Number Fields

March 3, 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 α. The ***degree*** of α is the degree of m_α

Proposition 1.1. *Suppose $\alpha \in F$ is algebraic. Then m_α 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_α □

If $\alpha \in F$, define $\mathbb{Q}(\alpha)$ to be the smallest subfield of F containing α. 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 α is algebraic of degree n.*

Proof. Consider the homomorphism $\phi : \mathbb{Q}[x] \to F; f \mapsto f(\alpha)$. Then $\ker(\phi) = (m_\alpha)$ which is maximal, so $\operatorname{im}\phi$ 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 α is algebraic of some degree. By the first part, this degree is n. □

Proposition 1.3. *$\{\alpha \in F : \alpha$ 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 α^{-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) α is an algebraic integer*
   - *(b) α is algebraic and $m_\alpha \in \mathbb{Z}[x]$*
   - *(c) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module*

   If these hold, then $1, \alpha, \ldots, \alpha^{d-1}$ 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 $\alpha_1, \ldots, \alpha_n \in F$, then $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ 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 $A\alpha_1^{i_1} \ldots \alpha_n^{i_n}$ for $A, i_1, \ldots, i_n \in \mathbb{Z}$.

Proof.

1. $\underline{a. \implies b.}$ 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_α, g are in $\mathbb{Z}[x]$.

   $\underline{b. \implies c.}$ 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 α^n is a $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{d-1}$. So $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{d-1}$ as a $\mathbb{Z}$-module. There is no linear relation between $1, \alpha, \ldots, \alpha^{d-1}$, as $d = \deg \alpha$. So $\mathbb{Z}[\alpha]$ is finitely generated and $1, \alpha, \ldots, \alpha^{d-1}$ is a $\mathbb{Z}$-basis.

   $\underline{c. \implies a.}$ Assume $\mathbb{Z}[\alpha]$ is finitely generated by $g_1(\alpha), \ldots, g_r(\alpha)$. For some $g_i \in \mathbb{Z}[x]$. Let $k = \max\{\deg g_i\}$. Then $\mathbb{Z}[\alpha]$ is certainly generated by $1, \alpha, \ldots, \alpha^k$ 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 α is an algebraic integer.

2. $\alpha \in \mathbb{Q} \implies m_\alpha = x - \alpha$, and so α 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_α 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 $z^2 d$ 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 $dk^2 \equiv 1 \mod 4$. If $d \equiv 1 \mod 4$, this holds if and only if k is odd, and if d is not $1 \mod 4$, 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 $d \not\equiv 1 \mod 4$, then $\mathfrak{o}_K = \{u + v\sqrt{d} : u, v \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}]$.*
2. *If $d \equiv 1 \mod 4$, 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 $\phi : \mathbb{Q}[x] \to \mathbb{C}$ 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 θ has degree $[K:F]$ over F. □

Remarks:

1. If $K \subset \mathbb{C}$ we can choose σ to be the inclusion.
2. For some $r \in \{0, \ldots, n\}$, exactly r of the σ_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.

[1] 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 $\sigma_1 : \sqrt{d} \to \mathrm{i}\sqrt{|d|}; \sigma_2 : \sqrt{d} \to -\mathrm{i}\sqrt{|d|}$. 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_α, each taken $n/\deg(\alpha)$ times.*

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

4 Norm and Trace

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

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

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 $f_\alpha = \det(x \cdot I_n - A), \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \det(A), \mathrm{Tr}_{K/\mathbb{Q}} = \mathrm{tr}(A)$. As an exercise, work these out for $\mathbb{Q}(\sqrt{d})$.

Proposition 4.1.

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha\beta) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\,\mathrm{N}_{K/\mathbb{Q}}(\beta)$$
$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha + \beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$$

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_α is m_α, and $f_\alpha \prod_{i=1}^n (x - \sigma_i(\alpha)) = m_\alpha^{n/d}$, where $\deg(\alpha) = d$.*
2. *$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$.*

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

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

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 $f_\alpha =$ (char. poly. of u_α on $\mathbb{Q}(\alpha))^{n/d} = m_\alpha^{n/d} = \prod_{i=1}^n (x - \sigma_i(\alpha))$. □

Corollary 4.3.

1. *Let $\alpha \in K$. Then $\alpha = 0 \iff \mathrm{N}_{K/\mathbb{Q}}(\alpha) = 0$.*
2. *Let $\alpha \in \mathfrak{o}_K$. Then $f_\alpha \in \mathbb{Z}[x]$, and $\mathrm{N}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Moreover, $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \{\pm 1\}$ 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 $\mathrm{N}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, since they are coefficients of f_α up to a choice of sign.

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

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

□

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

$$\mathrm{Tr}_{K/\mathbb{Q}} = \mathrm{Tr}_{F/\mathbb{Q}} \cdot \mathrm{Tr}_{K/F} \qquad \mathrm{N}_{K/\mathbb{Q}} = \mathrm{N}_{F/\mathbb{Q}} \cdot \mathrm{N}_{K/F}$$

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 $x_1, \ldots, x_n$. Let $H \subset G$ be the subgroup generated by $y_1, \ldots, y_n \in G$, where $y_i = \sum_{j=1}^n A_{ji} x_j$ for some $A \in Mat_{n,n}(\mathbb{Z})$ 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 $D = diag(d_1, \ldots, d_n)$ for $d_i \geq 0$, $d_i | d_{i+1}$. Then $G/H \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$, 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 $\prod_i d_i = |\det A|$. □

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:

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

Proposition 5.2. *If H is finitely generated as an abelian group then $H = \bigoplus_{i=1}^r \mathbb{Z}v_i$ where $r = \mathrm{rank}(H)$ and $x_1, \ldots, x_r \in V$ 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 $x_1, \ldots, x_r$. 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 $r = \operatorname{rank}(H)$ by the definition of rank. □

6 Discriminants and Integral Bases

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

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

Theorem 6.1.

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

Proof.

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

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

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

   For the other direction, suppose (α_i) is a $\mathbb{Q}$-basis for K, and let $T = (\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{ij}$. 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 $c^\intercal Tb \neq 0$. But if $\beta = \sum_j jb_j\alpha_j, \gamma = \sum_j c_j\alpha_j$, then $c^\intercal Tb = \sum_{i,j} c_i \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)b_j = \operatorname{Tr}_{K/\mathbb{Q}}(\sum_{i,j} c_i b_j \alpha_i\alpha_j) = \operatorname{Tr}_{K/\mathbb{Q}}(\beta\gamma)$, so taking $\gamma = \frac{1}{\beta}$, we get $\operatorname{Tr}_{K/\mathbb{Q}}(1) = n \neq 0$.

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, $\operatorname{Disc}(\beta_i) = (\det A)^2 \operatorname{Disc}(\alpha_i) = \operatorname{Disc}(\alpha_i)$.

□

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

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

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

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

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

□

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

Proof. Certainly, there is $\omega_1, \ldots, \omega_n \in \mathfrak{o}_K$ 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, $\operatorname{Disc}(H) \in \mathbb{Z} \setminus \{0\}$ where $H = \sum_i \mathbb{Z}\omega_i \subset K$.

Choose such a basis with $|\operatorname{Disc}(H)|$ 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**, $\operatorname{Disc}(H) = (H' : H)^2 \operatorname{Disc}(H')$, and by minimality of $\operatorname{Disc}(H), H' = H$, so $\alpha \in H$. □

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

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

$d \not\equiv 1 \mod 4$: 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 $d_K = (\det \Delta)^2 = 4d$.

