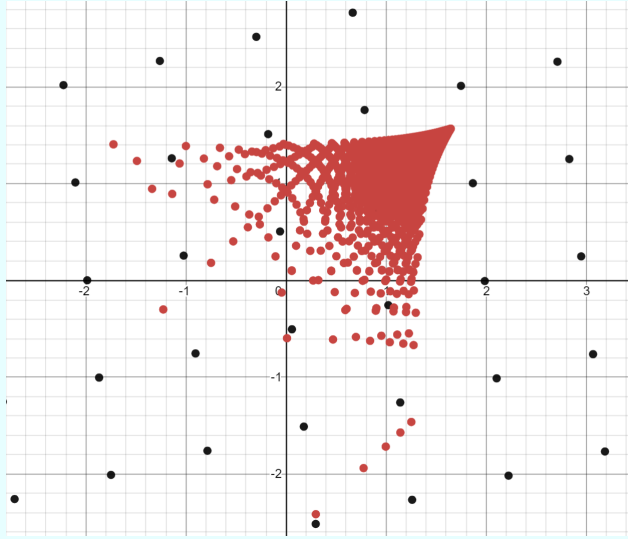
Then, after the log embedding, the lattice becomes (with all the points in the picture):



Observe the scale, i.e. log embedding is growing much slower than the standard one.

Here are few more examples (note those pictures are only to help grasp the concept and may not be accurate):





where the black dots would be the lattice and the red dots are after log embedding.

**Remark 5.3.7.** It is easy to observe

1. For all  $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ , we have  $\log(\alpha\beta) = \log(\alpha) + \log(\beta)$ .
2.  $\log(\mathcal{O}_K^*)$  contains the hyperplane  $H \subseteq \mathbb{R}^{r+s}$ , defined by  $\{(x_1, \dots, x_{r+s}) : x_1 + \dots + x_{r+s} = 0\}$  because the norm of a unit is  $\pm 1$ . To elaborate, say  $x$  is a unit, then  $N(x) = \pm 1$  where  $N(x) = \prod_{i=1}^n \sigma_i(x)$ . Then if we sum over all components of  $\log(x)$ , we get

$$\sum_{i=1}^r \log |a_i| + \sum_{j=r+1}^{r+s-1} \log(a_j + a_{j+1}) = \log\left(\prod |a_i| \cdot \prod (a_i^2 + a_{i+1}^2)\right) = \log(|N_{\mathbb{Q}}^K(a)|)$$

where we get the last part because  $\sigma_i(x) = a_i$  for  $1 \leq i \leq r$  and when  $i > r$  we get  $\text{Re}(\sigma_i(x))^2 + \text{Im}(\sigma_i(x))^2 = a_i^2 + a_{i+1}^2$  is exactly  $\sigma_i(x) \cdot \overline{\sigma_i(x)}$ . Now observe  $\log(1) = 0$  and thus we indeed have our claim.

3. Any bounded set  $A$  in  $\mathbb{R}^{r+s}$  has a finite inverse image (under  $\log$ ) in the unit group  $\mathcal{O}_K^*$  because  $A$  has a bounded, hence finite inverse image in  $\Lambda_K \in \mathbb{R}^n$ .

Those observation make us to conclude:

- (i) (1) and (2) together imply  $\log : \mathcal{O}_K^* \rightarrow H$  is a multiplicative to additive group homomorphism.
- (ii) The kernel of the map  $\log : \mathcal{O}_K^* \rightarrow H$  is finite. In addition,  $\text{Ker}(\log)$  is consisting all algebraic integers in  $K$  whose conjugates have absolute value 1. In addition, we see all such algebraic integers are roots of unity, therefore, we see  $\text{Ker}(\log)$  must be a cyclic group.
- (iii) From (3), the subgroup  $\log(\mathcal{O}_K^*)$  of  $\mathbb{R}^{r+s}$  has the property that every bounded subset is finite. By Lemma 5.2.8, we know  $\log(\mathcal{O}_K^*)$  must be a lattice in  $\mathbb{R}^{r+s}$ . We denote this lattice to be  $\Lambda_{\mathcal{O}_K^*} := \log(\mathcal{O}_K^*)$  and  $d$  be the dimension of it. Since  $\Lambda_{\mathcal{O}_K^*}$  is contained in a hyperplane  $H$ , we have  $d$  is less or equal to  $r+s-1$ .

