Number fields

Shing Tak Lam

May 23, 2023

Contents

1 Integrality

1.1 Number fields and rings of integers

Definition 1.1 (number field)

A number field L is a finite extension of $\mathbb{Q}$.

Definition 1.2 (algebraic integer)

If L is a number field, we say that $\alpha \in L$ is an algebraic integer if there exists $f \in \mathbb{Z}[x]$ monic such that $f(\alpha) = 0$. The set of ring of integers in L is written as $\mathcal{O}_L$.

Definition 1.3 (integral)

Suppose $R \leq S$ rings. Then $\alpha \in S$ is integral over R if there exists $f \in R[x]$ monic such that $f(\alpha) = 0$. We say that S is integral over R if all $\alpha \in S$ are integral over R.

Definition 1.4 (finitely generated over)

Suppose $R \leq S$ rings, then S is finitely generated over R if there exists $\alpha_1, \dots, \alpha_n \in S$ such that every element of$S$ is an R-linear combination of the $\alpha_1, \dots, \alpha_n$. That is, S is a finitely generated R-module.

Proposition 1.5.

1. if $S = R[s]$, with s integral over R, then S is finitely generated over R,

2. if $S = R[s_1, \dots, x_n]$ with each s_i integral over R, then S is finitely generated over R.

Proof. (i) As an R-module, S is spanned by $1, s, s^2, \dots$. But as s is integral over R, we have that

$$s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0$$

for some $a_0, \dots, a_{n-1} \in R$. So $1, s, \dots, s^{n-1}$ generate S.

(ii) Let $S_i = R[s_1, \dots, s_{i-1}]$, so $S_{i+1} = S_i[s_i]$. s_i is integral over R, so it is integral over S_i. Hence S_{i+1} is finitely generated over S_i. Hence by induction, S_{i+1} is finitely generated over R. Hence $S = S_{n+1}$ is finitely generated over R. □

Theorem 1.6. Suppose S is finitely generated over R. Then S is integral over R.

Proof. Let $\alpha_1, \dots, \alpha_n$ generate S as an R-module. Without loss of generality, $\alpha_1 = 1$. Let $s \in S$, and consider $m_s : S \to S$, given by $x \mapsto sx$. Then

$$s\alpha_i = \sum_j b_{ij}\alpha_j$$

for some $b_{ij} \in R$. Let B be the matrix (b_{ij}). By definition, we have that

$$(sI - B)\begin{pmatrix}\alpha_1 \\ \cdot s \\ \alpha_n\end{pmatrix} = 0$$

Multiplying this by $\operatorname{adj}(sI - B)$, we get that

$$\det(sI - B)\begin{pmatrix}\alpha_1 \\ \cdot s \\ \alpha_n\end{pmatrix} = 0$$

But $\alpha_1 = 1$, so $\det(sI - B) = 0$. Define $f(t) = \det(tI - B) \in R[t]$. This is a monic polynomial with coefficients in R, and with $f(s) = 0$. So s is integral over R. □

Corollary 1.7. If L is a number field, the $\mathcal{O}_L$ is a ring.

Proof. If $\alpha, \beta \in \mathcal{O}_L$, then $\mathbb{Z}[\alpha, \beta]$ is finitely generated over $\mathbb{Z}$, so it is integral over $\mathbb{Z}$. Hence $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$, so $\alpha \pm \beta, \alpha\beta \in \mathcal{O}_L$. □

Corollary 1.8. If $A \leq B \leq C$ rings, B integral over A, C integral over B, then C is integral over A.

Proof. If $c \in C$, let $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ be a monic polynomial over $B[x]$ such that $f(c) = 0$. Set $B_0 = A[b_0, \dots, b_{n-1}]$, and $C_0 = B_0[c]$. Then B_0 is finitely generated over A, C_0 is finitely generated over B_0 as c is integral over B_0. Hence C_0 is finitely generated over A, qso C_0 is integral over A. □

Proposition 1.9. Let L be a number field. Then $\alpha \in \mathcal{O}_L$ if and only if the minimal polynomial $p_\alpha(x) \in \mathbb{Q}[x]$ for α is in $\mathbb{Z}[x]$.

Proof. ($\Longleftarrow$) is true by definition. For the converse, let $\alpha \in \mathcal{O}_L$, with minimal polynomial p_α. Let M/L be a splitting field for p_α, so $p_\alpha(x) = (x - \alpha_1)\cdots(x - \alpha_n)$ in $M[x]$. Let $h(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $h(\alpha) = 0$. Then $p_\alpha \mid h <$ so each $\alpha_i \in M$ is an algebraic integer. But $\mathcal{O}_L$ is a ring, so the coefficients of p_α are in $\mathcal{O}_L$. Finally, the result follows by $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$. $\square$

Lemma 1.10. If $\alpha \in L$, then there exists $n \in \mathbb{Z} \setminus 0$ such that $n\alpha \in \mathcal{O}_L$.

Proof. Let $g \in \mathbb{Q}[x]$ be the minimal polynomial for α. Then by clearing denominators, we have $n \in \mathbb{Z} \setminus 0$ such that $h(x) = n^{\deg(g)} g(x/n) \in \mathbb{Z}[x]$ is monic. Now notice that $h(n\alpha) = n^{\deg(g)} g(\alpha) = 0$, so $n\alpha \in \mathcal{O}_L$. $\square$

1.2 Trace and norm

Recall from Galois theory that if L/K is a field extension, $\alpha \in L$, let $m_\alpha(x) = \alpha x$. Then we have the norm and the trace of α,

$$N_{L/K}(\alpha) = \det(m_\alpha) \quad \text{and} \quad \mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}(m_\alpha)$$

If $p_\alpha(x)$ is the minimal polynomial of α over K, then the characteristic polynomial of m_α is $\det(xI - m_\alpha) = p_\alpha^{[L:K(\alpha)]}$. Furthermore, if M is a splitting field for p_α, with $p_\alpha)(x) = (x - \alpha_1)\cdots(x - \alpha_n)$, then

$$N_{K(\alpha)/K} = \prod_i \alpha_i \quad \text{and} \quad \mathrm{tr}_{K(\alpha)/K} = \sum_i \alpha_i$$

By the tower law of norm and trace, we then have that

$$N_{L/K}(\alpha) = \left(\prod_i \alpha_i\right)^{[L:K(\alpha)]} \qquad \text{and} \quad \mathrm{Tr}_{L/K}(\alpha) = [L : K_\alpha] \sum_i \alpha_i$$

Proposition 1.11. Let L be a number field, $\alpha \in L$. Then the following are equivalent.

