

# Number Fields

February 12, 2020

## 1 Algebraic Numbers and Algebraic Integers; Number Fields

Here, we will use  $F$  to denote any field containing  $\mathbb{Q}$ , for instance  $F = \mathbb{C}$ . Recall that an element  $\alpha \in F$  is **algebraic** (over  $\mathbb{Q}$ ) if it is the root of some polynomial in  $\mathbb{Q}[x]$ . If so, there is a unique monic polynomial  $m_\alpha \in \mathbb{Q}[x]$  of minimal degree with  $m_\alpha(\alpha) = 0$ , called the **minimal polynomial** of  $\alpha$ . The **degree** of  $\alpha$  is the degree of  $m_\alpha$ .

**Proposition 1.1.** *Suppose  $\alpha \in F$  is algebraic. Then  $m_\alpha$  is irreducible in  $\mathbb{Q}[x]$ , and if  $f \in \mathbb{Q}[x]$ , then  $f(\alpha) = 0 \iff m_\alpha | f$ .*

*Proof.* If  $m_\alpha = fg$ , then  $f(\alpha)g(\alpha) = 0$ , and since fields are integral domains we have  $f(\alpha) = 0$  or  $g(\alpha) = 0$ . By minimality of degree,  $f$  or  $g$  is constant.

If  $f(\alpha) = 0$ , we write  $f = gm_\alpha + h$ , with  $g, h \in \mathbb{Q}[x]$ , and  $\deg h < \deg m_\alpha$ . Then  $h(\alpha) = f(\alpha) - g(\alpha)m_\alpha(\alpha) = 0$ , and so by minimality  $h = 0$  and  $m_\alpha | f$ .

I.e.  $\{f : f(\alpha) = 0\}$  is a principal ideal in  $\mathbb{Q}[x]$  generated by  $m_\alpha$  □

If  $\alpha \in F$ , define  $\mathbb{Q}(\alpha)$  to be the smallest subfield of  $F$  containing  $\alpha$ . Explicitly, it can be shown that  $\mathbb{Q}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \mathbb{Q}[x], g(\alpha) \neq 0 \right\}$ .

**Proposition 1.2.** *If  $\alpha \in F$  is algebraic of degree  $n$ , then  $1, \alpha, \dots, \alpha^{n-1}$  is a  $\mathbb{Q}$ -basis for  $\mathbb{Q}(\alpha)$ . Conversely, if  $[\mathbb{Q}(\alpha) : \mathbb{Q}] := \dim_{\mathbb{Q}} \mathbb{Q}(\alpha)$  is finite, say  $n$ , then  $\alpha$  is algebraic of degree  $n$ .*

*Proof.* Consider the homomorphism  $\phi : \mathbb{Q}[x] \rightarrow F; f \mapsto f(\alpha)$ . Then  $\ker(\phi) = (m_\alpha)$  which is maximal, so  $\text{im } \phi$  is a field, and hence equal to  $\mathbb{Q}(\alpha)$ . As  $\deg m_\alpha = n$ , a basis for  $\mathbb{Q}[x]/(m_\alpha)$  is  $1, x, \dots, x^{n-1}$ , and hence  $1, \alpha, \dots, \alpha^{n-1}$  is a basis for  $\mathbb{Q}(\alpha)$ .

For the converse part, if  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n < \infty$ , then  $1, \alpha, \dots, \alpha^n$  are linearly dependent and so  $\alpha$  is algebraic of some degree. By the first part, this degree is  $n$ . □

**Proposition 1.3.**  *$\{\alpha \in F : \alpha \text{ algebraic}\}$  is a subfield of  $F$ .*

*Galois theory.* It is enough to prove that it is closed under  $+$ ,  $\times$  and inverse. For  $+$  and  $\times$  see **1.6** below for a stronger statement. If  $0 \neq \alpha$  is algebraic, then  $\sum^n b_j \alpha^j = 0 \implies \sum^n b_{n-j} (\alpha^{-1})^j = 0$ , and so  $\alpha^{-1}$  is algebraic. □

$\alpha \in F$  is an **algebraic integer** if there is a monic polynomial  $f \in \mathbb{Z}[x]$  with  $f(\alpha) = 0$ .

**Lemma 1.5.**

1. Let  $\alpha \in F$ . Then the following are equivalent:

- (a)  $\alpha$  is an algebraic integer
- (b)  $\alpha$  is algebraic and  $m_\alpha \in \mathbb{Z}[x]$
- (c)  $\mathbb{Z}[\alpha]$  is a finitely generated  $\mathbb{Z}$ -module

If these hold, then  $1, \alpha, \dots, \alpha^{d-1}$  is a  $\mathbb{Z}$ -bases for  $\mathbb{Z}[\alpha]$ , with  $d = \deg \alpha$ .

2.  $\alpha \in \mathbb{Q}$  is an algebraic integer  $\iff \alpha \in \mathbb{Z}$

Recall the notation that, if  $\alpha_1, \dots, \alpha_n \in F$ , then  $\mathbb{Z}[\alpha_1, \dots, \alpha_n]$  is the smallest subring of  $F$  containing  $\{\alpha_i : i \in [n]\}$ , i.e. the set of all finite sums of terms of the form  $A\alpha_1^{i_1} \dots \alpha_n^{i_n}$  for  $A, i_1, \dots, i_n \in \mathbb{Z}$ .

*Proof.*

1. a.  $\implies$  b. Suppose  $f(\alpha) = 0, f \in \mathbb{Z}[x]$ ,  $f$  monic. Then **1.1** gives that  $f = gm_\alpha$  for some  $g \in \mathbb{Q}[x]$  necessarily monic. Gauss's lemma from GRM gives us that  $m_\alpha, g$  are in  $\mathbb{Z}[x]$ .

b.  $\implies$  c. Write  $m_\alpha = x^d + \sum_{j=1}^{d-1} b_j x^j$ , for  $b_j \in \mathbb{Z}$ . Then  $\alpha^d = -\sum_{j=1}^{d-1} b_j \alpha^j$ , from which we say that every  $\alpha^n$  is a  $\mathbb{Z}$ -linear combination of  $1, \alpha, \dots, \alpha^{d-1}$ . So  $\mathbb{Z}[\alpha]$  is generated by  $1, \alpha, \dots, \alpha^{d-1}$  as a  $\mathbb{Z}$ -module. There is no linear relation between  $1, \alpha, \dots, \alpha^{d-1}$ , as  $d = \deg \alpha$ . So  $\mathbb{Z}[\alpha]$  is finitely generated and  $1, \alpha, \dots, \alpha^{d-1}$  is a  $\mathbb{Z}$ -basis.

c.  $\implies$  a. Assume  $\mathbb{Z}[\alpha]$  is finitely generated by  $g_1(\alpha), \dots, g_r(\alpha)$ . For some  $g_i \in \mathbb{Z}[x]$ . Let  $k = \max\{\deg g_i\}$ . Then  $\mathbb{Z}[\alpha]$  is certainly generated by  $1, \alpha, \dots, \alpha^k$  as a  $\mathbb{Z}$ -module. So  $\alpha^{k+1} = \sum_{j=0}^k b_j \alpha^j$  for  $b_j \in \mathbb{Z}$ , and so  $\alpha$  is an algebraic integer.

2.  $\alpha \in \mathbb{Q} \implies m_\alpha = x - \alpha$ , and so  $\alpha$  is an algebraic integer  $\iff \alpha \in \mathbb{Z}$  using (a)  $\iff$  (b). □

**Theorem 1.6.** If  $\alpha, \beta \in F$  are algebraic integers, then so are  $\alpha\beta, \alpha \pm \beta$ .

*Proof.* The  $\mathbb{Z}$ -module  $\mathbb{Z}[\alpha, \beta]$  is generated by  $\{\alpha^i \beta^j : 0 \leq i < \deg \alpha; 0 \leq j < \deg \beta\}$ , and so is finitely generated. Hence so is the submodule  $\mathbb{Z}[\alpha\beta] \subseteq \mathbb{Z}[\alpha, \beta]$ . So  $\alpha\beta$  is an algebraic integer by **1.4**. The same applies for  $\alpha + \beta, \alpha - \beta$ . □

Now to introduce the main characters of this course:

An **algebraic number field** (or just **number field**) is a field  $K \supset \mathbb{Q}$  which is a finite extension, i.e.  $[K : \mathbb{Q}] < \infty$ . The **ring of integers of  $K$** , written  $\mathfrak{o}_K$ , is the set of algebraic integers in  $K$ . By **1.6** it is a ring. It is useful to have the converse:

**Proposition 1.7.** Let  $\alpha \in F$  be algebraic. Then for some  $0 \neq b \in \mathbb{Z}$ ,  $b\alpha$  is an algebraic integer.