$d \equiv 1 \mod 4$: 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 θ. Then:*

$$\operatorname{Disc}(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\sigma_i(\theta) - \sigma_j(\theta))^2 = (-1)^{n(n-1)/2} \operatorname{N}_{K/\mathbb{Q}}(f'(\theta))$$

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

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

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

Proposition 6.5. *Let $\omega_1, \ldots, \omega_n \in \mathfrak{o}_K$ with $\operatorname{Disc}(\omega_i)$ squarefree. Then (ω_i) is an integral basis.*[2]

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

[2] The converse is false, e.g. for $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1 \mod 4$ 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 $(\mathfrak{o}_K : I)^2 = \frac{Disc(I)}{d_K}$*

2. *If $0 \neq \alpha \in \mathfrak{o}_K$, then $(\mathfrak{o}_K : \alpha\mathfrak{o}_K) = |\operatorname{N}_{K/\mathbb{Q}}(\alpha)|$.*

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

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 $\operatorname{Disc}(I) = \operatorname{Disc}(\alpha\omega_i) = (\det \sigma_i(\alpha\omega_j))^2 = (\det \sigma_i(\alpha)\sigma_i(\omega_j))^2 = \operatorname{N}_{K/\mathbb{Q}}(\alpha)^2 d_K$.

   And so by (1.), $(\mathfrak{o}_k : \alpha\mathfrak{o}_k)^2 = (\operatorname{N}_{K/\mathbb{Q}}(\alpha))^2$.

□

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, $\operatorname{N}(I)x = 0$ by Lagrange, and so $\operatorname{N}(I) \in I$.

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 σ_K containing $M\sigma_K$" and "ideals of $\mathfrak{o}_K/M\mathfrak{o}_K$" by isomorphism theorems. his 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 $\operatorname{N}(p) = p^f$ 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 $\alpha_1, \ldots, \alpha_k \in \mathfrak{o}_K$, we write $(\alpha_1, \ldots, \alpha_k)$ for the ideal they generate. So if $\alpha \in \mathfrak{o}_K$, (α) is the principal ideal $\alpha\mathfrak{o}_K$. Other texts will use angle brackets or square brackets for this notation.

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

8 Ideals II: Unique Factorisation Boogaloo

As an example, take $K = \mathbb{Q}(\sqrt{-5})$. We was 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. $\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2$. $\mathrm{N}_{K/\mathbb{Q}}(2) = 4$, so if if $2 = \alpha\beta$ for α, β not units, then by multiplicativity of norm, $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 2 = x^2 + 5y^2$, which has no solutions in the integers.

Some ideal computations:

$$\begin{aligned} \left(2, 1 + \sqrt{-5}\right)^2 &= \left(4, 2(1 + \sqrt{-5}), (1 + \sqrt{-5})^2\right) = \left(4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}\right) = (2) \\ (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) &= (3) \\ (2, 1 + \sqrt{-5})(3, 1 \pm \sqrt{-5}) &= (1 \pm \sqrt{-5}) \\ \text{And so: } (6) &= (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \end{aligned}$$

As an exercise, check that $\mathrm{N}(2, 1 + \sqrt{-5}) = 2, \mathrm{N}(3, 1 \pm \sqrt{-5}) = 3$, 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 $I \supseteq P_i P_2 \dots P_r$.*
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 $\mathrm{N}(I)$. 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 $P \nsubseteq P_1, P_1 \nsubseteq P$. 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 $P_w \dots P_r \subset P$, 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 β 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**, $\alpha^{-1}\beta I \nsubseteq I$, 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 β 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 $JI' \subset (\alpha)$, and so $H := \alpha^{-1}JI' \subset \mathfrak{o}_K$ is an ideal, and $IH = \alpha^{-1}JII' = J$.

3. Existence we do by induction in $\mathrm{N}(I)$. 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 αI, 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 α 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 π_i are irreducible. As P is prime, some $\pi_i \in P$ - WLOG take it to be π_1. Then since π_1 is an irreducible in a UFD, (π_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* $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.

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

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 ($\mathfrak{o}_K$-module) homomorphism given by $\widetilde{\alpha} : \mathfrak{o}_K/P \to I/IP; \widetilde{\alpha}(\beta+P) = \alpha\beta+IP$. It is surjective, since $\mathfrak{Im}(\widetilde{\alpha}) = ((\alpha)+IP)/IP = I/IP$. Also, $\widetilde{\alpha}$ 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 $\mathrm{N}(P) = (I : IP)$ as required. □

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

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. $n = \mathrm{N}(I)$). 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 $\{P_1 : 1 \leq i \leq r\}$ the prime ideals containing p. Let $\mathrm{N}(P_i) = p^{f_i}$, 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 $\prod \mathrm{N}(P_i)^{e_i} = \mathrm{N}((p)) = |\,\mathrm{N}_{K/\mathbb{Q}}(p)| = p^n$, and so $\sum e_i f_i = n$. □

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 $r = 1 = f_i$. p is ***inert*** if (p) is prime so $(r = 1 = e_1, f_1 = n)$, and ***splits completely*** if $r = n$ and so $(e_i = f_i = 1$ 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$^{\text{rd}}$ 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, $\mathfrak{o}_K/P_i = \mathbb{Z}[\theta]/(p, g_i(\theta)) \cong Z[x]/(g, p, g_i) \cong \mathbb{F}_p[x]/(\bar{g}, \bar{g}_i) = \mathbb{F}_p[x]/(\bar{g}_i)$, 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 $\phi : \mathbb{Z}[\theta]/Q_i \to \mathfrak{o}_K/P_i; \alpha + Q_i \mapsto \alpha + P_i$, where $Q_i = (p, g_i(\theta))$, is an isomorphism. As $\mathbb{Z}[\theta]/Q_i$ is a field, ϕ 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. □

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

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

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:

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

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 $d \equiv a^2 \mod p$, 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 $d \not\equiv 1 \mod 4$, $(2) = (d, d - \sqrt{d})^2 = P^2$, of norm 2.

The final case is $p = 2, d \equiv 1 \mod 4$. 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 $d \equiv 1 \mod 8$, 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 $d \equiv 5 \mod 8$, then $g \equiv x^2 + x + 1 \mod 2$ 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_θ 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 θ 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 $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha P) \equiv \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) \mod p$, for p prime.*

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

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

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, $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha\beta) \equiv 0 \mod p$.