(i) $\alpha \in \mathcal{O}_L$,

(ii) $p_\alpha \in \mathbb{Z}[x]$,

(iii) the characteristcic polynomial of m_α is in $\mathbb{Z}[x]$.

Therefore, $N_{L/\mathbb{Q}}(\alpha), \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

1.3 Integral basis, discriminant

Definition 1.12 (integral basis)
Let L be a number field. A basis $\alpha_1, \ldots, \alpha_n$ of $L/\mathbb{Q}$ is called an integral basis if

$$\mathcal{O}_L = \left\{ \sum_{i=1}^n m_i \alpha_i \;\middle|\; m_i \in \mathbb{Z} \right\} = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i$$

Recall from Galois:

(i) $L/\mathbb{Q}$ is a finite separable extension, as $\mathrm{char}(\mathbb{Q}) = 0$, so by the primitive element theorem, $L = \mathbb{Q}(\alpha)$ for some $\alpha \in L$.

$$\mathbb{Q}(\alpha) \simeq \frac{\mathbb{Q}[x]}{(p_\alpha)}$$

L is a field, so (p_α) is a maximal ideal in a PID, so p_α is irreducible.

Let $\deg(p_\alpha) = n$. Then $L/\mathbb{Q}$ has basis $1, \alpha, \ldots, \alpha^{n-1}$.

(ii) The number of field embeddings $L \to \mathbb{C}$ is n. Let $\sigma_1, \ldots, \sigma_n : L \to \mathbb{C}$ be the distinct embeddings. Then for $\beta \in L$,

$$\mathrm{Tr}_{L/\mathbb{Q}}(\beta) = \sum_i \sigma_i(\beta) \quad \text{and} \quad N_{L/\mathbb{Q}}(\beta) = \prod_i \sigma_i(\beta)$$

Definition 1.13 (r, s)

Let L be as above. Define r to be the number of real roots of $p_\alpha(x)$, or equivalently the number of field embeddings $L \to \mathbb{R}$, s to be the number of complex conjugate pairs of roots of $p_\alpha(x)$. So $r + 2s = n$.

Proposition 1.14. r, s are independent of α.

Proof. Since r is the number of field embeddings $L \to \mathbb{R}$. □

Proposition 1.15. Let L/K be a finite separable extension. Then the K-bilinear form

$$(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$$

is nondegenerate. We call it the trace form. Equivalently, if $\alpha_1, \ldots, \alpha_n$ is a basis for L/K, the matrix

$$\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{i,j}$$

has nonzero determinant. We write

$$\Delta(\alpha_1, \ldots, \alpha_N) = \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)$$

Proof. Let $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ be the n distinct K-linear field emebeddings, let

$$S = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}$$

Then we have that

$$(S^T S)_{ij} = \sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_k \sigma_k(\alpha_i \alpha_j) = \mathrm{Tr}_{L/K}(\alpha_i \alpha_j)$$

which means that $\Delta(\alpha_1, \ldots, \alpha_n) = \det\left(S^T S\right) = (\det(S))^2$. Now by the primitive element theorem, there exists $\theta \in L$ such that $L = K(\theta)$, so $1, \theta, \ldots, \theta^{n-1}$ are a basis for L/K. In this case, we have that

$$S = \begin{pmatrix} 1 & \sigma_1(\theta) & \ldots & \sigma_1(\theta)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\theta) & \ldots & \sigma_n(\theta)^{n-1} \end{pmatrix}$$

which is a Vandermonde matrix, so we find that

$$\det(S)^2 = \prod_{i<j} (\sigma_i(\theta) - \sigma_j(\theta))^2 = \Delta(1, \theta, \ldots, \theta^{n-1})$$

which is nonzero since $L = K(\theta)$ and the σ_i are distinct. Finally, if $\alpha_1, \ldots, \alpha_n$ is any basis for L/K, $\alpha'_1, \ldots, \alpha'_n$ is any other basis, then

$$\Delta(\alpha'_1, \ldots, \alpha'_n) = (\det(A))^2 \, \Delta(\alpha_1, \ldots, \alpha_n)$$

where $\alpha_i = \sum_j a_{ij} \alpha_j$, so it is nonzero for any basis. □

Proposition 1.16. Let $L = K(\theta)$, where the minimal polynomial of θ is

$$p_\theta(t) = \prod_i (t - \sigma_i(\theta))$$

Then we have that

$$\mathrm{Disc}(p_\theta) = \prod_{i<j} (\sigma_i(\theta) - \sigma_j(\theta))^2 = \Delta(1, \theta, \dots, \theta^{n-1})$$

Unfortunately in Galois, we have that Disc $= \Delta^2$, but not much we can do about that...

Proposition 1.17. If $\alpha_1, \dots, \alpha_n \in L$ is a basis of $L/\mathbb{Q}$, with $\alpha_i \in \mathcal{O}_L$, then $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

Proof. $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}$ for all $\alpha, \beta \in \mathcal{O}_L$. □

Theorem 1.18. Let $L/\mathbb{Q}$ be a number field. Then there exists an integral basis for L.

Proof. Let $\alpha_1, \dots, \alpha_n$ be any basis of $L/\mathbb{Q}$. Since we have $m_i \in \mathbb{Z}$ nonzero such that $m_i\alpha_i \in \mathcal{O}_L$, wlog we may assume $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$. So $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Z} \setminus 0$. Choose $\alpha_1, \dots, \alpha_n$ such that $|\Delta(\alpha_1, \dots, \alpha_n)|$ is minimal.

Now let $x \in \mathcal{O}_L$, $x = \sum_i \lambda_i \alpha_i$, with $\lambda_i \in \mathbb{Q}$. Suppose for contradiction $\lambda_1 \notin \mathbb{Z}$. Write $\lambda_1 = n_1 + \varepsilon_1$, with $0 < \varepsilon_1 < 1$ and $n_1 \in \mathbb{Z}$. Let $\alpha_1' = x - n_1\alpha_1 = \varepsilon_1\alpha_1 + \lambda_2\alpha_2 + \dots + \lambda_n\alpha_n \in \mathcal{O}_L$.