*Proof.* Exercise. □

**Theorem 1.8** (Primitive Element). If  $K$  is a number field, then  $K = \mathbb{Q}(\alpha)$  for some  $\alpha \in K$ .

*Proof.* Done in Galois theory. □

## 2 Quadratic Fields

$K$  is a **quadratic field** if  $[K : \mathbb{Q}] = 2$ . In this case, let  $\alpha \in K \setminus \mathbb{Q}$ . The minimal polynomial  $m_\alpha$  is a quadratic, and so solving we get  $\alpha = x + \sqrt{y}^1$  for  $x, y \in \mathbb{Q}, y \neq 0$ . Since  $y$  is not a rational square, we can write  $y$  uniquely as  $z^2d$  for  $z \in \mathbb{Q} \setminus \{0\}, d \neq 0, 1$  a square-free integer. So  $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[x]/(x^2 - d)$ . If  $d' \neq d$  also square-free, then  $\mathbb{Q}(\sqrt{d}) \not\cong \mathbb{Q}(\sqrt{d'})$ .

Now we want to compute  $\mathfrak{o}_K$ . Let  $\alpha = u + v\sqrt{d} \in K$  for  $u, v \in \mathbb{Q}$ . If  $v = 0, \alpha \in \mathfrak{o}_K \iff \alpha \in \mathbb{Z}$ . Otherwise,  $\alpha \notin \mathbb{Q}$ , and  $m_\alpha = x^2 - 2ux + (u^2 - dv^2)$ . So  $\alpha \in \mathfrak{o}_K \iff 2u \in \mathbb{Z}$  and  $u^2 - dv^2 \in \mathbb{Z}$ .

If  $u \in \mathbb{Z}$ , then  $dv^2 \in \mathbb{Z}$ , and since  $d$  is square-free, we must have  $v \in \mathbb{Z}$ . Otherwise,  $u = \frac{2a+1}{2}, a \in \mathbb{Z}$ , and we must have  $4dv^2 - (2a+1)^2 \in 4\mathbb{Z}$ , which holds if and only if  $v = \frac{k}{2}, k \in \mathbb{Z}$  and  $dk^2 \equiv 1 \pmod{4}$ . If  $d \equiv 1 \pmod{4}$ , this holds if and only if  $k$  is odd, and if  $d$  is not  $1 \pmod{4}$ , then this congruence cannot hold.

In conclusion,

**Theorem 2.1.** *If  $d \in \mathbb{Z} \setminus \{0, 1\}$  is square-free, and  $K = \mathbb{Q}(\sqrt{d})$ , then:*

1. *If  $d \not\equiv 1 \pmod{4}$ , then  $\mathfrak{o}_K = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}]$ .*
2. *If  $d \equiv 1 \pmod{4}$ , then  $\mathfrak{o}_K = \{u + v\sqrt{d} : u, v \in \frac{1}{2}\mathbb{Z}, u - v \in \mathbb{Z}\} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$*

Examples: If  $d = -3$ , then  $\mathfrak{o}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\xi_3]$ .

Note that, for a general number field  $K$ , we needn't have  $\mathfrak{o}_K = \mathbb{Z}[\alpha]$  for  $\alpha \in K$ , and in fact for  $\deg K > 2$  this method is unlikely to be practical for computing  $\mathfrak{o}_K$ .

## 3 Embeddings

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

**Theorem 3.1.** *There are precisely  $n$  homomorphisms  $\sigma_i : K \hookrightarrow \mathbb{C}$ . These are called the **complex embeddings** of  $K$ . More generally, if  $\mathbb{Q} \subset F \subset K$  are number fields, then each of the  $[F : \mathbb{Q}]$  complex embeddings of  $F$  extend to exactly  $[K : F]$  complex embeddings of  $K$ .*

*Proof. (Galois Theory).* Assume  $K = \mathbb{Q}(\theta) = \mathbb{Q}[x]/(m_\theta)$  by the theorem of the primitive element. Then to give  $\sigma : K \hookrightarrow \mathbb{C}$  is the same as to give  $\phi : \mathbb{Q}[x] \rightarrow \mathbb{C}$  with  $\phi(m_\theta) = 0$ . If  $z = \phi(x)$ , then  $\phi(m_\theta) = m_\theta(z)$ , giving a bijection  $\{\sigma : K \hookrightarrow \mathbb{C}\} \leftrightarrow \{\text{roots of } m_\theta \in \mathbb{C}\}$ , coming from  $\sigma \mapsto \sigma(\theta)$ . The second part is the same as the first, but replacing  $\mathbb{Q}$  by  $F$  since  $\theta$  has degree  $[K : F]$  over  $F$ .  $\square$

Remarks:

1. If  $K \subset \mathbb{C}$  we can choose  $\sigma$  to be the inclusion.
2. For some  $r \in \{0, \dots, n\}$ , exactly  $r$  of the  $\sigma_i$  will be **real**, i.e.  $\sigma_i(K) \subseteq \mathbb{R}$ . The remaining embeddings will then come in complex conjugate pairs  $\sigma_i, \overline{\sigma_i}$ . So  $n = r + 2s$ , where  $r$  is the number of real embeddings, and  $s$  is the number of complex conjugate pairs of embeddings.

---

<sup>1</sup>By  $\sqrt{y}$  we just mean some  $\beta \in K$  with  $\beta^2 = y$

Examples:

$\mathbb{Q}(\sqrt{d})$ . We have two cases:

$d > 0$ . There are 2 real embeddings:  $\sigma_1 : \sqrt{d} \mapsto +\sqrt{d} \in \mathbb{R}$ , and  $\sigma_2 : \sqrt{d} \mapsto -\sqrt{d} \in \mathbb{R}$ . So  $(r, s) = (2, 0)$ .

$d < 0$ . There is now one pair of complex embeddings, given by  $\sigma_1 : \sqrt{d} \mapsto i\sqrt{|d|}$ ;  $\sigma_2 : \sqrt{d} \mapsto -i\sqrt{|d|}$ . So  $(r, s) = (0, 1)$ .

$\mathbb{Q}(\sqrt[3]{2})$ . We have 1 real embedding  $\sqrt[3]{2} \mapsto \sqrt[3]{2} \in \mathbb{R}$ , and the two complex embeddings  $\sqrt[3]{2} \mapsto \omega^{\pm 1} \sqrt[3]{2} \in \mathbb{C}$ , so  $(r, s) = (1, 1)$ .

**Proposition 3.2.** *If  $\alpha \in K$ , then the complex numbers  $\sigma_i(\alpha)$  are the complex roots of  $m_\alpha$ , each taken  $n/\deg(\alpha)$  times.*

*Proof.* Apply the 2<sup>nd</sup> part of 3.1 with  $F = \mathbb{Q}(\alpha)$ . □

## 4 Norm and Trace

Given  $K$  a number field,  $\alpha \in K$ , define a map  $u_\alpha : K \rightarrow K$  by  $u_\alpha(x) = \alpha x$ .  $K$  is a  $\mathbb{Q}$ -vector space, and  $u_\alpha$  is a  $\mathbb{Q}$ -linear map. Define:

- $f_\alpha$  to be the **characteristic polynomial** of  $u_\alpha$ , so  $f_\alpha = \det(x - u_\alpha) \in \mathbb{Q}[x]$ , monic
- $N_{K/\mathbb{Q}}(\alpha) = \det(u_\alpha) \in \mathbb{Q}$ , the **norm** of  $\alpha$
- $\text{Tr}_{K/\mathbb{Q}}(\alpha) = \text{tr}(u_\alpha) \in \mathbb{Q}$ , the **trace** of  $\alpha$

More explicitly, let  $\beta_1, \dots, \beta_n$  be a  $\mathbb{Q}$ -basis for  $K$ . Then  $\alpha\beta_i = \sum_{j=1}^n A_{ji}\beta_j$  for some  $A \in M_{n,n}(\mathbb{Q})$ . Then  $f_\alpha = \det(x \cdot I_n - A)$ ,  $N_{K/\mathbb{Q}}(\alpha) = \det(A)$ ,  $\text{Tr}_{K/\mathbb{Q}} = \text{tr}(A)$ . As an exercise, work these out for  $\mathbb{Q}(\sqrt{d})$ .