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

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

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

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

10 Geometry of Numbers

The aim of this section is to prove two important theorems:

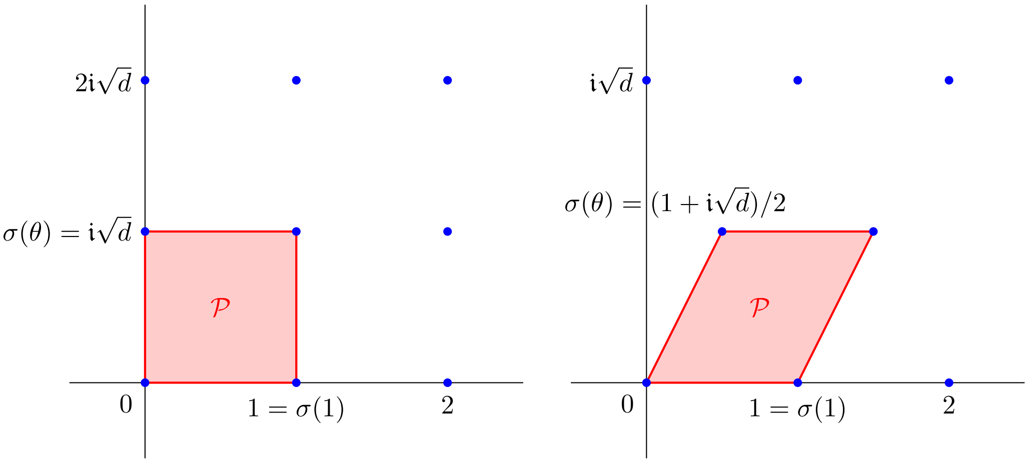
1. If K is a number field then $Cl(K)$ is finite.
2. $\mathfrak{o}_K^*$ is finitely generated of rank $r + s - 1$ where r is the number of real embeddings of K, and s the number of pairs of complex embeddings.

Neither of these theorems can be proved by "pure algebra". The idea is to embed $\mathfrak{o}_K$ as a lattice in $\mathbb{R}^n$. But what is a lattice?

A ***lattice*** in $\mathbb{R}^n$ is a subgroup $\Lambda \subset \mathbb{R}^n$ generated by a basis $\{e_1, \ldots, e_n\}$ of $\mathbb{R}^n$. For instance, $\mathbb{Z}^n \subset \mathbb{R}^n$ is a lattice generated by the standard orthonormal basis.

Take $K = \mathbb{Q}(\sqrt{-d})$ to be an imaginary quadratic field. Then K embeds in $\mathbb{C} \cong \mathbb{R}^2$ via the map $\sqrt{-d} \mapsto \mathrm{i}\sqrt{d}$. Then $\sigma(\mathfrak{o}_K)$ is a lattice in $\mathbb{C}$.

$$\mathfrak{o}_K = \mathbb{Z} \oplus \mathbb{Z}(\theta) = \begin{cases} \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{-d} & d \not\equiv 3 \mod 4 \\ \mathbb{Z} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{-d}}{2} & d \equiv 3 \mod 4 \end{cases}, \text{ and } 1, \sigma(\theta) \text{ are lin. indep. over } \mathbb{R}.$$



(a) $d \not\equiv 3 \mod 4$. $\operatorname{covol} \sigma(\mathfrak{o}_K) = \sqrt{d}$

(b) $d \equiv 3 \mod 4$. $\operatorname{covol} \sigma(\mathfrak{o}_K) = \frac{1}{2}\sqrt{d}$

The ***fundamental parallelepiped*** attached the basis $\{e_i\}$ is $\mathcal{P} = \{\sum_{i=1}^n x_i e_i : 0 \leq x_i < 1\}$. The ***covolume*** of Λ, $\operatorname{covol}(\Lambda)$, is the volume of $\mathcal{P}$, written $\operatorname{vol}(\mathcal{P}) = |\det(e_{ij})|$.

Note that in both cases above, $\operatorname{covol}(\sigma(\mathfrak{o}_K)) = \frac{1}{2}|d_K|^{\frac{1}{2}}$.

Observe that if $x \in \mathbb{R}^n$ then there is a unique $y \in \mathbb{P}$ and $\lambda \in \Lambda$ such that $x = y + \lambda$, i.e. $\mathcal{P}$ is a set of coset representatives for $\Lambda \leq \mathbb{R}^n$

Theorem 10.1 (Special Case of Minkowski's Theorem)**.** *Let $X = \{z \in \mathbb{C} : |z|^2 \leq R\}$, and $\Lambda \subset \mathbb{C}$ be a lattice. If $\pi R \geq 4 \operatorname{covol}(\Lambda)$, then $X \cap \Lambda \neq \{0\}$.*

Theorem 10.2. *Let $I \subset \mathfrak{o}_K \subset K = \mathbb{Q}(\sqrt{-d})$ be a non-zero ideal. Then there is some $\alpha \in I \setminus \{0\}$ with $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \leq c_K \mathrm{N}(I)$, and $c_K = \frac{2}{\pi}|d_K|^{\frac{1}{2}}$.*

Proof. $I \subset \mathfrak{o}_K \hookrightarrow_\sigma \mathbb{C}$ is a lattice, and $\operatorname{covol}(\sigma(I)) = \mathrm{N}(I) \operatorname{covol}(\sigma(\mathfrak{o}_K)) = \mathrm{N}(I)\frac{1}{2}|d_K|^{\frac{1}{2}}$. Take X as in **10.1**, and $R = \frac{2}{\pi}|d_K|^{\frac{1}{2}} \mathrm{N}(I)$.

Then by **10.1**, $X \cap \sigma(I) \neq \{0\}$. But if $\alpha = u + v\sqrt{-d} \in K$, then $\sigma(\alpha) \in K \iff |\sigma(\alpha)|^2 = u^2 + dv^2 \leq R \iff \mathrm{N}_{K/\mathbb{Q}}(\alpha) \leq R$. So there does exist some non-zero α in I with $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \leq R$. □

Corollary 10.3. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic. Then:*

1. *$Cl(K)$ is finite.*
2. *Every element of $Cl(K)$ contains an ideal of norm $\leq c_K = \frac{2}{\pi}|d_K|^{\frac{1}{2}}$.*

3. *$Cl(K)$ is generated by the class of prime ideals of norm $\leq c_K$.*

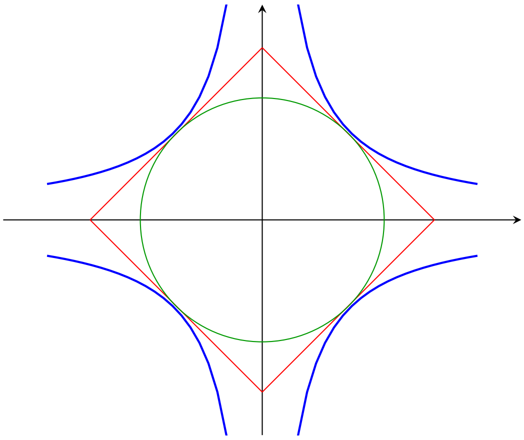
Proof. 2. Let $I \subset \mathfrak{o}_K$ be a non-zero ideal. Choose J with $IJ = (\beta)$. Then by **10.2**, there is some $\alpha \in J \setminus \{0\}$ with $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \leq c_K \, \mathrm{N}(J)$. Then $(\alpha) = JI'$ for some I', and $\mathrm{N}(I') = \frac{\mathrm{N}((\alpha))}{\mathrm{N}(J)} = \frac{\mathrm{N}_{K/\mathbb{Q}}(\alpha)}{\mathrm{N}(J)} \leq c_K$, and $(\alpha\beta) = \alpha IJ = \beta JI'$, so $\alpha I = \beta I'$, i.e. $I' \simeq I$.

Then (2.) $\Longrightarrow$ (3.) by writing $I' = \prod P_i$ as a product of primes of norm $\leq c_K$, and (2.) $\Longrightarrow$ (1.) since the number of ideals of norm $\leq c_K$ is finite by **7.2**. □

Examples:
$K = \mathbb{Q}(\mathfrak{i})$. Then $d_K = 4$, so every ideal class contains an ideal I with norm $\leq c_K = \frac{2}{\pi} 4^{1/2} = \frac{4}{\pi} < 2$, i.e. with norm 1, so $I = \mathfrak{o}_K$. So $Cl(K)$ is trivial, and we have another proof that $\mathbb{Z}[i]$ is a PID.