Then $\alpha_1', \dots, \alpha_n'$ is still a basis for $L/\mathbb{Q}$, with

$$\Delta(\alpha_1', \alpha_2, \dots, \alpha_n) = \varepsilon_1^2 \Delta(\alpha_1, \dots, \alpha_n)$$

Contradicting minimality. □

Corollary 1.19. If $\alpha_1', \dots, \alpha_n'$ is any other integral basis, then

$$\Delta(\alpha_1, \dots, \alpha_n) = \Delta(\alpha_1', \dots, \alpha_n')$$

Proof. We have a change of basis matrix $g \in \mathrm{GL}_n(\mathbb{Z})$ with $g(\alpha_i') = \alpha_i$. Then $\det(g) = \pm 1$, so $\det(g)^2 = 1$. □

Definition 1.20 (discriminant)
The discriminant of a number field L is

$$D_L = \Delta(\alpha_1, \dots, \alpha_n)$$

for any integral basis $\alpha_1, \dots, \alpha_n$.

2 Ideals in number fields

Lemma 2.1. Let $x \in \mathcal{O}_L$. Then x is a unit if and only if $N_{L/\mathbb{Q}}(x) = \pm 1$.

Proof. ($\implies$) follows by the fact that $N_{L/\mathbb{Q}}(ab) = N_{L/\mathbb{Q}}(a)N_{L/\mathbb{Q}}(b)$ for all $a, b \in L$, and $N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathcal{O}_L$.

For the converse, let $\sigma_1, \dots, \sigma_n : L \to \mathbb{C}$ be the distinct field embeddings. Since $\mathbb{C}$ is algebraically closed, we can assume wlog that $L \leq \mathbb{C}$,and σ_1 is the inclusion map. If $x \in \mathcal{O}_L$, then

$$N_{L/\mathbb{Q}}(x) = x\sigma_2(x) \cdots \sigma_n(x)$$

so if $N_{L/\mathbb{Q}}(x) = \pm 1$, we get that

$$\frac{1}{x} = \pm \prod_{i=2}^{n} \sigma_i(x) \in \mathcal{O}_L$$

as the right hand side is a product of algebraic integers. □

2.1 Ideal operations

Definition 2.2 (product)
Let $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ be ideals, then we define their product to be

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

Proposition 2.3.

(i) $\mathfrak{a}\mathfrak{b}$ is an ideal in R,

(ii) $\langle a_1, \dots, a_n \rangle \langle b_1, \dots, b_m \rangle = \langle a_i b_j \mid 1 \le i \le n, 1 \le j \le m \rangle$,

(iii) $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$

Proof. Easy checks. □

Definition 2.4 (divides)
We say that $\mathfrak{b}$ divides $\mathfrak{a}$, written $\mathfrak{b} \mid \mathfrak{a}$, if there exists $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Lemma 2.5. If $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ is a nonzero ideal, then $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$, and $\mathcal{O}_L/\mathfrak{a}$ is a finite abelian group.

Proof. Let $\alpha \in \mathfrak{a}$ be nonzero, and let $p_\alpha(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be its minimal polynomial. As p_α is irreducible, $a_0 \neq 0$. Then we have that

$$a_0 = -\alpha(\alpha^{m-1} + a_{m-1}\alpha^{m-2} + \cdots + a_2\alpha + a_1) \in \mathfrak{a}$$

so $a_0 \in \mathfrak{a} \cap \mathbb{Z}$. Hence $a_0\mathcal{O}_L \le \mathfrak{a}$, so we have a map $\mathcal{O}_L/\langle a_0 \rangle \to \mathcal{O}_L/\mathfrak{a}$, which is a surjection. But for any $d \in \mathbb{Z}$, we have that $\mathcal{O}_L/\langle d \rangle = \mathbb{Z}^n/d\mathbb{Z}^n = (\mathbb{Z}/d\mathbb{Z})^n$ which is a finite abelian group, so $\mathcal{O}_L/\mathfrak{a}$ is also a finite abelian group. □

Proposition 2.6. Let L be a number field. Then

(i) $\mathcal{O}_L$ is an integral domain,

(ii) $\mathcal{O}_L$ is a Noetherian ring,

(iii) $\mathcal{O}_L$ is integrally closed in L, i.e. if $\alpha \in L$ is integral over $\mathcal{O}_L$, then $\alpha \in \mathcal{O}_L$,

(iv) every nonzero prime ideal in $\mathcal{O}_L$ is maximal.

That is, L is a Dedekind domain.

Proof. (i) is immediate since $\mathcal{O}_L$ is a subring of a field.

For (ii), we have shown that $\mathcal{O}_L \simeq \mathbb{Z}^n$ as abelian groups, so if $\mathfrak{a}$ is an ideal in $\mathcal{O}_L$, then $\mathfrak{a}$ is isomorphic to a subgroup of $\mathbb{Z}^n$, so it is finitely generated as an abelian group, hence it is finitely generated as an ideal.

For (iii), if $\alpha \in L$ is integral over $\mathcal{O}_L$, as $\mathcal{O}_L$ is integral over $\mathbb{Z}$, α is integral over $\mathbb{Z}$. But this means that $\alpha \in \mathcal{O}_L$.

For (iv), if $\mathfrak{p} \trianglelefteq \mathcal{O}_L$ is a nonzero prime ideal, then by the previous lemma, $\mathcal{O}_L/\mathfrak{p}$ is a finite integral domain, so it is a field. Hence $\mathfrak{p}$ is maximal. □

Corollary 2.7. If $\mathfrak{a}$ is a nonzero ideal, then $\mathfrak{a} \simeq \mathbb{Z}^n$ as abelian groups.

Lemma 2.8. Let $\mathfrak{p}$ be a prime ideal in R, $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$. Then $\mathfrak{a}\mathfrak{b} \leq \mathfrak{p}$ implies that $\mathfrak{a} \leq \mathfrak{p}$ or $\mathfrak{b} \leq \mathfrak{p}$.

Proof. Easy proof by contradiction. □

Lemma 2.9. If $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ is a nonzero ideal, then $\mathfrak{a}$ contains a product of prime ideals.