**Lemma 5.3.8.** *Let  $K$  be a number field of degree  $n$  with  $r$  real embeddings and  $2s$  complex embeddings. Then for each fixed  $k$  where  $1 \leq k \leq r+s$  and for each  $0 \neq \alpha \in \mathcal{O}_K$ , there exists  $\beta \in \mathcal{O}_K$  such that*

$$|N_{\mathbb{Q}}^K(\beta)| \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|\text{disc}(K)|}$$

such that  $b_i < a_i$  for all  $i \neq k$  where  $\log(\alpha) = (a_1, \dots, a_{r+s})$  and  $\log(\beta) = (b_1, \dots, b_{r+s})$

*Proof.* Take  $A$  to be the subset of  $\mathbb{R}^n$  defined by the inequalities as follows:  $A := \{(x_1, \dots, x_n) : |x_i| \leq c_i \text{ for } i = 1, \dots, r \text{ and } x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \dots, x_{n-1}^2 + x_n^2 \leq c_{r+s}\}$  where the  $c_i$  can be chosen to satisfy

$$0 < c_i < e^{a_i}, 1 \leq i \leq r+s, i \neq k$$

and

$$c_1 \dots c_{r+s} = \left(\frac{2}{\pi}\right)^2 \sqrt{|\text{disc}(K)|}$$

Then it follows the Lebesgue measure of  $A$  is equal  $2^r \pi^s c_1 \dots c_{r+s} = 2^n \cdot d(\Lambda_K)$ . Thus, Minkowski's Lemma, 5.3.3, would give us a point  $y \in \Lambda_K$  that is contained in  $A$ . Therefore, by definition we have  $\beta = v^{-1}(y)$  would be the point we want where  $v$  is the standard lattice embedding into  $\mathbb{R}^n$ .  $\heartsuit$

**Lemma 5.3.9.** *Let  $K$  be a number field of degree  $n$  with signature  $(r, s)$ . Then fix any  $k$  where  $1 \leq k \leq r+s$ , there exists  $u \in \mathcal{O}_K^*$  such that  $y_i < 0$  for all  $i \neq k$  where  $\log(u) = (y_1, \dots, y_{r+s})$ .*

*Proof.* Start with any non-zero  $\alpha_1 \in \mathcal{O}_K$ , apply Lemma 5.3.8 repeatedly to obtain a sequence  $\alpha_1, \alpha_2, \alpha_3, \dots$  of non-zero elements of  $\mathcal{O}_K$  with the property that for each  $i \neq k$  and for each  $j \geq 1$ , the  $i$ th coordinate of  $\log(\alpha_{j+1})$  is less than coordinate of  $\log(\alpha_j)$ . Moreover, the number  $|N_{\mathbb{Q}}^K(\alpha_j)|$  are bounded and in  $\mathbb{Z}_{\geq 1}$ .



This imply there are only finitely many distinct ideal  $\langle \alpha_j \rangle$  in the list  $\{\langle \alpha_j \rangle : j \geq 1\}$ . Hence there exists  $j < h$  such that  $\langle \alpha_j \rangle = \langle \alpha_h \rangle$  and so  $\alpha_h = \alpha_j u$  for some  $u \in \mathcal{O}_K^*$ . Then this  $u$  would work as  $j < h$  and the coordinate condition.  $\heartsuit$

**Theorem 5.3.10 (Dirichlet's Unit Theorem).** *Let  $K$  be number field of degree  $n$  with signature  $(r, s)$ . The unit group  $\mathcal{O}_K^*$  of  $\mathcal{O}_K$  is a direct product  $W_K \times V_K$  where  $W_K$  is a finite cyclic group consisting of roots of unity in  $K$  and  $V_K$  is a free abelian group of rank  $r + s - 1$ .*

*More precisely, there are  $\zeta, \epsilon_1, \dots, \epsilon_{r+s-1} \in \mathcal{O}_K^*$ , where  $\zeta$  in an  $m$ -th root of unity, so that every  $\gamma \in \mathcal{O}_K^*$  can be written as a unique representation using those elements, i.e.  $\gamma = \zeta^l \prod_{i=1}^{r+s-1} \epsilon_{r+s-1}^{k_i}$  where  $k_i \in \mathbb{Z}$ .*