$K = \mathbb{Q}(\sqrt{-5}$. We've seen already that $\mathfrak{o}_K$ is not a PID. Let's compute $Cl(K)$. We have $d_K = -20$, so $c_K = \frac{2\sqrt{20}}{\pi} < \frac{9}{\pi} < 3$, so every ideal class contains an ideal of norm ≤ 2. Recall that $(2) = (2, 1 + \sqrt{-5})^2 = P^2, \mathrm{N}(P) = 2$. So the only ideals of norm ≤ 2 are $\mathfrak{o}_K$ and P, and hence $Cl(K)$ has order two, with elements $[\mathfrak{o}_K], [P]$.

$K = \mathbb{Q}(\sqrt{d})$. Then we have the two embeddings $\sigma_1, \sigma_2 : \sqrt{d} \mapsto \pm\sqrt{d}$. So the lattice we get is generated by $\sigma(1) = (\sigma_1(1), \sigma_2(1)) = (1,1), \sigma(\sqrt{d}) = (\sqrt{d}, -\sqrt{d})$, which is indeed a basis for $\mathbb{R}^2$, and so $\sigma(\mathbb{Z}[\sqrt{d}])$ is indeed a lattice. Then $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \leq R$ if and only if $\sigma(\alpha)$ lies in the region bounded by $x_1 x_2 = \pm R$.



Theorem 10.4 (Minkowski's Theorem)**.** *Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and $X \subset \mathbb{R}^n$ be a convex, measurable set that is symmetric about 0. Then if either:*

- $\mathrm{vol}(X) > 2^n \, \mathrm{covol}(\Lambda)$
- $\mathrm{vol}(X) \geq 2^n \, \mathrm{covol}(\Lambda)$ *and X is compact*

it must be the case that $X \cap \Lambda \neq \{0\}$.

Note the strict inequality in the first case versus the weak one in the second case. Before we can prove this we will need the following lemma:

Lemma 10.5 (Blichfeldt's Lemma)**.** *Let* $\Lambda \subset \mathbb{R}^n$ *be a lattice and* $Y \subset \mathbb{R}^n$ *be a measurable subset. If* $\mathrm{vol}(Y) > \mathrm{covol}(\Lambda)$ *there is* $x, y \in Y$ *with* $x \neq y$ *such that* $x - y \in \Lambda$*.*

The idea behind this slightly messy proof is that we have a projection map $\pi : \mathbb{R}^n \to \mathbb{R}^n/\Lambda$, where $\mathrm{vol}(\mathbb{R}^n/\Lambda) = \mathrm{covol}(\Lambda) \geq \mathrm{vol}(\pi(Y))$, but $\mathrm{vol}(Y) > \mathrm{covol}(\Lambda)$, and so $Y \to \pi(Y)$ is not 1-1.

Proof. For $\lambda \in \Lambda$, let $Y_\lambda = \{x \in Y : x - \lambda \in \mathcal{P}\} = Y \cap (\lambda + \mathcal{P})$. Then we have that $-\lambda + Y_\lambda = \{x - \lambda : x \in Y_\lambda\} \subset \mathcal{P}$.

Then Y is the disjoint union of the Y_λ, since $\mathbb{R}^n = \coprod_{\lambda\in\Lambda} \lambda + \mathcal{P}$.

So $\mathrm{vol}(Y) = \sum \mathrm{vol}(Y_\lambda) = \sum \mathrm{vol}(-\lambda + Y_\lambda) > \mathrm{vol}(\mathcal{P})$, so the subsets $-\lambda + Y_\lambda$ cannot be disjoint, and so there is $x, y \in Y$ with $x - \lambda_1 = y - \lambda_2$. But then $x - y = \lambda_1 - \lambda_2 \in \Lambda$. □

Proof of Minkowski. Assume $\mathrm{vol}(X) > 2^n \mathrm{covol}(\Lambda) = \mathrm{covol}(2\lambda)$. Then by Blichfeldt, there is $x, y \in X$ with $0 \neq x - y \in 2\Lambda$. As X is symmetric, $-y \in X$. As X is convex, $\frac{x+(-y)}{2} \in X$, but also $\frac{x-y}{2} \in \Lambda \setminus \{0\}$.

Now suppose X is compact and $\mathrm{vol}(X) = 2^n \mathrm{covol}(\Lambda)$. For $\delta > 0$, let $X_\delta = \{(1+\delta)x : x \in X\} \supset X$ as X is convex and $0 \in X$. By the first part $X_\delta \cap \Lambda \neq \{0\}$ as $\mathrm{vol}(X_\delta) > 2^n \mathrm{covol}(\Lambda)$.

X_δ is bounded, and $\Lambda = \bigoplus_{i=1}^n \mathbb{Z}e_i$ for a basis (e_i) of $\mathbb{R}^n$, so $X_\delta \cap \Lambda$ is finite. X is also closed, so $X = \bigcap_{\delta>0} X_\delta$, so $X \cap \Lambda = \bigcap_\delta (X_\delta \cap \Lambda) = X_{\delta'} \cap \Lambda$ for some $\delta' > 0$, and so $X \cap \Lambda \neq \{0\}$. □

Now let K be a number field, and order the embeddings $K \hookrightarrow \mathbb{C}$ as $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}; \sigma_{r+1}, \ldots, \sigma_{r+2s} : K \hookrightarrow \mathbb{C}$, with $\sigma_{r+s+i} = \overline{\sigma_{r+i}} \neq \sigma_{r+i}$.

Then the ***product*** is an embedding $\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n; \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha))$.

Proposition 10.6. $\sigma(\mathfrak{o}_K) \subset \mathbb{R}^n$ *is a lattice of covolume* $2^{-s}|d_K|^{\frac{1}{2}}$*.*

Proof. Let $\omega_1, \ldots, \omega_n$ be an integral basis for K. Then $e_i = \sigma(\omega_i) \in \mathbb{R}^n$ is the vector $e_i = (\sigma_1(\omega_i), \ldots, \sigma_r(\omega_i), \mathfrak{Re}\,\sigma_{r+1}(\omega_i), \mathfrak{Im}\,\sigma_{r+1}(\omega_i), \ldots, \mathfrak{Im}\,\sigma_{r+1}(\omega_i)) = (e_{ij})_{1\leq j\leq n}$.