Proof. Suppose not. Then as $\mathcal{O}_L$ is Noetherian, there exists an ideal $\mathfrak{a}$ such that if $\mathfrak{b}$ is any ideal with $\mathfrak{a} < \mathfrak{b}$, then $\mathfrak{b}$ contains a product of prime ideals. In particular, $\mathfrak{a}$ cannot be prime. Choose $x, y \in \mathcal{O}_L$ such that $x, y \notin \mathfrak{a}$, $xy \in \mathfrak{a}$. Since $\mathfrak{a} < \mathfrak{a} + \langle x \rangle$ and $\mathfrak{a} < \mathfrak{a} + \langle y \rangle$, there exists prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a} + \langle x \rangle$, and $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{a} + \langle y \rangle$. Then we have that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \leq (\mathfrak{a} + \langle x \rangle)(\mathfrak{a} + \langle y \rangle) \leq \mathfrak{a}$$

Contradiction. □

Lemma 2.10. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ be a nonzero ideal, $x \in L$ such that $x\mathfrak{a} \subseteq \mathfrak{a}$. Then $x \in \mathcal{O}_L$.

Proof. Since $\mathfrak{a}$ is a finitely generated abelian group, choose a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ for $\mathfrak{a}$. Then consider the map $m_x : \mathfrak{a} \to \mathfrak{a}$, $\alpha \mapsto x\alpha$. Writing $x\alpha_i = \sum_j a_{ij}\alpha_j$, with $a_{ij} \in \mathbb{Z}$, and letting $A = (a_{ij})$, we find that

$$(xI - A)\begin{pmatrix} \alpha_1, \\ \vdots \\ \alpha_n \end{pmatrix} = 0$$

which means that $\det(xI - A) = 0$, so x is integral over $\mathbb{Z}$, hence $x \in \mathcal{O}_L$. □

2.2 Fractional ideals and unique factorisation of ideals

Lemma 2.11. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$, with $\mathfrak{a} \neq 0, \mathcal{O}_L$. Then

$$\mathcal{O}_L \subsetneq \{y \in L \mid y\mathfrak{a} \subseteq \mathcal{O}_L\}$$

Proof. First of all, note that if this is true for an ideal $\mathfrak{a}$, then it is true for all $\mathfrak{b} \leq \mathfrak{a}$. So wlog we can assume that $\mathfrak{a}$ i.e. $\mathfrak{a} = \mathfrak{p}$ prime.

Let $\alpha \in \mathfrak{p}$ be nonzero. Then we have prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ such that $\mathfrak{q}_1 \cdots \mathfrak{q}_r \leq \alpha\mathcal{O}_L$. Suppose r is minimal. Then as $\mathfrak{p}$ is prime, there exists i such that $\mathfrak{q}_i \leq \mathfrak{p}$. wlog $i = 1$. As $\mathfrak{q}_1$ is prime, it is maximal. So $\mathfrak{q}_1 = \mathfrak{p}$. By minimality of r, we must have that $\mathfrak{q}_2 \cdots \mathfrak{q}_r \nsubseteq \alpha\mathcal{O}_L$. Choose $\beta \in \mathfrak{q}_2 \cdots \mathfrak{q}_r \setminus \alpha\mathcal{O}_L$. Then $\beta\mathfrak{p} \leq \mathfrak{p}(\mathfrak{q}_2 \cdots \mathfrak{q}_r) \leq \alpha\mathcal{O}_L$, but $\beta \notin \alpha\mathcal{O}_L$. Dividing by α, we get that

$$\frac{\beta}{\alpha}\mathfrak{p} \subseteq \mathcal{O}_L \quad \text{and} \quad \frac{\beta}{\alpha} \notin \mathcal{O}_L$$

□

Definition 2.12 (fractional ideal)
A fractional ideal in L is a finitely generated $\mathcal{O}_L$ submodule of L.

Lemma 2.13. $\mathfrak{q} \subseteq L$ is a fractional ideal if and only if there exists $c \in L$ such that $c\mathfrak{q} \subseteq \mathcal{O}_L$ is an ideal.

Proof. For ($\Longleftarrow$) notice that $c\mathfrak{q} \simeq \mathfrak{q}$ as $\mathcal{O}_L$ modules. Conversely, let $x_1, \dots, x_r$ generate $\mathfrak{q}$ as an $\mathcal{O}_L$ module. Then $x_i = y_i/n_i$, where $y_i \in \mathcal{O}_L$ and $n_i \in \mathbb{Z}$. Let $c = \operatorname{lcm}(n_1, \dots, n_r)$. Then $c\mathfrak{q} \subseteq \mathcal{O}_L$ and is an $\mathcal{O}_L$ submodule. So it is an ideal. □

Corollary 2.14. If $\mathfrak{q}$ is a fractional ideal, then $\mathfrak{q} \simeq \mathbb{Z}^n$ as abelian groups, where $n = [L : \mathbb{Q}]$.

We define multiplication of fractional ideals in the same way we defined multiplication of ideals.

Definition 2.15 (invertible)
A fractional ideal $\mathfrak{q}$ is invertible if there exists a fractional ideal $\mathfrak{r}$ such that $\mathfrak{q}\mathfrak{r} = \mathcal{O}_L$.

Proposition 2.16. Every nonzero fractional $\mathfrak{q}$ is invertible with

$$\mathfrak{q}^{-1} = \{x \in L \mid x\mathfrak{q} \subseteq \mathcal{O}_L\}$$

Equivalently, for every $\mathfrak{a} \trianglelefteq \mathcal{O}_L$, there exists an ideal $\mathfrak{b} \trianglelefteq \mathcal{O}_L$ such that $\mathfrak{a}\mathfrak{b}$ is principal.