**Proposition 4.1.**

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha\beta) &= N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\beta) \\ \text{Tr}_{K/\mathbb{Q}}(\alpha + \beta) &= \text{Tr}_{K/\mathbb{Q}}(\alpha) + \text{Tr}_{K/\mathbb{Q}}(\beta) \end{aligned}$$

*Proof.* From the definition,  $u_{\alpha\beta} = u_\alpha u_\beta$ , and  $u_{\alpha+\beta} = u_\alpha + u_\beta$ , so the result follows from linear algebra. □

**Theorem 4.2.**

1. The minimal polynomial of  $u_\alpha$  is  $m_\alpha$ , and  $f_\alpha \prod_{i=1}^n (x - \sigma_i(\alpha)) = m_\alpha^{n/d}$ , where  $\deg(\alpha) = d$ .
2.  $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ ,  $\text{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ .

We call the  $\sigma_i(\alpha)$  the **conjugates** of  $\alpha$ .

*Proof.* Note that 1.  $\implies$  2., because  $\det u_\alpha = (-1)^n f_\alpha(0)$ , the product of the eigenvalues, and  $\text{tr } u_\alpha = -(\text{coeff. of } x^{n-1} \text{ in } f_\alpha)$ .

For 1., we first do the case  $\deg \alpha = n$ , i.e.  $K = \mathbb{Q}(\alpha)$ . Then  $f_\alpha, m_\alpha \in \mathbb{Q}[x]$  are monic of degree  $n$ , and if  $\beta \in K$  then  $f_\alpha(\alpha)\beta = f_\alpha(u_\alpha)\beta = 0$  by Cayley-Hamilton. So  $f_\alpha(\alpha) = 0 \implies m_\alpha = f_\alpha$ .

In general, if  $[K : \mathbb{Q}(\alpha)] = \frac{n}{d}$ , then  $K \cong \mathbb{Q}(\alpha)^{\oplus(n/d)}$ , and then  $f_\alpha = (\text{char. poly. of } u_\alpha \text{ on } \mathbb{Q}(\alpha)^{n/d} = m_\alpha^{n/d} = \prod_{i=1}^n (x - \sigma_i(\alpha)))$ .  $\square$

**Corollary 4.3.**

1. Let  $\alpha \in K$ . Then  $\alpha = 0 \iff N_{K/\mathbb{Q}}(\alpha) = 0$ .
2. Let  $\alpha \in \mathfrak{o}_K$ . Then  $f_\alpha \in \mathbb{Z}[x]$ , and  $N_{K/\mathbb{Q}}(\alpha), \text{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ . Moreover,  $N_{K/\mathbb{Q}}(\alpha) \in \{\pm 1\}$  if and only if  $\alpha \in \mathfrak{o}_K^*$  is a **unit**, i.e.  $\alpha^{-1} \in \mathfrak{o}_K$ .

*Proof.*

1.  $\alpha = 0 \iff \sigma_i(\alpha) = 0$  for all  $i$ .
2.  $m_\alpha \in \mathbb{Z}[x]$ , so  $f_\alpha \in \mathbb{Z}[x]$ , and hence  $N_{K/\mathbb{Q}}(\alpha), \text{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ , since they are coefficients of  $f_\alpha$  up to a choice of sign.

If  $\alpha$  is a unit, then  $N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\alpha^{-1}) = N_{K/\mathbb{Q}}(\alpha \alpha^{-1}) = N_{K/\mathbb{Q}}(1) = 1$ , and so  $N_{K/\mathbb{Q}}(\alpha)$  is a unit and an integer, so in  $\{\pm 1\}$ .

If  $N_{K/\mathbb{Q}}(\alpha) \in \{\pm 1\}$ ,  $f_\alpha = x^n + \sum_{i=1}^{n-1} b_i x^i \pm 1$ , so  $f_\alpha(\alpha) = 0 \implies \alpha \cdot (\alpha^{n-1} + \sum_{i=1}^{n-1} b_i \alpha^{i-1}) = \mp 1$ , so  $\alpha^{-1} \in \mathfrak{o}_K$  and we have an explicit representation of  $\alpha^{-1}$ .  $\square$

Note that we can also define, if  $\mathbb{Q} \subset F \subset K$  the relative trace  $\text{Tr}_{K/F}(\alpha), N_{K/F}(\alpha)$  as the trace/determinant of  $u_\alpha$  viewed as an  $F$ -linear map from  $K \simeq F^{[K:F]}$  to itself, and we have that:

$$\text{Tr}_{K/\mathbb{Q}} = \text{Tr}_{F/\mathbb{Q}} \cdot \text{Tr}_{K/F} \quad N_{K/\mathbb{Q}} = N_{F/\mathbb{Q}} \cdot N_{K/F}$$

## 5 Some Modules from GRM

**Proposition 5.1.**  *$G$  is a finitely generated abelian group written additively with no torsion, i.e. no elements of finite order, and a finite set of generators  $x_1, \dots, x_n$ . Let  $H \subset G$  be the subgroup generated by  $y_1, \dots, y_n \in G$ , where  $y_i = \sum_{j=1}^n A_{ji} x_j$  for some  $A \in \text{Mat}_{n,n}(\mathbb{Z})$ . Then if  $\det(A) \neq 0$ ,  $H$  has finite index in  $G$ , with  $(G : H) = |\det A|$ .*

*Proof.* Using Smith normal form,  $A = PDQ$  for  $P, Q, D$  integer  $n \times n$  matrices where  $\det P, \det Q \in \{\pm 1\}$  and  $D = \text{diag}(d_1, \dots, d_n)$  for  $d_i \geq 0, d_i | d_{i+1}$ . Then  $G/H \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$ , where  $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ .

Hence if  $|\det A| = \prod_i d_i \neq 0$ , then  $G/H$  contains no  $\mathbb{Z}$  terms and has dimension  $\prod_i d_i = |\det A|$ .  $\square$

Let  $V$  be a  $\mathbb{Q}$ -vector space, and  $\dim(V) = n < \infty$ . Let  $H \subset V$  be a subgroup, viewed as a sub- $\mathbb{Z}$ -module. Then define:

$$\text{rank}(H) = \dim(\text{span}(H)) \in \{0, 1, \dots, n\}$$

**Proposition 5.2.** *If  $H$  is finitely generated as an abelian group then  $H = \bigoplus_{i=1}^r \mathbb{Z}v_i$  where  $r = \text{rank}(H)$  and  $x_1, \dots, x_r \in V$  are linearly independent.*

*Proof.*  $H$  has no torsion as  $V$  is a  $\mathbb{Q}$ -vector space, so by classification  $H$  is an abelian group freely generated by some  $x_1, \dots, x_r$ . If  $a_i \in \mathbb{Q}$  and  $\sum a_i x_i = 0$  in  $V$ , then clearing denominators we have  $\sum b_i x_i = 0$  with  $b_i \in \mathbb{Z}$ . So we must have  $b_i = 0$  for all  $i$ , so  $a_i = 0$  and the  $x_i$  are linearly independent, and  $r = \text{rank}(H)$  by the definition of rank.  $\square$

## 6 Discriminants and Integral Bases

Let  $\alpha_1, \dots, \alpha_n \in K$ . Define the *discriminant*

$$\text{Disc}(\alpha_1) = \text{Disc}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \in \mathbb{Q}$$

**Theorem 6.1.**

1.  $\text{Disc}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$ .
2.  $\text{Disc}(\alpha_i) \neq 0 \iff \alpha_1, \dots, \alpha_n$  is a  $\mathbb{Q}$ -basis for  $K$ .
3. If  $\beta_i = \sum_{j=1}^n A_{ji} \alpha_j$  for  $A \in \text{Mat}_{n,n}(\mathbb{Q})$ , then  $\text{Disc}(\beta_i) = (\det A)^2 \text{Disc}(\alpha_i)$
4. Suppose  $(\alpha_i)$  is a  $\mathbb{Q}$ -basis. Then  $\text{Disc}(\alpha_i)$  depends only on the subgroup  $\mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n \in K$ .