Then $\mathrm{covol}\,\sigma(\mathfrak{o}_K) = |\det(e_{ij})|$. But:

$$\begin{pmatrix} \sigma_j(\omega_i) \\ \bar{\sigma_j}(\omega_i) \end{pmatrix} = \begin{pmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{pmatrix} \begin{pmatrix} \mathfrak{Re}\,\sigma_j(\omega_i) \\ \mathfrak{Im}\,\sigma_j(\omega_i) \end{pmatrix}$$

And so $\det(e_{ij}) = \pm \left(\frac{1}{-2\mathrm{i}}\right)^{-s} \det(\sigma_j(\omega_i))$, and so $\mathrm{covol}(\sigma(\mathfrak{o}_K)) = 2^{-s}|\det(\sigma_j * \omega_i))| = 2^{-s}|d_K|^{\frac{1}{2}}$. □

Then by **7.1** we can immediately deduce:

Corollary 10.7. *Let* $I \subset \mathfrak{o}_K$ *be a nonzero ideal. Then* $\sigma(I)$ *is a lattice of covolume* $2^{-s}|\,\mathrm{disc}(I)|^{\frac{1}{2}} = 2^{-s}\,\mathrm{N}(I)|d_K|^{\frac{1}{2}}$*.*

This then lets us state the main theorem of this section:

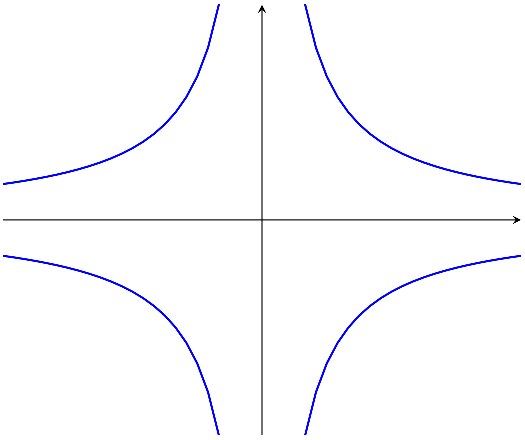
Theorem 10.8 (Minkowski Bound)**.** *For any nonzero $I \subset \mathfrak{o}_K$, there exists $0 \neq \alpha \in I$ with $|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| \leq c_K \operatorname{N}(I)$, where:*

$$c_k = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |d_K|^{\frac{1}{2}}$$

where $n = r + 2s$ in the usual way.

Some special cases to be aware of: real quadratic fields give $c_K = \frac{1}{2}|d_K|^{\frac{1}{2}}$, and imaginary quadratics give $\frac{2}{\pi}|d_K|^{\frac{1}{2}}$.

Proof. We will first consider the case $K = \mathbb{Q}(\sqrt{d})$, $d > 0$. Then $\sigma : K \hookrightarrow \mathbb{R}^2$ is given by $u + v\sqrt{d} \mapsto (u + v\sqrt{d}, u - v\sqrt{d})$. $\operatorname{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = u^2 - dv^2$, and so $|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| \leq R$ if and only if $\sigma(\alpha)$ lies in the region bounded by the hyperbolae $x_1 x_2 = \pm R$.



To apply Minkowski's theorem, we need to choose a convex symmetric subset of this region, and for optimal bound we want it to have the largest possible area. This is the square with vertices $(\pm 2R^{\frac{1}{2}}, 0), (0, \pm 2R^{\frac{1}{2}})$, and area $8R$. Then Minkowski's theorem gives us a lattice point in this region if $8R \geq 4 \operatorname{covol} \sigma(I) = 4|d_k|^{\frac{1}{2}} \operatorname{N}(I)$.

Then taking $R = \frac{1}{2}|d_K|^{\frac{1}{2}} \operatorname{N}(I)$, there is some $0 \neq \alpha \in I$ with $\operatorname{N}_{K/\mathbb{Q}}(\alpha)| \leq c_K \operatorname{N}(I)$, with $c_K = \frac{1}{2}|d_K|^{\frac{1}{2}}$, the c_K of the theorem if $(r, s) = (2, 0)$

For the general case, we have $\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$. The quadratic cases suggest the following choice:

$$X = X_R = \{(x_1, \ldots, x_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s | \sum |x_j| + 2\sum |z_j| \leq nR^{\frac{1}{n}}\}$$

Then the AM-GM inequality gives that:

$$\prod |x_j| \prod |z_j|^2 \leq R$$
$$\sigma(\alpha) \in X_R \implies |\operatorname{N}_{K/\mathbb{Q}}(\alpha)| \leq R$$

It is an exercise to show that X_R is convex and symmetric about 0 and compact. It remains only to compute the volume of X_R - see Lemma **10.10**. □

Corollary 10.9. *Every ideal class of K contains an ideal of norm $\leq c_K$. In particular, $Cl(K)$ is finite, generated by the classes of prime ideals of norm $\leq c_K$.*

Proof. Word for word the same as **10.3** □

Lemma 10.10.

$$\mathrm{vol}(X_r) = 2^r \left(\frac{\pi}{2}\right)^s \frac{n^n}{n!} R$$

If we put this with Minkowski's theorem, we get Minkowski's bound.

Examples of using Minkowski's bound:

- Let $K = \mathbb{Q}(\sqrt{-17})$, $d_K = -68$, $c_K = 2\frac{\sqrt{68}}{\pi} < 2\frac{9}{3} = 6$, so $Cl(K)$ is generated by classes of prime ideals of norm $2, 3$, or 5, since if P is prime of norm p^2 then P would be (p), so principal.

– $p = 5$. $-17 \equiv -2$ which is not a square mod 5, so 5 is inert and there is no P of norm 5.

– $p = 3$. $-17 \equiv 1^2 \mod 3$, so $(3) = P_3 P_3'$. Then we can compute $P_3 = (3, 1 + \sqrt{-17}), P_3' = (3, 1 - \sqrt{-17})$.

– $p = 2$. This is ramified as $-17 \not\equiv 1 \mod 4$, so $(2) = P_2^2, P_2 = 2, 1 + \sqrt{-17})$.

Note that none of P_2, P_3, P_3' are principal as there is no solution of $u^2 + 17v^2 = 2$ or 3 in the integers.

We have the relations $[P_2]^2 = 1 = [P_3][P_3']$ in the class group $Cl(K)$. To find more relations, we can do $P_3^2 = (3, 1 + \sqrt{-17})^2 = (9, 1 + \sqrt{-17})$, which has norm 9. Now $\mathrm{N}_{K/\mathbb{Q}}(1 + \sqrt{-17}) = 18$, and $1 + \sqrt{-17} \in P_3^2$, and so $(1 + \sqrt{-17}) = P_3^2 \times (\text{norm } 2) = P_2 P_3^2$, as P_2 is the only ideal of norm 2. Hence in $Cl(K), [P_3]^2 = [P_2]^{-1} = [P_2]$.

Hence $Cl(K)$ is cyclic of order 4 generated by $[P_3]$.

- $K = \mathbb{Q}(\theta)$, for θ a root of $g = x^5 - x + 1$, which is irreducible mod 5 and hence irreducible. We can show that g has 1 real root, so $(r, s) = (1, 2)$. The discriminant of g is $2689 = 19 \times 151$ is squarefree. So $\mathfrak{o}_K = \mathbb{Z}[\theta]$. $c_K = 3.3\ldots$, and so $Cl(K)$ is generated by prime ideals of norm ≤ 3. Dedekind's criterion says that there is a prime of norm p if and only if g has a root mod p. But g has no root mod 2 or mod 3. So $Cl(K)$ is trivial.

It is known that $\#Cl(\mathbb{Q}(\sqrt{-d})) \to \infty$ as $d \to \infty$, and $Cl(K) \neq \{1\}$ for all $d > 163$. If $K = \mathbb{Q}(\sqrt{d})$, it is thought that there are infinitely many d with $|Cl(K)| = 1$.

Example: Compute $Cl(K)$ for $K = \mathbb{Q}(\sqrt{10})$.

The Minkowski constant $c_K = \frac{1}{2}\sqrt{40} = \sqrt{10} < 4$, so $Cl(K)$ is generated by classes of prime ideals of norm 2 or 3.