Proof. First we show the equivalence. If $\mathfrak{q}, \mathfrak{r}$ are fractional ideals, then we have $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_L$, $m, n \in L^\times$, such that $\mathfrak{q} = \frac{1}{m}\mathfrak{a}$ and $\mathfrak{r} = \frac{1}{n}\mathfrak{b}$. Then

$$\mathfrak{q}\mathfrak{r} = \mathcal{O}_L \iff \mathfrak{a}\mathfrak{b} = mn\mathcal{O}_L$$

Now notice that $\mathfrak{q}$ is invertible if and only if $\mathfrak{a}$ is, so wlog we can assume $\mathfrak{q} \trianglelefteq \mathcal{O}_L$. Hence if the result is false, it is false for some ideal $\mathfrak{a}$ in $\mathcal{O}_L$. As $\mathcal{O}_L$ is Noetherian, we can assume that if $\mathfrak{a} < \mathfrak{a}'$, then $\mathfrak{a}'$ is invertible.

Let $\mathfrak{b} = \{x \in L \mid x\mathfrak{a} \subseteq \mathcal{O}_L\}$. Then $\mathfrak{b}$ is a fractional ideal, with $\mathcal{O}_L \subsetneq \mathfrak{b}$. Hence we have that $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{b}$. Again this inclusion is strict, since if $\mathfrak{a}\mathfrak{b} = \mathfrak{a}$, then for all $x \in \mathfrak{b}$, $x\mathfrak{a} \subseteq \mathfrak{a}$, so $x \in \mathcal{O}_L$. But $\mathfrak{b} \not\subseteq \mathcal{O}_L$. Hence $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{b}$, so $\mathfrak{a}\mathfrak{b}$ is invertible. Let $\mathfrak{c}$ be the inverse of $\mathfrak{a}\mathfrak{b}$. Then $\mathfrak{b}\mathfrak{c}$ is the inverse to $\mathfrak{a}$. But we assumed $\mathfrak{a}$ was not invertible. Contradiction.

Hence we must have that all fractional ideals are invertible. Finally, let $\mathfrak{c} = \{x \in L \mid x\mathfrak{q} \subseteq \mathcal{O}_L\}$. Then by definition, we have that $q^{-1} \subseteq \mathfrak{c}$, and

$$\mathcal{O}_L = \mathfrak{q}\mathfrak{q}^{-1} \subseteq \mathfrak{q}\mathfrak{c} \subseteq \mathcal{O}_L$$

so we must have that $\mathfrak{q}\mathfrak{c} = \mathcal{O}_L$, so $\mathfrak{c} = \mathfrak{q}^{-1}$. □

Corollary 2.17. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \trianglelefteq \mathcal{O}_L$, with $\mathfrak{c} \neq 0$. Then

(i) $\mathfrak{b} \subseteq \mathfrak{a} \iff \mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}\mathfrak{c}$,

(ii) $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{a}\mathfrak{c} \mid \mathfrak{b}\mathfrak{c}$,

(iii) $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a}$.

Proof. For (i) and (ii), ($\Longrightarrow$) follows by multiplying by $\mathfrak{c}$, and ($\Longleftarrow$) follows by multiplying by $\mathfrak{c}^{-1}$.

For (iii), ($\Longrightarrow$) is clear by definition of $\mid$ and ideal multiplication. For the converse, there exists $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c} = \alpha\mathcal{O}_L$ principal. Then by (i) and (ii), we see that $\mathfrak{b} \subseteq \mathfrak{a} \iff \mathfrak{b}\mathfrak{c} \subseteq \alpha\mathcal{O}_L$, and $\mathfrak{a} \mid \mathfrak{b} \iff \alpha\mathcal{O}_L \mid \mathfrak{b}\mathfrak{c}$. But if $\mathfrak{b}\mathfrak{c} = \langle \beta_1, \dots, \beta_r \rangle$, then $\mathfrak{b}\mathfrak{c} \subseteq \alpha\mathcal{O}_L$ implies that we can write $\beta_i = \gamma_i\alpha$, where $\gamma_i \in \mathcal{O}_L$. So we have that

$$\mathfrak{bc} = \langle \beta_1, \dots, \beta_r \rangle = \langle \beta_1, \dots, \beta_r \rangle \cdot \alpha \mathcal{O}_L$$

□

Theorem 2.18. Let $\mathfrak{a}$ be a nonzero ideal. Then $\mathfrak{a}$ can be written uniquely as a product of prime ideals.

Proof. **Existence:** If $\mathfrak{a}$ is not prime, then it is not maximal. So there exists a proper ideal $\mathfrak{b} \trianglelefteq \mathcal{O}_L$ such that $\mathfrak{a} < \mathfrak{b}$. So $\mathfrak{b} \mid \mathfrak{a}$, and we have that $\mathfrak{a} = \mathfrak{bc}$ for some $\mathfrak{c}$. So $\mathfrak{a} \subseteq \mathfrak{c}$, and as ascending chains of ideals are finite, this must terminate.

Uniqueness: The same proof as in the integers works. □

2.3 Class group

Corollary 2.19. The nonzero fractional ideals form a group under multiplication, which we will denote I_L. It is the free abelian group generated by the prime ideals $\mathfrak{p} \trianglelefteq \mathcal{O}_L$.

That is, any $\mathfrak{q} \in I_L$ can be written uniquely as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, and $\mathfrak{q}$ is an ideal if and only if all $e_i \geq 0$.

Proposition 2.20. The map $L^\times \to I_L$, given by $\alpha \mapsto \alpha \mathcal{O}_L$ defines a group homomorphism, with kernel $\mathcal{O}_L^\times$, and image the principal ideals. We denote the set of principal ideals in I_L by P_L.

Definition 2.21 (class group)

The class group of a number field L is

$$\mathrm{Cl}(L) = \frac{I_L}{P_L}$$

for $\mathfrak{a} \in I_L$, we write $[\mathfrak{a}]$ for its class in $\mathrm{Cl}(L)$. So $[\mathfrak{a}] = [\mathfrak{b}]$ if and only if $\gamma \in L^\times$ such that $\gamma \mathfrak{a} = \mathfrak{b}$.

Theorem 2.22. The following are equivalent.