*Proof.*

1. Let  $\Delta = (\sigma_i(\alpha_j))_{ij} \in \text{Mat}_{n,n}(\mathbb{C})$ . Then  $(\Delta^\top \Delta)_{ij} = \sum_{k=1}^n \sigma_k(\alpha_i) \sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i \alpha_j) = \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)$

So  $(\det \Delta)^2 = \det(\Delta^\top \Delta) = \det \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)$ .

2. If  $\alpha_1, \dots, \alpha_n$  is not a  $\mathbb{Q}$ -basis, then there are some  $b_1, \dots, b_n \in \mathbb{Q}$ , not all 0, with  $\sum b_j \alpha_j = 0$ . Then for all  $i$ ,  $0 = \sigma_i(\sum_{j=1}^n b_j \alpha_j) = \sum_{j=1}^n b_j \sigma_i(\alpha_j)$ , so  $\det \Delta = 0$ , hence  $\text{disc}(\alpha_i) = 0$ .

For the other direction, suppose  $(\alpha_i)$  is a  $\mathbb{Q}$ -basis for  $K$ , and let  $T = (\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))_{ij}$ . It is enough to prove that, for  $b \in \mathbb{Q}^n \setminus \{0\}$ ,  $Tb \neq 0$ , or equivalently that there is  $c \in \mathbb{Q}^n$  such that  $c^\top T b \neq 0$ . But if  $\beta = \sum_j j b_j \alpha_j$ ,  $\gamma = \sum_j c_j \alpha_j$ , then  $c^\top T b = \sum_{i,j} c_i \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) b_j = \text{Tr}_{K/\mathbb{Q}}(\sum_{i,j} c_i b_j \alpha_i \alpha_j) = \text{Tr}_{K/\mathbb{Q}}(\beta \gamma)$ , so taking  $\gamma = \frac{1}{\beta}$ , we get  $\text{Tr}_{K/\mathbb{Q}}(1) = n \neq 0$ .

3.  $\Delta = (\sigma_i(\alpha_j))$ ,  $\Delta' = (\sigma_i(\beta_j))$ , so  $\Delta'_{ij} = \sum_k \sigma_i(A_{kj} \alpha_k) = \sum_k A_{kj} \sigma_i(\alpha_k) = (\delta A)_{ij}$ . Hence  $\det \Delta' = \det \Delta \det A$ , and result follows by part 1.
4. If  $(\alpha_i), (\beta_i)$ , generate the same subgroup, then  $\beta_i = \sum A_{ji} \alpha_j$ , where  $A_{ij} \in \mathbb{Z}$ ,  $\det A \in \{\pm 1\}$ . Then by part 3,  $\text{Disc}(\beta_i) = (\det A)^2 \text{Disc}(\alpha_i) = \text{Disc}(\alpha_i)$ .

$\square$

If  $H \subset K$  is a finitely generated subgroup of rank  $n$ , and  $(\alpha_1, \dots, \alpha_n)$  is a  $\mathbb{Z}$ -basis for  $H$ , then above implies that  $\text{Disc}(\alpha_1, \dots, \alpha_n)$  is a non-zero rational, depending only on  $H$ , which we call  $\text{Disc}(H)$ .

**Lemma 6.2.** If  $H \subset H' \subset K$  are finitely generated subgroups of rank  $n$ , then

$$\text{Disc}(H) = (H' : H)^2 \text{Disc}(H')$$

*Proof.* Pick  $\mathbb{Z}$ -bases  $(\alpha_i), (\alpha'_i)$  for  $H, H'$ . Then  $\alpha_i = \sum_j B_{ji} \alpha'_j$ , for  $B \in \text{Mat}_{n,n}(\mathbb{Z})$ . Then by **6.1**(3.), together with **5.1**, give that:

$$(H' : H)^2 = (\det B)^2 = \text{Disc}(H) / \text{Disc}(H')$$

□

**Theorem 6.3.** *There exist  $\omega_1, \dots, \omega_n \in \mathfrak{o}_K$  such that  $\mathfrak{o}_K = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_n$  (i.e. that  $\mathfrak{o}_K$  is finitely generated as a  $\mathbb{Z}$ -module). We say that  $(\omega_i)$  is an **integral basis** for  $K$ .*

*Proof.* Certainly, there is  $\omega_1, \dots, \omega_n \in \mathfrak{o}_K$  which form a  $\mathbb{Q}$ -basis for  $K$  - take any  $\mathbb{Q}$ -basis of  $K$  and multiply by a suitable non-zero integer. Then for such a basis,  $\text{Disc}(H) \in \mathbb{Z} \setminus \{0\}$  where  $H = \sum_i \mathbb{Z}\omega_i \subset K$ .

Choose such a basis with  $|\text{Disc}(H)|$  minimal. Then let  $\alpha \in \mathfrak{o}_K$ , and let  $H' = \mathbb{Z}\alpha + H \subset K$ . Then  $H' \subset H$  are finitely generated of rank  $n$ , and so by **6.2**,  $\text{Disc}(H) = (H' : H)^2 \text{Disc}(H')$ , and by minimality of  $\text{Disc}(H)$ ,  $H' = H$ , so  $\alpha \in H$ . □

The **discriminant of  $K$**   $d_K = \text{Disc}(\mathfrak{o}_K) = \text{Disc}(\omega_i)$  for any integral basis  $(\omega_i)$ .

Example: Let  $K = \mathbb{Q}(\sqrt{d})$  for  $d$  a square free integer not 0 or 1.

$d \not\equiv 1 \pmod{4}$ : An integral basis is  $\{1, \sqrt{d}\}$  and so we have  $\Delta = (\sigma_i(\alpha_k)) = \begin{pmatrix} 1 & \delta \\ 1 & -\delta \end{pmatrix}$ , where  $\sigma_1(\sqrt{d}) = \delta, \sigma_2(\sqrt{d}) = -\delta, \delta^2 = d$ , and so  $d_K = (\det \Delta)^2 = 4d$ .

$d \equiv 1 \pmod{4}$ : An integral basis is  $\{1, \frac{1+\sqrt{d}}{2}\}$ . Then  $d_K = (\det \Delta)^2 = \left| \begin{pmatrix} 1 & (1+\delta)/2 \\ 1 & (1-\delta)/2 \end{pmatrix} \right|^2 = d$ .

We will now have a few useful results to help with computation of discriminants:

**Proposition 6.4.** *Suppose  $K = \mathbb{Q}(\theta)$ , and  $f = m_\theta$  is the minimal polynomial of  $\theta$ . Then:*

$$\text{Disc}(1, \theta, \dots, \theta^{n-1}) = \prod_{i < j} (\sigma_i(\theta) - \sigma_j(\theta))^2 = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f'(\theta))$$

*Proof.* Recall the **Vandermonde determinant**:

$$\text{VDM}(x_1, \dots, x_n) = \left| \begin{pmatrix} x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_n \\ 1 & 1 & \dots & 1 \end{pmatrix} \right| = \prod_{i < j} (x_i - x_j)$$

Then  $\text{Disc}(1, \dots, \theta^{n-1}) = \text{VDM}(\sigma_1(\theta), \dots, \sigma_n(\theta))^2$ , giving the first equality. For the second, see example sheet 1 q.7. □

**Proposition 6.5.** *Let  $\omega_1, \dots, \omega_n \in \mathfrak{o}_K$  with  $\text{Disc}(\omega_i)$  squarefree. Then  $(\omega_i)$  is an integral basis.<sup>2</sup>*

*Proof.* Let  $H = \sum \mathbb{Z}\omega_j \subset \mathfrak{o}_K$ . Then **6.2** implies that  $\text{Disc}(\omega_i) = (\mathfrak{o}_k : H)^2 \text{Disc}(\mathfrak{o}_k)$ . Since  $\text{Disc}(\omega_i)$  is squarefree, then  $(\mathfrak{o}_K : H) = 1$  and  $\mathfrak{o}_K = H$ . □

<sup>2</sup>The converse is false, e.g. for  $\mathbb{Q}(\sqrt{d})$  with  $d \not\equiv 1 \pmod{4}$  gives  $d_K = 4d$ , which is not squarefree.