- $(2) = (2, \sqrt{10})^2 = P_2^2$
- $(3) = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}) = P_3 P_3'$

So $[P_2]^2 = [P_3][P_3'] = 1$ in $Cl(K)$. To get more relations, look at elements of $\mathfrak{o}_K$ of small norm. Any relation between $[P_2]$ and $[P_3]$ is of the form $P_2^m P_3^n = (\alpha)$, where $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 2^m 3^n$.

- $Nn_{K/\mathbb{Q}}(1 + \sqrt{10}) = -9$, and $1 + \sqrt{10} \in P_3 \implies P_3 | (1 + \sqrt{10})$. As $1 + \sqrt{10} \notin P_3'$, we must have $P_3^2 = (1 + \sqrt{10})$.

- $\mathrm{N}_{K/\mathbb{Q}}(2+\sqrt{10}) = -6$, and $2+\sqrt{10} \in P_2 \cap P_3'$. So $(2+\sqrt{10}) = P_2P_3'$.

Hence $[P_2] = [P_3] = [P_3']$ has order 1 or 2 in $Cl(K)$, so either $Cl(K) = \{1\}$ or $\mathbb{Z}/2\mathbb{Z}$. Is P_2 principal? If so $P = (u + v\sqrt{10})$, and $u^2 - 10v^2 = \pm 2$, so $u^2 \equiv \pm 2 \mod 5$, which is impossible. So P_2 is not principal and $Cl(K) \cong \mathbb{Z}/2\mathbb{Z}$.

We call the order of the class group $\#Cl(K)$ the ***class number*** of K, and write h_K. If K is an imaginary quadratic, then the ideal class group is closely related to the classes of binary quadratic forms of discriminant d_K.

11 Units

If K is a number field, then we call the group of units $\mathfrak{o}_K^*$, the multiplicative group of algebraic integers.

Theorem 11.1 (Dirichlet's Unit Theorem)**.** $\mathfrak{o}_K^*$ *is finitely generated of rank* $r+s-1$.

The torsion subgroup of $\mathfrak{o}_K^*$ is the subgroup of elements of finite order in K^*, i.e. the roots of unity, as every root of unity is an algebraic integer. So this group is finite and therefore is *cyclic* by Galois theory.

So this theorem says that there are $\epsilon_1, \ldots, \epsilon_{r+s-1} \in \mathfrak{o}_K^*$ such that every $\epsilon \in \mathfrak{o}_K^*$ can be uniquely written as $\epsilon = \zeta\epsilon_1^{a_1} \ldots \epsilon_{r+s-1}^{a_{r+s-1}}$ for $a_i \in \mathbb{Z}$, where ζ is a root of unity in K.

Example: $K = \mathbb{Q}(\sqrt{d})$ quadratic, $\mathfrak{o}_K = \{u + v\sqrt{d}\}$. Recall if $\alpha \in \mathfrak{o}_K$ then $\alpha \in \mathfrak{o}_K^* \iff \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1 = u^2 - dv^2$ in this case.

- $K = \mathbb{Q}(\sqrt{d})$ imaginary quadratic. $\alpha \in \mathfrak{o}_K^* \iff u^2 - dv^2 = 1$, so $\mathfrak{o}_K^*$ is finite, and $r + s - 1 = 0 + 1 - 1 = 0$. It is easy to check that $\mathfrak{o}_K^* = \{\pm 1\}$ except in the case $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, where $\mathrm{ord}(\mathfrak{o}_K^*) = 4$ or 6 respectively.

- $K = \mathbb{Q}(\sqrt{d})$ real quadratic. Then we get ***Pell's Equation*** $u^2 - dv^2 = 1$, and by Part II Number Theory, there are infinitely many solutions for fixed $d > 1$, and so $\mathfrak{o}_K^*$ is infinite. In fact we can be more precise:

Theorem 11.2. *Let* $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ *for* $d > 0$ *squarefree. Then there exists a unique smallest* $\epsilon \in \mathfrak{o}_K^*$ *with* $\epsilon > 1$*, called the* **fundamental unit***, and* $\mathfrak{o}_K^* = \{\pm\epsilon^m : m \in \mathbb{Z}\}$.

Proof. Take as known that $\mathfrak{o}_K^*$ is infinite - another proof of this will follow. Then the only roots of unity in K are ± 1 since $K \subset \mathbb{R}$. Let $\epsilon \in \mathfrak{o}_K^* \setminus \{\pm 1\}$, $\epsilon = u + v\sqrt{d}$. We then claim claim that $\epsilon > 1$ if and only if both $u, v > 0$.

Indeed, as ϵ is unit, i.e. $u^2 - dv^2 = \pm 1$, all of $\{\pm u \pm v\sqrt{d}\} = \{\pm\epsilon, \pm 1/\epsilon\}$ are units, and exactly one of them lies in the each of the intervals $(-\infty, -1), (-1, 0), (0, 1), (1, \infty)$. So $\epsilon > 1 \iff \epsilon$ is the largest of these four, and so $\epsilon \in (1, \infty)$.

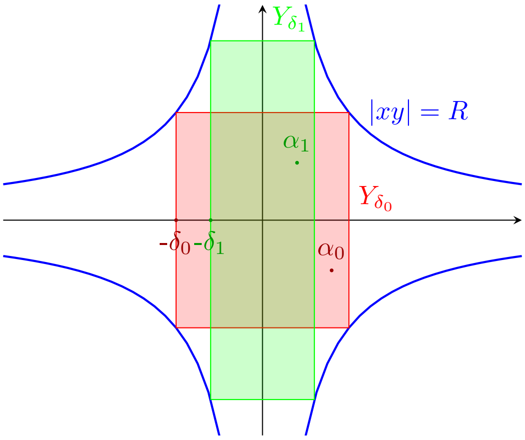
So now choose $\epsilon \in \mathfrak{o}_K^*$, $\epsilon > 1$ with v minimal. It is then easy to see that ϵ is minimal, and then if $\epsilon' \in \mathfrak{o}_K^*$, $\epsilon' > 1$ and so there exists $m \geq 1$ with $\epsilon^m \leq \epsilon' < \epsilon^{m+1}$. Then $1 \leq \epsilon'/\epsilon^m < \epsilon$, so by minimality, $\epsilon'/\epsilon^m = 1$, So the set of units > 1 is precisely $\{\epsilon^m : m \geq 1\}$. Repeating this for each of the four intervals, we see that $\mathfrak{o}_K^* = \{\pm\epsilon^m : m \in \mathbb{Z}\}$. □

Direct proof without using continued fractions. We first construct lots of elements of K of bounded norm, using the following lemma:

Lemma 11.3. *If $R \geq |d_K|^{\frac{1}{2}}$, there are infinitely many $\alpha \in \mathfrak{o}_K$ with $|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq R$.*

Assuming this, using the fact that there are only finitely many ideals of norm $\leq R$, we have that $\exists\ \alpha \neq \beta \in \mathfrak{o}_K$ with $(\alpha) = (\beta)$, and then $\alpha/\beta \in \mathfrak{o}_K^*$.

Proof of Lemma. $\sigma : K \hookrightarrow \mathbb{R}^2; \sqrt{d} \mapsto (\sqrt{d}, -\sqrt{d})$. Consider the rectangle $Y_\delta = [-R/\delta, R/\delta] \times [-\delta, \delta]$.