(i) $\mathcal{O}_L$ is a PID,

(ii) $\mathcal{O}_L$ is a UFD,

(iii) $\mathrm{Cl}(L) = 1$

Proof. (i) $\iff$ (iii) is true by definition, and (i) $\implies$ (ii) follow from GRM. Now suppose (ii) holds. Let $\mathfrak{p}$ be a prime ideal, $x \in \mathfrak{p} \setminus 0$. Then $x = \alpha_1 \cdots \alpha_r$, where each $\alpha_i \in \mathcal{O}_L$ is irreducible. As $\mathfrak{p}$ is prime, some $\alpha_i \in \mathfrak{p}$, so $\langle \alpha_i \rangle \subseteq \mathfrak{p}$. As $\mathcal{O}_L$ is a UFD, α_i irreducible, $\langle \alpha_i \rangle$ is prime. So $\langle \alpha_i \rangle$ is maximal, and $\mathfrak{p} = \langle \alpha_i \rangle$ is principal. □

Proposition 2.23. We have an exact sequence

$$1 \longrightarrow \mathcal{O}_L^\times \hookrightarrow L^\times \xrightarrow{x \mapsto x\mathcal{O}_L} I_L \twoheadrightarrow \mathrm{Cl}(L) \longrightarrow 1$$

Proof. The class group is precisely the cokernel. □

2.4 Ideal norm

Definition 2.24 (ideal norm)
Let L be a number field, $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ nonzero, then define

$$N(\mathfrak{a}) = \left| \frac{\mathcal{O}_L}{\mathfrak{a}} \right|$$

which is finite.

Proposition 2.25. $N(\mathfrak{a}) \in \mathfrak{a} \cap \mathbb{Z}$.

Proof. By Lagrange's theorem $N(\mathfrak{a}) \cdot 1 = 0$ in $\mathcal{O}_L/\mathfrak{a}$. □

Proposition 2.26. Let $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_L$, then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Proof. **Step 1: Reduction and definition of ϕ** By prime factorisation of ideals, it suffices to show the result for $\mathfrak{b} = \mathfrak{p}$ prime. By unique factoriation, $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}$, so choose $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}$. Then we can define a map $\phi : \mathcal{O}_L/\mathfrak{p} \to \mathfrak{a}/\mathfrak{a}\mathfrak{p}$ by $\phi(x \mod \mathfrak{p}) = \alpha x \mod \mathfrak{a}\mathfrak{p}$.

Step 2: ϕ is well defined. First of all, as $x \in \mathcal{O}_L$, and $\mathfrak{a}$ is an ideal, $\alpha x \in \mathfrak{a}$. Next, if $x \mod \mathfrak{p} = y \mod \mathfrak{p}$, then there exists $p \in \mathfrak{p}$ such that $x = y + p$. Then $\alpha x \mod \mathfrak{p} = (\alpha y + \alpha p) \mod \mathfrak{p} = \alpha y \mod \mathfrak{p}$, since $\alpha \in \mathfrak{a}, p \in \mathfrak{p}$. So ϕ is well defined.

Step 3: ϕ is injective. As $\langle \alpha \rangle \leq \mathfrak{a}$, $\langle \alpha \rangle = \mathfrak{a}\mathfrak{c}$ for some ideal $\mathfrak{c}$. Now suppose x is such that $\alpha x \in \mathfrak{a}\mathfrak{p}$, i.e. $x \mod \mathfrak{p} \in \ker(\phi)$. Then we have that $\langle x\alpha \rangle = x \langle \alpha \rangle = x\mathfrak{a}\mathfrak{c} \leq \mathfrak{a}\mathfrak{p}$, so $x\mathfrak{c} \leq \mathfrak{p}$. But $\mathfrak{p}$ is prime, so either $\mathfrak{c} \leq \mathfrak{p}$, or $x \in \mathfrak{p}$. But $c \leq \mathfrak{p}$ implies that $\alpha \in \mathfrak{a}\mathfrak{p}$. Contradiction. So $x \in \mathfrak{p}$, so $x \mod \mathfrak{p} = 0 \mod \mathfrak{p}$. Hence $\ker(\phi) = 0$, so ϕ is injective.

Step 4: ϕ is surjective. We have that $\mathfrak{a}\mathfrak{p} \subsetneq \langle \alpha \rangle + \mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a}$. Multiplying by $\mathfrak{a}^{-1}$, we get that $\mathfrak{p} \subsetneq \mathfrak{a}^{-1} \langle \alpha \rangle + \mathfrak{p} \leq \mathcal{O}_L$. But $\mathfrak{p}$ is prime, so it is maximal. Hence we must have that $\langle \alpha \rangle + \mathfrak{a}\mathfrak{p} = \mathfrak{a}$. So ϕ is surjective.

Step 5: Conclusion. By the third isomorphism theorem, we have that

$$N(\mathfrak{a}) = \left| \frac{\mathcal{O}_L}{\mathfrak{a}} \right| = \left| \frac{\mathcal{O}_L/\mathfrak{a}\mathfrak{p}}{\mathfrak{a}/\mathfrak{a}\mathfrak{p}} \right| = \frac{N(\mathfrak{a}\mathfrak{p})}{N(\mathfrak{p})}$$

since ϕ is an isomorphism, so $|\mathfrak{a}/\mathfrak{a}\mathfrak{p}| = |\mathcal{O}_L/\mathfrak{p}|$. □

Lemma 2.27. Let $M \leq \mathbb{Z}^n$ be a subgroup. Then $M \simeq \mathbb{Z}^r$ for some $0 \leq r \leq n$. Moreover, if $r = n$, then there exists a basis $v_1, \ldots, v_n$ of M, such that if $v_j = \sum_i a_{ij} e_i$, with $e_1, \ldots, e_n$ the standard basis of $\mathbb{Z}^n$, then $A = (a_{ij}$ is upper triangular. In particular, $|\mathbb{Z}^n/M| = |a_{11} \cdots a_{nn}| = |\det(A)|$.

Proof. See GRM for most of it. To see that we can choose A upper triangular, notice that if we use an algorithm like Smith normal form, but only use row operations, then we can write $A = LU$, where U is upper triangular, L is invertible. So L corresponds to a change of basis for M. □

Lemma 2.28. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ be a nonzero ideal, $n = [L : \mathbb{Q}]$, then

(i) there exists $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$ such that

$$\mathfrak{a} = \left\{ \sum r_i \alpha_i \mid r_i \in \mathbb{Z} \right\} = \bigoplus_i \mathbb{Z}\alpha_i$$

and $\alpha_1, \ldots, \alpha_n$ is a basis of $L/\mathbb{Q}$.