## 7 Ideals I

Example:  $\mathbb{Q}(\sqrt{-5}) = K$ ,  $\mathfrak{o}_K = \mathbb{Z}[\sqrt{-5}]$ . Then  $6 = 2 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , and so  $\mathfrak{o}_K$  is not a UFD. But it turns out that we can restore unique factorisation by replacing elements of  $\mathfrak{o}_K$  by ideals.

### Proposition 7.1.

1. Let  $I \subset \mathfrak{o}_K$  be a nonzero ideal. Then  $I = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i$  for some  $\mathbb{Q}$ -linearly independent  $\alpha_i \in I$ , and  $(\mathfrak{o}_K : I)^2 = \frac{\text{Disc}(I)}{d_K}$ .
2. If  $0 \neq \alpha \in \mathfrak{o}_K$ , then  $(\mathfrak{o}_K : \alpha\mathfrak{o}_K) = |\text{N}_{K/\mathbb{Q}}(\alpha)|$ .

If  $I \subset \mathfrak{o}_K$  is a nonzero ideal, its **norm** is  $N(I) := (\mathfrak{o}_K : I) \in \mathbb{Z}_{>0}$ .

*Proof.*

1. Since  $\mathfrak{o}_K$  is finitely generated as an abelian group, so is  $I$ . Let  $0 \neq \alpha \in I$ , and let  $\omega_1, \dots, \omega_n$  be an integral basis for  $K$ . Then  $\alpha\omega_1, \dots, \alpha\omega_n$  are  $\mathbb{Q}$ -linearly independent elements of  $I$ , so  $I$  has rank  $n$ . By proposition 5.2,  $I$  is free, and the second statement comes from lemma 6.2.
2. If  $I = \alpha\mathfrak{o}_K$  is principal, then we can take  $\alpha_i = \alpha\omega_i$  in (1.), and then  $\text{Disc}(I) = \text{Disc}(\alpha\omega_i) = (\det \sigma_i(\alpha\omega_j))^2 = (\det \sigma_i(\alpha)\sigma_i(\omega_j))^2 = \text{N}_{K/\mathbb{Q}}(\alpha)^2 d_K$ .  
And so by (1.),  $(\mathfrak{o}_K : \alpha\mathfrak{o}_K)^2 = (\text{N}_{K/\mathbb{Q}}(\alpha))^2$ .

□

### Corollary 7.2.

1.  $I \neq \{0\} \implies I \cap \mathbb{Z} \neq \{0\}$ .
2. There are only finitely many ideals of a given norm.

*Proof.*

1. Considering the quotient ring  $\mathfrak{o}_K/I$ , we see that for any  $x$  in this ring,  $N(I)x = 0$  by Lagrange, and so  $N(I) \in I$ .
2. If  $I$  is of norm  $M$ , then  $M \in I$ , and so  $\sigma_K \supset I \supset M\sigma_K$ . There is a bijection between “ideals of  $\sigma_K$  containing  $M\sigma_K$ ” and “ideals of  $\mathfrak{o}_K/M\mathfrak{o}_K$ ” by isomorphism theorems. This second set is finite as  $\mathfrak{o}_K/M\mathfrak{o}_K$  is finite.

□

Recall that an ideal  $P \subset \mathfrak{o}_K$  is **prime** if  $P \neq \mathfrak{o}_K$  and for all  $\alpha, \beta \in \mathfrak{o}_K$ ,  $\alpha\beta \in P \implies \alpha \in P$  or  $\beta \in P$ . Equivalently,  $\mathfrak{o}_K/P$  is an integral domain.

### Lemma 7.3. Let $P \subset \mathfrak{o}_K$ be a prime ideal.

1. Either  $P = \{0\}$  or  $P$  is a maximal ideal.
2. If  $P \neq \{0\}$  then  $P \cap \mathbb{Z} = p\mathbb{Z}$  for some prime  $p$ , and  $N(p) = p^f$  is a power of  $p$  for some  $1 \leq f \leq n$ .

*Proof.*



1. If  $P \neq \{0\}$  then as  $P$  has finite index,  $\mathfrak{o}_K/P$  is a finite integral domain, so a field, and hence  $P$  is a maximal ideal.
2. By 7.2(1.), if  $P \neq 0$  then  $P \cap \mathbb{Z}$  is nonempty, so contains some  $m \geq 1$ . As  $P$  is prime, some prime factor  $p$  of  $m$  belongs to  $P$ . Therefore  $\mathbb{Z} \supset P \cap \mathbb{Z} \supset p\mathbb{Z}$ . As  $P \cap \mathbb{Z}$  is an ideal of  $\mathbb{Z}$ , and  $P \neq \mathfrak{o}_K$ ,  $P \cap \mathbb{Z} = p\mathbb{Z}$ , then  $(p) \subset P \subsetneq \mathfrak{o}_K$ , so  $(\mathfrak{o}_K : P)$  divides  $(\mathfrak{o}_K : (p)) = p^n$ .

□

From now on, when we refer to a prime ideal, we will mean a non zero prime ideal. We will also use the following conventions on arithmetic of ideals:

$$I + J = \{\alpha + \beta : \alpha \in I, \beta \in J\}$$

$$IJ = \{\text{finite sums } \sum \alpha_i \beta_j : \alpha_i \in I, \beta_j \in J\}$$

Every ideal of  $\mathfrak{o}_K$  is finitely generated as an ideal, and so we say that  $\mathfrak{o}_K$  is **Noetherian**. If  $\alpha_1, \dots, \alpha_k \in \mathfrak{o}_K$ , we write  $(\alpha_1, \dots, \alpha_k)$  for the ideal they generate. So if  $\alpha \in \mathfrak{o}_K$ ,  $(\alpha)$  is the principal ideal  $\alpha\mathfrak{o}_K$ . Other texts will use angle brackets or square brackets for this notation.

Then we see that  $(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_m) = (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ , and  $(\alpha_1, \dots, \alpha_n)(\beta_1, \dots, \beta_m) = (\alpha_1\beta_1, \dots, \alpha_1\beta_m, \alpha_2\beta_1, \dots, \alpha_n\beta_m)$ .

## 8 Ideals II: Unique Factorisation Boogaloo

As an example, take  $K = \mathbb{Q}(\sqrt{-5})$ . We saw before that  $\mathfrak{o}_K = \mathbb{Z}[\sqrt{-5}]$  is not a UFD, and so not a PID either, as  $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ .

These are both distinct factorisations into irreducibles, which can be checked using the norm.  $N_{K/\mathbb{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2$ .  $N_{K/\mathbb{Q}}(2) = 4$ , so if  $2 = \alpha\beta$  for  $\alpha, \beta$  not units, then by multiplicativity of norm,  $N_{K/\mathbb{Q}}(\alpha) = \pm 2 = x^2 + 5y^2$ , which has no solutions in the integers.

Some ideal computations:

$$(2, 1 + \sqrt{-5})^2 = (4, 2(1 + \sqrt{-5}), (1 + \sqrt{-5})^2) = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) = (2)$$

$$(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (3)$$

$$(2, 1 + \sqrt{-5})(3, 1 \pm \sqrt{-5}) = (1 \pm \sqrt{-5})$$

$$\text{And so: } (6) = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

As an exercise, check that  $N(2, 1 + \sqrt{-5}) = 2$ ,  $N(3, 1 \pm \sqrt{-5}) = 3$ , so these ideals are all maximal, since they have prime norm, and hence are prime. One can check that this is the only factorisation of  $(6)$  as a product of prime ideals.