$4R = \mathrm{vol}(Y_\delta) \geq 4\,\mathrm{covol}\,\sigma(\mathfrak{o}_K) = 4|d_K|^{\frac{1}{2}}$. Then take $\delta = \delta_0 = 1$. By Minkowski, there exists $\alpha_0 \in \mathfrak{o}_K \setminus \{0\}$ with $\sigma(\alpha) \in Y_\delta$.

Hence $|\mathrm{N}_{K/\mathbb{Q}}(\alpha_0)| \leq R$, and $|\sigma_1(\alpha_0)| \leq \delta_0$. Now let $0 < \delta_1 < |\sigma_1(\alpha_0)| \implies \alpha_1 \in \mathfrak{o}_K \setminus \{0\}$, with $|\mathrm{N}_{K/\mathbb{Q}}(\alpha_1)| \leq R$ and $|\sigma_1(\alpha_1)| \leq \delta_1 < |\sigma_1(\alpha_0)|$. Continuing, we get an infinite sequence of $\alpha_0, \alpha_1, \ldots$ of distinct elements of $\mathfrak{o}_K$ with $|\mathrm{N}_{K/\mathbb{Q}}(\alpha_j)| \leq R$. □

□

Lemma 11.4. *A subgroup $\Lambda \subset \mathbb{R}^n$ is a lattice if and only if:*

1. *It spans $\mathbb{R}^n$*

2. *For every bounded $X \subset \mathbb{R}^n$, $X \cap \Lambda$ is finite.*

A subgroup satisfying the second condition is called a ***discrete subgroup***, because the induced topology on Λ is discrete. In this case, if $V \subset \mathbb{R}^n$ is the span of Λ, the lemma implies that Λ is a lattice in $V \cong \mathbb{R}^m$ for some $m \leq n$, so is freely generated by $m \leq n$ linearly independent elements.

Proof. Suppose $\Lambda \subset \mathbb{R}^n$ is a lattice, so is $= \bigoplus_{i=1}^n \mathbb{Z}e_i$, with (e_i) a basis. Then there is invertible $u : \mathbb{R}^n \to \mathbb{R}^n$ such that $u(\Lambda) = \mathbb{Z}^n$. Then X bounded if and only if $u(X)$ is bounded, and if so, $u(X) \cap \mathbb{Z}^n$ is clearly finite.

Conversely, assume the two conditions. Then Λ contains a basis for $\mathbb{R}^n$ by *1.*, so after a change of basis we may assume $\Lambda \supset \mathbb{Z}^n$. Then let $S = \{x = (x_i) \in \Lambda | 0 \leq x_i < 1 \forall i\}$. Then $\Lambda = \{x + \lambda : x \in S, \lambda \in \mathbb{Z}^n\}$, i.e. S is a set of coset representatives of $\mathbb{Z}^n \leq \Lambda$. Now S is finite, so $(\Lambda : \mathbb{Z}^n) = d < \infty$, and so $\frac{1}{d}\mathbb{Z}^n \supset \Lambda$. Then by GRM, Λ is free abelian of rank n, so is $\sum \mathbb{Z}e_i$, but since Λ spans $\mathbb{R}^n$, the e_i are independent, so $\Lambda = \bigoplus \mathbb{Z}e_i$, a lattice. □

Lemma 11.5. *Let $C > 0$, K an algebraic field. Then $\{\alpha \in \mathfrak{o}_K : \forall i |\sigma_i(\alpha)| \leq C\}$ is finite.*

Proof. Consider the characteristic polynomial of α:

$$\begin{aligned}\prod_i (x - \sigma_i(\alpha)) &= x^n + \sum_{r=1}^{n} c_r x^{n-r} \\ &= x^n + \sum_{r=1}^{n} (-1)^r \sum_{i_1 < \ldots < i_r} \sigma_{i_1}(\alpha) \ldots \sigma_{i_r}(\alpha) x^{n-r}\end{aligned}$$

As $c_r \in \mathbb{Z}$, $|c_r| \leq \binom{n}{r} C^r$, there are only finitely many such characteristic polynomials. □

Corollary 11.6. *The group of roots of unity in K is finite, so cyclic by Galois theory.*

Proof. Roots of unity are algebraic integers as they satisfy $x^n - 1$, and satisfy $|\sigma_i(\alpha)| = 1$. □

To show $\mathfrak{o}_K^*$ is finitely generated, we use lattice methods by mapping into some $\mathbb{R}^m$, so we will take logarithms.

We define the ***logarithmic embedding*** $\mathscr{L} : K^* \to \mathbb{R}^{r+s}$, given by:

$$\mathscr{L}(\alpha) = (\mathscr{L}(\alpha)_i)_{1 \leq i \leq r+s} \in \mathbb{R}^{r+s}$$
$$\mathscr{L}(\alpha)_i = \begin{cases} \log |sigma_i(\alpha) & 1 \leq i \leq r \\ 2 \log |\sigma_i(\alpha)| & r+1 \leq i \leq r+s \end{cases}$$

Then we have the following properties of $\mathscr{L}$:

1. $\mathscr{L}$ is a homomorphism.
2. $\alpha in K^* \implies \sum_{i=1}^{r+s} \mathscr{L}(\alpha)_i = \log |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$, since:

$$\begin{aligned}\log |\mathrm{N}_{K/\mathbb{Q}}(\alpha)| &= \sum_{i=1}^{n} \log |\sigma_i(\alpha)| \\ &= \sum_{i=1}^{r} \log |\sigma_i(\alpha)| + \sum_{i=1}^{s} \log |\sigma_{r+i}(\alpha)| + \log |sigma_{r+s+i}(\alpha)| \\ &= \sum_{i=1}^{r+s} \mathscr{L}(\alpha)_i\end{aligned}$$

3. $\alpha \in \mathfrak{o}_K^* \implies \mathscr{L}(\alpha) \in \mathbb{R}^{r+s,0} := \{(x_i) \in \mathbb{R}^{r+s} : \sum x_i = 0\}$, and $\mathscr{L}(\alpha) = 0$ if α is a root of unity.

Proposition 11.7.

1. $\ker \mathscr{L} \cap \mathfrak{o}_K^*$ *is the subgroup of roots of unity in K.*
2. $\mathscr{L}(\mathfrak{o}_K^*)$ *is a discrete subgroup of* $\mathbb{R}^{r+s,0}$.

Proof. Let $M > 0$ and consider $Z = \{(x_i) \in \mathbb{R}^{r+s} : \forall i |x_i| \leq M\}$. Then $\mathscr{L}(\alpha) \in Z \iff e^{-M} \leq |\sigma_i(\alpha)| \leq e^M$ for $i \leq r$, and the same with $|\sigma_i(\alpha)|^2$ for $i > r$.

So by lemma **11.5** $S = \{\alpha \in \mathfrak{o}_K^* : \mathscr{L}(\alpha) \in Z\}$ is finite. As $0 \in Z, S \supset \ker \mathscr{L} \cap \mathfrak{o}_K^*$, so $\ker \mathscr{L} \cap \mathfrak{o}_K^*$ is finite. By the third property above, we have *1.* S is finite, so $\mathscr{L}(\mathfrak{o}_K^*) \cap Z$ is finite for all M, yielding *2.* □

Corollary 11.8. $\mathfrak{o}_K^*$ *is finitely generated of rank* $\leq r + s - 1$.