(ii) for any such $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$,

$$\Delta(\alpha_1, \ldots, \alpha_n) = N(\mathfrak{a})^2 D_L$$

Proof. (i) We've shown $\mathcal{O}_L$ has an integral basis. Choose $d \in \mathfrak{a} \cap \mathbb{Z}$, for example $d = N(\mathfrak{a})$. Thne $d\mathcal{O}_L \le \mathfrak{a} \le \mathcal{O}_L$, so as abelian groups, we have

$$(d\mathbb{Z})^n \le \mathfrak{a} \le \mathbb{Z}^n$$

so $\mathfrak{a} \simeq \mathbb{Z}^n$ as a submodule of a free module is free, and so (i) follows.

(ii) Now let $\alpha'_1, \dots, \alpha'_n$ be an integral basis for $\mathcal{O}_L$, and A be the matrix expressing the basis $\alpha_1, \dots, \alpha_N$ for $\mathfrak{a}$ in terms of the α'_i. Then we have that

$$\Delta(\alpha_1, \dots, \alpha_n) = (\det(A))^2 \Delta(\alpha'_1, \dots, \alpha'_n)$$

But the previous lemma gives us that $|\det(A)| = |\mathcal{O}_L/\mathfrak{a}|$[1], and $D_L = \Delta(\alpha'_1, \dots, \alpha'_n)$ by definition. □

Corollary 2.29. If $\alpha_1, \dots, \alpha_n$ is a basis for $\mathfrak{a}$ such that $\Delta(\alpha_1, \dots, \alpha_n)$ is squarefree, then $\mathfrak{a} = \mathcal{O}_L$ and D_L is squarefree.

Corollary 2.30. Let $L = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_L$ with minimal polynomial p_α over $\mathbb{Q}$. Let d be the largest integer such that $d^2 \mid \mathrm{Disc}(p_\alpha) = \Delta(1, \alpha, \dots, \alpha^{n-1})$. Then

$$|\mathcal{O}_L/\mathbb{Z}[\alpha]| \mid d \quad \text{and} \quad \mathbb{Z}[\alpha] \le \mathcal{O}_L \le \frac{1}{d}\mathbb{Z}[\alpha]$$

Proof. Omitted. □

Lemma 2.31. If $\alpha \in \mathcal{O}_L$ is nonzero, then $N(\langle \alpha \rangle) = |N_{L/\mathbb{Q}}(\alpha)|$.

Proof. Let $\alpha_1, \dots, \alpha_n$ be an integral basis for $\mathcal{O}_L$, so $\alpha\alpha_1, \dots, \alpha\alpha_n$ is an integral basis for $\langle \alpha \rangle$. Then

$$\Delta(\alpha\alpha_1, \dots, \alpha\alpha_n) = \det\big(\sigma_i(\alpha\alpha_j)\big)^2 = \det\big(\sigma_i(\alpha)\sigma_i(\alpha_j)\big)^2 = \left(\prod_i \sigma_i(\alpha)\right)^2 \Delta(\alpha_1, \dots, \alpha_n) = N_{L/\mathbb{Q}}(\alpha)^2 D_L$$

□

2.5 Dedekind's Criterion

Lemma 2.32. Given $\mathfrak{p} \trianglelefteq \mathcal{O}_L$ a nonzero prime ideal, then there exists a unique prine $p \in \mathbb{Z}$ such that $\mathfrak{p} \mid p\mathcal{O}_L$. Moreover, $N(\mathfrak{p}) = p^f$ for some $1 \le f \le n = [L : \mathbb{Q}]$.

Proof. $\mathfrak{p} \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$, so it is principal. Say $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We will show p is prime. If $p = ab$, then as $p \in \mathfrak{p}$, either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. So $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. So p is prime. Now write $\langle p \rangle = \mathfrak{p}\mathfrak{a}$ by ideal factorisation, and we find that

$$p^n = N(\langle p \rangle) = N(\mathfrak{p})N\mathfrak{a} \implies N(\mathfrak{p}) = p^f$$

□

Definition 2.33 (ramification indices)

For a prime $p \in \mathbb{Z}$, write $\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, with the $\mathfrak{p}_i$ distinct prime ideals. We call the $e_1, \dots, e_r$ the ramification indices of p.

[1] In the previous lemma, we have that $A = LU$ so we could assume A was upper triangular. But $L \in \mathrm{GL}_n(\mathbb{Z})$, so $|\det(L)| = 1$, and the result holds for *any* basis for M and the corresponding change of basis matrix A.

Definition 2.34 (ramifies, inert, splits (completely))
Let $p \in \mathbb{Z}$ be prime, with

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

Then we say that

(i) p ramifies in L if there exists i with $e_i > 1$,

(ii) p is inert in L if $\langle p \rangle$ is prime,

(iii) p splits (completely)in L if $r = n$, $e_1 = \cdots = e_n = 1$.

Theorem 2.35 (Dedekind's criterion)**.** Let $\alpha \in \mathcal{O}_L$, with minimal polynomial $g(x) \in \mathbb{Z}[x]$. Suppose $\mathbb{Z}[\alpha] \leq \mathcal{O}_L$ has finite index coprime to p. Then let $\overline{g}(x) = g(x) \mod p \in \mathbb{F}_p[x]$. Say

$$\overline{g}(x) = \overline{\phi_1}^{e_1} \cdots \overline{\phi_r}^{e_r}$$

be the factorisation of $\overline{g}$ into irreducibles in $\mathbb{F}_p[x]$. Then

$$\langle p \rangle = p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

where $\mathfrak{p}_i = \langle p, \phi_i(\alpha) \rangle$, where $\phi_i(x) \in \mathbb{Z}[x]$ is such that $\phi_i \mod p = \overline{\phi_i}$. Moreover, the $\mathfrak{p}_i$ are distinct.

Proof. **Part 1: Each ϕ_i defines a prime ideal in $\mathbb{Z}[\alpha]$ containing p.** Consider the following diagram

$$\begin{array}{ccc} \mathbb{Z}[x] & \overset{e}{\twoheadrightarrow} & \mathbb{Z}[\alpha] = \mathbb{Z}[x]/g\mathbb{Z}[x] \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle m'} \\ \mathbb{F}_p[x] & \underset{e'}{\twoheadrightarrow} & \mathbb{F}_p[x]/\overline{\phi_i}\mathbb{F}_p[x] \end{array}$$

where e, e' are the quotient maps, m is the map given by reduction $\mod p$, and $m'(f \mod g) = \overline{f} \mod \overline{\phi_i}$. Note that m' is well defined since $\overline{\phi_i} \mid \overline{g}$.