**Lemma 8.1.** *If  $I \subset \mathfrak{o}_K$  is a non-zero ideal, with  $\alpha \in K$  s.t.  $\alpha I \subset I$ , then  $\alpha \in \mathfrak{o}_K$ .*

*Proof.*  $\alpha I \subset I \implies \alpha^k I \subset I$  for all  $k \geq 0$ . Let  $0 \neq \beta \in I$ . Then  $\mathbb{Z}[\alpha]\beta \subset I$ , and so  $\mathbb{Z}[\alpha]\beta$  is a finitely generated  $\mathbb{Z}$ -module, since  $I$  is, so  $\mathbb{Z}[\alpha]$  is finitely generated, and hence  $\alpha \in \mathfrak{o}_K$ . □

Note that this proof relies on the fact that  $\mathfrak{o}_K$  is all the algebraic integers. It fails if you replace  $\mathfrak{o}_K$  by a subring. We will next seek to prove that every  $I = \prod P_i^{a_i}$  where  $P_i$  are prime ideals is a unique representation, i.e. we have unique factorisation into prime ideals.

**Lemma 8.2.**

1. Let  $I \neq \{0\}$  be an ideal. Then there are prime ideals  $P_1, \dots, P_r$  not necessarily such that  $I \supseteq P_1 P_2 \dots P_r$ .
2. Let  $P, P_1, \dots, P_r$  be prime ideals with  $P \supseteq P_1 \dots P_r$ . Then  $P = P_i$  for some  $i$ .

*Proof.*

1. We do this by induction on  $N(I)$ . If  $I = \mathfrak{o}_K$  or  $I = P$  is prime, then there is nothing to prove. Otherwise, there exists  $\alpha, \beta \in \mathfrak{o}_K \setminus I$  with  $\alpha\beta \notin I$ . Then  $I + (\alpha) \supsetneq I, I + (\beta) \supsetneq I$ . By induction,  $I + (\alpha) \supset P_1 \dots P_r, I + (\beta) \supset Q_1 \dots Q_s$  for  $P_i, Q_i$  prime ideals. Then  $P_1 \dots P_r Q_1 \dots Q_s \subset (I + (\alpha))(I + (\beta)) = I^2 + \alpha I + \beta I + (\alpha\beta) \subseteq I$ .
2. Suppose  $P \neq P_1$  and let  $\alpha \in P_1 \setminus P$ , since prime ideals are maximal  $P \not\subseteq P_1, P_1 \not\subseteq P$ . Then for all  $\beta \in P_2 \dots P_r, \alpha\beta \in P_1 \dots P_r \subset P$ , so, as  $P$  prime,  $\beta \in P$ . So  $P_2 \dots P_r \subset P$ , and repeat until one of the  $P_i$  is equal to  $P$ .

□

**Corollary 8.3.** Let  $I \subset \mathfrak{o}_K$  be a nonzero proper ideal,  $0 \neq \alpha \in I$ . Then there exists  $\beta \in \mathfrak{o}_K \setminus (\alpha)$  such that  $\beta I \subset (\alpha)$ .

*Proof.* Let  $P$  be a prime ideal containing  $I$ . It is enough to find  $\beta \in \mathfrak{o}_K \setminus (\alpha)$  with  $\beta P \subset (\alpha)$ . By 8.2, there are prime ideals  $P_1, \dots, P_r$  with  $(\alpha) \supset P_1 \dots P_r$ . Choose such a collection of primes with  $r$  minimal. Then  $P \supset (\alpha)$ , without loss of generality we may take  $P = P_1$ . Then  $(\alpha) \not\supseteq P_2 \dots P_r$ , so let  $\beta \in P_2 \dots P_r \setminus (\alpha)$ . Then  $\beta I \subset P P_2 \dots P_r = P_1 P_2 \dots P_r \subset (\alpha)$  as required. □

**Theorem 8.4** (“Ideals are invertible”). Let  $I \subset \mathfrak{o}_K$  be a nonzero ideal. Then there exists a nonzero ideal  $J$  such that  $IJ$  is principal.

*Proof.* If  $I = \mathfrak{o}_K$  then  $J = \mathfrak{o}_K$  will do. So assume  $I \subsetneq \mathfrak{o}_K$  and that the result holds for every  $I' \supsetneq I$ . Pick  $0 \neq \alpha \in I$ , and choose  $\beta$  as in 8.3. Then  $\alpha^{-1}\beta \notin \mathfrak{o}_K$  and  $\alpha^{-1}\beta I \subset \mathfrak{o}_K$ . So by 8.1,  $\alpha^{-1}\beta I \not\subseteq I$ , and so  $I \subsetneq I' := I + \alpha^{-1}\beta I$ . So by induction, there is a nonzero ideal  $J'$  with  $I'J' = (\gamma)$ . Let  $J = \alpha J' + \beta J' = (\alpha, \beta)J'$ . Then  $IJ = (\alpha, \beta)IJ' = \alpha I'J' = (\alpha\gamma)$  is principal. □

The key point in this proof which is obscured is that if  $I = P \ni \alpha$  and  $\beta$  are as in 8.3, then  $(\alpha\beta)P = (\alpha)$ .

Now we come to the main theorem of this section:

**Theorem 8.5.** Let  $I, J, I'$  be nonzero ideals of  $\mathfrak{o}_K$ . Then

1. If  $IJ = I'J$  then  $I = I'$  (Cancellation)
2.  $I \supset J$  if and only if there is an ideal  $H$  with  $IH = J$  (To divide is to contain)
3. There are unique distinct prime ideals  $P_1, \dots, P_r$  and integers  $a_i \geq 1$  such that  $I = P_1^{a_1} \dots P_r^{a_r}$ . (Unique prime factorisation)

*Proof.*

1. By 8.4, there is  $J'$  with  $JJ' = (\alpha)$  principal. Then  $\alpha I = IJJ' = I'JJ' = \alpha I' \implies I = I'$ .

2. The “if” direction is clear. Suppose that  $I \supset J$ , and let  $II' = (\alpha)$  as in 8.4. Then  $JII' \subset (\alpha)$ , and so  $H := \alpha^{-1}JII' \subset \mathfrak{o}_K$  is an ideal, and  $IH = \alpha^{-1}JII' = J$ .
3. Existence we do by induction in  $N(I)$ . If  $I \neq \mathfrak{o}_K$ , let  $P$  be prime,  $P \supset I$ . Then by part 2,  $I = PJ$  for some ideal  $J$ , and by part 1,  $I \neq J$ . But  $J \supseteq I$ , and so by induction,  $J$  is a product of prime ideals, and hence so is  $I$ .

For uniqueness, suppose  $I = P_1 \dots P_K = Q_1 \dots Q_\ell$ . If  $k = 0$ ,  $I = \mathfrak{o}_K$ , so  $\ell = 0$  so done. Otherwise, as  $I \subset P_1$ , we have  $P_1 = Q_j$  for some  $j$  by 8.1. Reordering,  $P_1 = Q_1$ , and so  $P_2 \dots P_K = Q_2 \dots Q_\ell$ , and finish by induction

□

We say two ideals  $I, J$  are **equivalent** if there are nonzero  $\alpha, \beta \in \mathfrak{o}_K$  such that  $\alpha I = \beta J$ . It is trivial to check that this is an equivalence relation.

**Theorem 8.6.** *The set of equivalence classes of ideals is an abelian group under multiplication, the ideal class group  $Cl(K)$  of  $K$ . The identity element is the class of principal ideals.*

*Proof.* All axioms are trivial to check apart from existence of inverses, but this follows from 8.4 □

Alternatively, we can define a **fractional ideal** to be a subset of  $K$  of the form  $\alpha I$ , for  $I \subseteq \mathfrak{o}_K$  some nonzero ideal, and  $0 \neq \alpha \in K$ . We can then multiply fractional ideals in the same way as ideals, and define a **principal fractional ideal** to be any  $\alpha \mathfrak{o}_K$  for  $\alpha$  nonzero.