Proof. $\mathscr{L}(\mathfrak{o}_K^*)$ is a discrete subgroup of $\mathbb{R}^{r+s}$, contained in $\mathbb{R}^{r+s,0}$. So it is generated by $e_1, \dots, e_t \in \mathbb{R}^{r+s,0}$ linearly independent, for some $0 \leq t \leq r + s - 1$. Choose $\epsilon_1, \dots, \epsilon_t \in \mathfrak{o}_K^*$ with $\mathscr{L}(\epsilon_i) = e_i$. Then for any $\epsilon \in \mathfrak{o}_K^*$, $\mathscr{L}(\epsilon) = \sum_{i=1}^t m_i e_i$ for some unique $(m_i) \in \mathbb{Z}^t$, and hence $\epsilon/(\epsilon_1^{m_1} \dots \epsilon_t^{m_t} = \zeta$ satisfies $\mathscr{L}(\zeta) = 0$, i.e. ζ is a root of unity. So $\mathfrak{o}_K^* = \{\zeta \epsilon_1^{m_1} \dots \epsilon_t^{m_t} : \zeta$ a root of unity, $m_i \in \mathbb{Z}\}$. □

Dirichlet's unit theorem says that, moreover, $\operatorname{rank} \mathfrak{o}_K^* = r + s - 1$. Note that $r + s - 1 = 0$ in precisely 2 cases:

- $(r, s) = (1, 0)$ in which case $K = \mathbb{Q}$
- $(r, s) = (0, 1)$ in which case $K = \mathbb{Q}(\sqrt{-d})$

So to prove the unit theorem, we will have to show:

Theorem 11.9. $\mathscr{L}(\mathfrak{o}_K^*)$ *is a lattice in* $\mathbb{R}^{r+s,0}$.

Then we will have $r + s - 1$ independent units in K, proving Dirichlet's unit theorem.

Proposition 11.10. *Given* $1 \leq jleqr + s$, *there is a constant* C *such that, for any* $\delta > 0$, *there is some* $\alpha \in \mathfrak{o}_K$ *with:*

1. $|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| \leq C$
2. $\forall i \neq j, |\sigma_i(\alpha)| \leq \delta$

Proof. Consider the set $Y \subset \mathbb{R}^r \times \mathbb{C}^s$ of points z_i given by the inequalities:

$$|z_i| \leq \begin{cases} C\delta^{1-n} & i = j \leq r \qquad (z_i \in \mathbb{R}) \\ \delta & i \neq j \qquad\quad\; (z_i \in \mathbb{C}) \end{cases}$$

Then if $\alpha \in K$ and $\sigma(\alpha) \in Y$,

$$|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \times \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)|^2 \leq C$$

and $\operatorname{vol} Y = 2^r \pi^s C$. Applying Minkowski for C sufficiently large, there is $\alpha \in \mathfrak{o}_K \setminus \{0\}$ with $\sigma(\alpha) \in Y$, and so satisfying the conditions. The argument is similar for $r + 1 \leq j \leq r + s$. □

Corollary 11.11. *Given* $1 \leq j \leq r + s$, *there exists* $\epsilon = \epsilon_j \in \mathfrak{o}_K^*$ *such that* $|\sigma_j(\epsilon)| > 1$ *and* $|\sigma_i(\epsilon)| < 1$ *for all* $i \neq j$.

Proof. By **11.10** we can find $\alpha_1, \alpha_2, \dots \in \mathfrak{o}_K$ with $|\operatorname{N}_{K/\mathbb{Q}}(\alpha_k)| \leq C$, and such that $|\sigma_i(\alpha_{k+1})| < |\sigma_i(\alpha_k)|$ for all $i \neq j$, choosing δ sufficiently small each time. So there exist k, ℓ with $k < \ell$ and $(\alpha_k) = (\alpha_\ell)$, since there are only finitely many ideals of norm $\leq C$. Then $\epsilon = \alpha_\ell/\alpha_k$ will do. □

To complete the proof, we will show that the elements $\mathscr{L}(\epsilon_j)$ for $1 \leq j \leq rs$ span $\mathbb{R}^{r+s,0}$. Consider the matrix $(\mathscr{L}(\epsilon_j)_k) \in Mat_{r+s,r+s}(\mathbb{R})$, with entries $(2) \log |\sigma_k(\epsilon_j)|$. The only positive entries lie on the principal diagonal.

Lemma 11.12. *Let $A \in Mat_{m,m}(\mathbb{R})$ such that:*

1. *For all $j \neq k$, $A_{jk} < 0$*
2. *For all $j, \sum_k A_{j,k} = C$.*

Then A has rank $m-1$.

Proof. Let $x \in \mathbb{R}^m$. Show that $Ax = 0 \iff x \in \operatorname{span}(1, \ldots, 1)$.Condition 2 gives $\Longleftarrow$. To prove $\Longrightarrow$, suppose that x_k is the largest coordinate of x. Then $Ax = 0 \implies \sum_{j \neq k} A_{kj}(x_k - x_j) = \sum_{j=1}^m A_{kj}x_k - \sum_{j=1}^m A_{kj}x_j = 0$

But $x_k \geq x_j \forall j$, and $A_{kj} < 0$, so we must have all $x_j = x_k$. □

12 Application to Diophantine Equations

Diophantine equations in ≥ 2 variables, where we ask for $\mathbb{Z}$ or $\mathbb{Q}$. For example, we might seek solutions to $y^2 + 5 = x^3$ where $x, y \in \mathbb{Z}$.

We can factor this in $\mathbb{Z}[\sqrt{-5}] = \mathfrak{o}_K$ for $K = \mathbb{Q}(\sqrt{-5})$. Then $x^3 = (y + \sqrt{-5})(y - \sqrt{-5})$. Notice $(x, 10) = 1$, as if $2|x$ then $y^2 + 5 \equiv 0 \mod 4$, and if $5|x$ then $5|y \implies 25|x^3 - y^2 = 5$.

Since $\mathbb{Z}[\sqrt{-5}]$ is not a UFD we have to use ideals. Suppose $P \subset \mathfrak{o}_K$ is prime with $P|(y + \sqrt{-5})$ and $P|(y - \sqrt{-5})$. Then $P|(y + \sqrt{-5}, y - \sqrt{-5}) \supset (2\sqrt{-5})$, so $P|(10)$. But also $P|(x^3)$ and $(x, 10) = 1$. So there is no such P.

So by unique factorisation of ideals, $(y + \sqrt{-5}) = I^3, (y0\sqrt{-5}) = J^3$ with $IJ = (x)$, as ideals $(y + \sqrt{-5}), (y - \sqrt{-5})$ have no common prime ideal factors. Now we use from earlier, that $Cl(K) \cong \mathbb{Z}/2\mathbb{Z}$. As I^3 is principal, we must have that I is principal, so $I = (a + b\sqrt{-5})$ say. So $y + \sqrt{-5} = (\text{unit})(a + b\sqrt{-5})^3 = \pm(a + b\sqrt{-5})^3$ as $\mathfrak{o}_K^* = \{\pm 1\}$. Absorbing the ± into a, b, we have $y + \sqrt{-5} = (a + b\sqrt{-5})^3 = (a^3 - 15ab^2) + (3a^2b - 3b^3)\sqrt{-5}$.

So $1 = 3a^2b - 5b^3 = (3a^2 - 3b^2)b$, so $b = \pm 1$, and there are no solutions in $\mathbb{Z}$.