**Theorem 8.7.** *The set of fractional ideals of  $K$  is an abelian group under multiplication, and is freely generated by the prime ideals of  $\mathfrak{o}_K$ . The principal fractional ideals form a normal subgroup, and the quotient is the class group  $Cl(K)$ .*

Remark: if  $I \subseteq \mathfrak{o}_K$  is a nonzero ideal, then its inverse in the group of fractional ideals is  $\alpha^{-1}J$ , where  $IJ = (\alpha)$ .

**Proposition 8.8.** *The following are equivalent:*

1.  $\mathfrak{o}_K$  is a principal ideal domain.
2.  $\mathfrak{o}_K$  is a unique factorisation domain.
3.  $Cl(K) = \{1\}$  is trivial.

*Proof.* 1. and 3. are equivalent by definition:  $Cl(K) = \{1\}$  if and only if every ideal is equivalent to  $\mathfrak{o}_K$ , i.e. if every ideal is principal. Moreover, we know from GRM that every principal ideal domain is a unique factorisation domain, so  $1. \implies 2.$ , so the only part to prove is that  $2. \implies 1.$

It is enough to show that, if  $P$  is prime, then  $P$  is principal. Let  $\alpha \in P \setminus \{0\}$ , and factor  $\alpha = \prod \pi_i$ , where  $\pi_i$  are irreducible. As  $P$  is prime, some  $\pi_i \in P$  - WLOG take it to be  $\pi_1$ . Then since  $\pi_1$  is an irreducible in a UFD,  $(\pi_1)$  is a prime ideal and hence maximal, so from  $(\pi_1) \subseteq P \subseteq \mathfrak{o}_K$  we must have  $P = (\pi_1)$  or  $\mathfrak{o}_K$ , both principal. □

**Theorem 8.9.** *Let  $I, J \subseteq \mathfrak{o}_K$  be nonzero ideals. Then  $N(IJ) = N(I)N(J)$ .*

*Proof.* It is sufficient to prove, by unique factorisation into primes, that if  $P$  is prime, then  $N(IP) = N(I)N(P)$ . Obviously,  $N(IP) = (\mathfrak{o}_K : I)(I : IP)$ , so STP that  $(I : IP) = N(P)$ .

By cancellation,  $I \neq IP$ . We claim that, if  $IP \subset J \subset I$ , then  $J = I$  or  $J = IP$ . Indeed, as  $J \subset I$ ,  $J = IJ'$  for some  $J'$ , so  $P \subset J' \subset \mathfrak{o}_K$  by cancellation, and so  $J' = P$  or  $\mathfrak{o}_K$ .

Let  $\alpha \in I \setminus IP$ . Then  $IP + (\alpha) = I$  by the claim. Consider the  $(\mathfrak{o}_K/\mathfrak{o}_K/P)$ -module homomorphism given by  $\tilde{\alpha} : \mathfrak{o}_K/P \rightarrow I/IP$ ;  $\tilde{\alpha}(\beta + P) = \alpha\beta + IP$ . It is surjective, since  $\mathfrak{Im}(\tilde{\alpha}) = ((\alpha) + IP)/IP = I/IP$ . Also,  $\tilde{\alpha}$  is a homomorphism of  $(\mathfrak{o}_K/P)$ -vector spaces.

$\dim_{\mathfrak{o}_K/P}(\mathfrak{o}_K/P) = 1$ ; as  $I \neq IP$ ,  $\dim_{\mathfrak{o}_K/P}(I/IP) \geq 1$ . As it is surjective, we must have  $\dim(I/IP) = 1$ , and so  $\mathfrak{o}_K/P \cong I/IP$ , and so  $N(P) = (I : IP)$  as required.  $\square$

This fails for  $R = \mathbb{Z}[2\sqrt{2}]$  and prime ideal  $P = (2, 2\sqrt{2})$ , since  $N(P) = 2$ , whereas  $P^2 = (4, 4\sqrt{2})$ , so  $N(P^2) = 8 \neq 2 \cdot 2$ .

## 9 Factorisation of Rational Primes

If  $I \subset \mathfrak{o}_K$ , then  $I \ni n = \prod p^{a(p)}$  for some  $n \geq 1$  (e.g.  $n = N(I)$ ). So if we first factor  $(p)$ , we can figure out how to factor  $I \supset \prod (p)^{a(p)}$

**Theorem 9.1.** *Let  $p$  be a rational prime and  $\{P_i : 1 \leq i \leq r\}$  the prime ideals containing  $p$ . Let  $N(P_i) = p^{f_i}$ , for  $f_i \geq 1$ . Then  $(p) = P_1^{e_1} \dots P_r^{e_r}$  for integers  $e_i \geq 1$  satisfying  $\sum_i e_i f_i = n$ .*

*Proof.* The factorisation exists for some  $e_i \geq 1$  by 8.5. Now  $\prod N(P_i)^{e_i} = N((p)) = |N_{K/\mathbb{Q}}((p))| = p^n$ , and so  $\sum e_i f_i = n$ .  $\square$

$f_i$  is called the **residue class degree** of  $P_i$ , and  $e_i$  is called the **ramification index/degree** of  $P_i$ . We say that  $p$  is **ramified** in  $K$  if some  $e_i > 1$ , and is **totally ramified** if  $e_1 = n$ , so  $r = 1 = f_1$ .  $p$  is **inert** if  $(p)$  is prime so  $(r = 1 = e_1, f_1 = n)$ , and **splits completely** if  $r = n$  and so  $(e_i = f_i = 1 \text{ for all } i)$ .

We will show soon that only finitely many primes  $p$  can be ramified, but for now let's think about how to compute the decomposition  $(p) = \prod P_i^{e_i}$ . The following often works:

**Theorem 9.2** (Dedekind's Criterion). *Let  $K = \mathbb{Q}(\theta)$ ,  $\theta \in \mathfrak{o}_K$ , the minimal polynomial  $g = m_\theta \in \mathbb{Z}[x]$ , and let  $p$  be prime such that  $p \nmid (\mathfrak{o}_K : \mathbb{Z}[\theta])$ . Let the reduction  $\bar{g} \in \mathbb{F}_p[x]$  factor as  $\bar{g} = \prod_{i=1}^r \bar{g}_i^{e_i}$ ,  $\bar{g}_i \in \mathbb{F}_p[x]$  distinct irreducibles, and  $e_i \geq 1$ .*

*Let  $g_i \in \mathbb{Z}[x]$  be monic, whose reduction mod  $p$  is  $\bar{g}_i$ . Then  $(p) = \prod_{i=1}^r P_i^{e_i}$ , where  $P_i = (p, g_i(\theta))$  are distinct prime ideals. Moreover,  $N(P_i) = p^{f_i}$ , where  $f_i = \deg g_i$ .*

*Proof.* We will often use the 3<sup>rd</sup> isomorphism theorem: if  $J \subset I \subset R$ , then  $R/I \cong (R/J)/(I/J)$ .

First assume  $\mathfrak{o}_K = \mathbb{Z}[\theta]$ .

Step 1: Since  $\bar{g}_i \in \mathbb{F}_p[x]$  is irreducible,  $\mathfrak{o}_K/P_i = \mathbb{Z}[\theta]/(p, g_i(\theta)) \cong \mathbb{Z}[x]/(g, p, g_i) \cong \mathbb{F}_p[x]/(\bar{g}, \bar{g}_i) = \mathbb{F}_p[x]/(\bar{g}_i)$ , is a finite field with  $p^{f_i}$  elements. So  $P_i$  is prime of norm  $p^{f_i}$ .

Step 2:  $g = \prod g_i^{e_i} + ph$ ,  $h \in \mathbb{Z}[x]$ , and so:

$$\prod P_i^{e_i} = \prod (p, g_i(\theta))^{e_i} \subset \prod (p, g_i(\theta)^{e_i}) \subset (p, \prod g_i(\theta)^{e_i}) = (p, ph(\theta)) = (p)$$

since  $g(\theta) = 0$ . But then comparing norms, we have  $N(\prod P_i^{e_i}) = p^{\sum e_i f_i}$ ;  $N((p)) = p^n$ , where  $n = \deg \bar{g} = \sum e_i \deg \bar{g}_i = \sum e_i f_i$ . So we have equality  $\prod P_i^{e_i} = (p)$ .

In general then, it is enough to show that  $\phi : \mathbb{Z}[\theta]/Q_i \rightarrow \mathfrak{o}_K/P_i; \alpha + Q_i \mapsto \alpha + P_i$ , where  $Q_i = (p, g_i(\theta))$ , is an isomorphism. As  $\mathbb{Z}[\theta]/Q_i$  is a field,  $\phi$  is injective since the kernel is an ideal and is not the whole ring, so must be trivial. Its image is a subgroup of  $\mathfrak{o}_K/P_i$  whose index divides  $\#\mathfrak{o}_K/P_i$ , and so is a power of  $p$  since  $p \in P_i$ , and also divides  $(\mathfrak{o}_K : \mathbb{Z}[\theta])$ , which is coprime to  $p$ . Hence its index is 1, the map is surjective, and hence is an isomorphism. Then step 2 finishes the proof.  $\square$

For example, take  $K = \mathbb{Q}(\sqrt{d})$  for  $d \neq 0, 1$  a squarefree integer. Recall that:

$$\mathfrak{o}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \pmod{4} \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod{4} \end{cases}$$

In the second case,  $(\mathfrak{o}_K : \mathbb{Z}[\sqrt{d}]) = 2$ .

Then let  $\theta = \sqrt{d}$ ,  $g(x) = x^2 - d$ . For  $p$  prime,  $g$  factors mod  $p$  as:

$$\bar{g} = \begin{cases} (x - \bar{a})(x + \bar{a}) & p \neq 2, \left(\frac{d}{p}\right) = 1, a^2 \equiv d \pmod{p} \\ \text{irreducible} & p \neq 2, \left(\frac{d}{p}\right) = -1 \\ (x - \bar{d})^2 & p = 2 \text{ or } p|d \end{cases}$$

Then by Dedekind's criterion, if  $p \neq 2$ , then:

- (Inert) If  $\left(\frac{d}{p}\right) = -1$ , then  $(p)$  is prime, of norm  $p^2$
- (Split) If  $\left(\frac{d}{p}\right) = 1$ , then  $d \equiv a^2 \pmod{p}$ , and then  $(p) = PP'$  where  $P = (p, a + \sqrt{d})$ ,  $P' = (p, a - \sqrt{d}) \neq P$ , both of norm  $p$ .
- (Ramified) If  $p|d$ , then  $(p) = P^2$ ,  $P = (p, \sqrt{d})$ , of norm  $p$ .

In the case where  $d \not\equiv 1 \pmod{4}$ ,  $(2) = (d, d - \sqrt{d})^2 = P^2$ , of norm 2.

The final case is  $p = 2, d \equiv 1 \pmod{4}$ . In this case, take  $\theta = \frac{1+\sqrt{d}}{2}$ , so  $\mathfrak{o}_K = \mathbb{Z}[\theta]$ . Then  $g = m_\theta = x^2 - x - \frac{d-1}{4}$ , and:

- (2 splits) If  $d \equiv 1 \pmod{8}$ , then  $\bar{g} = x(x-1)$ , hence  $(2) = PP'$ , where  $P = (2, \theta) = (2, \frac{1+\sqrt{d}}{2})$ ,  $P' = (2, \theta - 1) = (2, \frac{1-\sqrt{d}}{2}) \neq P$  of norm 2.
- (2 inert) If  $d \equiv 5 \pmod{8}$ , then  $\bar{g} \equiv x^2 + x + 1 \pmod{2}$  is irreducible mod 2, so  $(2)$  is prime.

Suppose that  $\mathfrak{o}_K = \mathbb{Z}[\theta]$ , and  $(p) = P_1 \dots P_n$  splits completely. Then by Dedekind,  $m_\theta$  has  $n$  distinct roots mod  $p$ . So  $p \geq n$ . In other words, if  $p < n$  and  $p$  splits completely, then  $\mathfrak{o}_K \neq \mathbb{Z}[\theta]$  - even more, there does not exist  $\theta$  with  $p \nmid (\mathfrak{o}_K : \mathbb{Z}[\theta])$ . It is not hard to find examples of this - see the second examples sheet.

Recall that  $p$  **ramifies** if  $(p) = P_1^{e_1} \dots P_r^{e_r}$ , and there is some  $e_i > 1$ .

**Theorem 9.3.** *If  $p$  ramifies in  $K$ , then  $p|d_K$ . In particular, only finitely many primes ramify in  $K$ .*

The converse is also true, and uses some more Galois theory. To prove it, we will need the following lemma:

**Lemma 9.4.** *If  $\alpha \in \mathfrak{o}_K$ , then  $\text{Tr}_{K/\mathbb{Q}}(\alpha P) \equiv \text{Tr}_{K/\mathbb{Q}}(\alpha) \pmod{p}$ , for  $p$  prime.*

*Proof.* By Fermat's little theorem,  $\text{Tr}_{K/\mathbb{Q}}(\alpha) \equiv \text{Tr}_{K/\mathbb{Q}}(\alpha)^p \pmod{p}$ . But:

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(\alpha)^p - \text{Tr}_{K/\mathbb{Q}}(\alpha^p) &= \left( \sum_{i=1}^n \sigma_i(\alpha) \right)^p - \sum_{i=1}^n (\sigma_i(\alpha)^p) \\ &= \sum_{\substack{0 \leq k_i \leq p \\ \sum k_i = p}} \frac{p^i}{k_1! \dots k_n!} \sigma_1(\alpha)^{k_1} \dots \sigma_n(\alpha)^{k_n} \end{aligned}$$

and each coefficient is 0 mod  $p$ . □

*Proof of Theorem 9.3.* Assume  $e_1 > 1$ . Let  $\alpha \in P_1^{e_1-1} P_2^{e_2} \dots P_r^{e_r} \setminus (p)$ . Then for any  $\beta \in \mathfrak{o}_K$ ,  $(\alpha\beta)^p \in P_1^{p(e_1-1)} P_2^{pe_2} \dots P_n^{pe_n}$ , i.e.  $(\alpha\beta)^p \in (p)$ .

So, by the lemma,  $\text{Tr}_{K/\mathbb{Q}}(\alpha\beta) \equiv 0 \pmod{p}$ .

Let  $(\theta_i)$  be an integral basis for  $K$ . Write  $\alpha = \sum_{i=1}^n b_i \theta_i$  for  $b_i \in \mathbb{Z}$ . Then  $\sum_{i=1}^n b_i \text{Tr}_{K/\mathbb{Q}}(\theta_i \theta_j) = \text{Tr}_{K/\mathbb{Q}}(\alpha \theta_j) \equiv 0 \pmod{p}$

As  $\alpha \notin (p)$ , not all  $b_i \equiv 0 \pmod{p}$ , and so the rows of the matrix  $(\text{Tr}_{K/\mathbb{Q}}(\theta_i \theta_j))$  are linearly dependent mod  $p$ . Then  $d_K = \det(\text{Tr}_{K/\mathbb{Q}}(\theta_i \theta_j)) \equiv 0 \pmod{p}$ , and so  $p | d_K$ . □

Note - with a bit more care, we can get  $\prod p^{(e_i-1)f_i} | d_K$ , which is a useful result for computing  $\mathfrak{o}_K$ .

For example, take  $K = \mathbb{Q}(\sqrt[3]{p})$ , where  $p \neq 3$  is a prime. Then  $\mathfrak{o}_K \supset \mathbb{Z}[\sqrt[3]{p}]$ , and  $(p) = (\sqrt[3]{p})^3$ . So  $p$  ramifies. Then:

$$\begin{aligned} \text{Disc}(\mathbb{Z}[\sqrt[3]{p}]) &= \det \text{Tr}_{K/\mathbb{Q}} \begin{pmatrix} 1 & p^{1/3} & p^{2/3} \\ p^{1/3} & p^{2/3} & p \\ p^{2/3} & p & p^{4/3} \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3p \\ 0 & 3p & 0 \end{pmatrix} \\ &= -27p^2 \end{aligned}$$

Then  $p$  ramifies, and so  $p | d_K$ ,