Step 1: $\ker(e' \circ m) = p\mathbb{Z}[x] + \phi_i\mathbb{Z}[x]$. $\supseteq$ is clear. Now suppose $f \in \mathbb{Z}[x]$, with $e'(m(f)) = 0$. That is, $\overline{f} \mod \overline{\phi_i} = 0$. So $\overline{f} = \overline{h\phi_i}$ for some $\overline{h} \in \mathbb{F}_p[x]$. But then this means that $f = h\phi_i + p \cdot (\text{stuff})$. So $\subseteq$ holds.

Step 2: $\ker(m') = p\mathbb{Z}[\alpha] + \phi_i(\alpha)\mathbb{Z}[\alpha]$. As e is a surjection, we have that

$$\ker(m') = e(e^{-1}(\ker(m'))) = e(\ker(m' \circ e)) = e(\ker(e' \circ m)) = e(p\mathbb{Z}[x] + \phi_i\mathbb{Z}[x]) = p\mathbb{Z}[\alpha] + \phi_i(\alpha)\mathbb{Z}[\alpha]$$

Step 3: Defining the prime ideal. Let $\mathfrak{q}_i = p\mathbb{Z}[\alpha] + \phi_i(\alpha)\mathbb{Z}[\alpha] = \ker(m')$. Then by the isomorphism theorem, we have that

$$\frac{\mathbb{Z}[\alpha]}{\mathfrak{q}_i} \simeq \frac{\mathbb{F}_p[x]}{\overline{\phi_i}\mathbb{F}_p[x]}$$

But $\overline{\phi}_i$ is irreducible, so $\mathbb{F}_p[x]/\overline{\phi_i}\mathbb{F}_p[x]$ is a field. Hence $\mathfrak{q}_i$ is a prime ideal. Furthermore, $\mathbb{F}_p[x]/\overline{\phi_i}\mathbb{F}_p[x]$ is a characteristic p finite field, so $|\mathbb{Z}[\alpha]/\mathfrak{q}_i| = p^{f_i}$, where $f^i = \deg(\overline{\phi_i})$.

Part 2: Using the correspondence theorem to define a ideals in $\mathcal{O}_L$.

Step 1: The inclusion map induces an isomorphism $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \mathcal{O}_L/p\mathcal{O}_L$. Since $p \not| |\mathcal{O}_L/\mathbb{Z}[\alpha]|$, the map $m_p : \mathcal{O}_L/\mathbb{Z}[\alpha] \to \mathcal{O}_L/\mathbb{Z}[\alpha]$, given by $m_p(x) = px$ is an injective homomorphism (of additive groups), so it is an isomorphism. But

$$\ker\left(\frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]} \to \frac{\mathcal{O}_L}{p\mathcal{O}_L}\right) = \frac{\mathbb{Z}[\alpha] \cap p\mathcal{O}_L}{p\mathbb{Z}[\alpha]} = \ker(m_p)$$

and

$$\frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]} \to \frac{\mathcal{O}_L}{p\mathcal{O}_L} \text{ surjective} \iff \mathcal{O}_L = \mathbb{Z}[\alpha] + p\mathcal{O}_L \iff m_p \text{ is surjective.}$$

Step 2: Correspondence theorem. Now consider the diagram

$$\begin{array}{ccc} \left\{\text{ideals in } \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}\right\} & \longleftrightarrow & \left\{\text{ideals in } \frac{\mathcal{O}_L}{p\mathcal{O}_L}\right\} \\ \updownarrow & & \updownarrow \\ \{\text{ideals in } \mathbb{Z}[\alpha] \text{ containing } p\} & \xrightarrow{\Psi} & \{\text{ideals in } \mathcal{O}_L \text{ containing } p\} \end{array}$$

where the vertical bijections are induced by the correspondence theorem, and the top bijection is induced by the isomorphism from step 1. In particular, note that the composite bijection gives $\Psi(\mathfrak{q}) = \mathfrak{q}\mathcal{O}_L$, and $\psi^{-1}(\mathfrak{p}) = \mathfrak{p} \cap \mathbb{Z}[\alpha]$. Furthemore, this bijection takes prime ideals to prime ideals. Finally,

$$\frac{\mathcal{O}_L}{\mathfrak{p}} \simeq \frac{\mathbb{Z}[\alpha]}{\mathfrak{p} \cap \mathbb{Z}[\alpha]}$$

which means that if we define $\mathfrak{p}_i = \mathfrak{q}_i\mathcal{O}_L$, then $N(\mathfrak{p}_i) = p^{f_i}$ as required.

Part 3: $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, and the $\mathfrak{p}_i$ are distinct.

First notice that $\mathfrak{p}_i^{e_i} = \langle p, \phi_i(\alpha)\rangle^{e_i} \leq \langle p, \phi_i(\alpha)^{e_i}\rangle$, so we have that

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \leq \langle p, \phi_1(\alpha)^{e_1} \cdots \phi_r(\alpha)^{e_r}\rangle = \langle p, g(\alpha)\rangle$$

since $\phi_1^{e_1} \cdots \phi_r^{e_r} \equiv g \pmod p$. But $g(\alpha) = 0$, so $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \leq \langle p\rangle$. Taking norms, and using the fact that $\sum e_i f_i = n$, we get that equality holds.

Finally, if i, j distinct, then $\overline{\phi_i}, \overline{\phi_j}$ are coprime in $\mathbb{F}_p[x]$, so $\mathfrak{p}_i + \mathfrak{p}_j = \big\langle p, \phi_i(\alpha), \phi_j(\alpha)\big\rangle \neq \mathfrak{p}_i$, so the $\mathfrak{p}_i$ are distinct. □

Corollary 2.36. If p is prime, $p < n = [L : \mathbb{Q}]$, $|\mathcal{O}_L/\mathbb{Z}[\alpha]|$ coprime to p, then p does not split completely.

Proof. Let g be the minimal polynomial of α. But $\deg(g) = n > p$, so $\overline{g}$ can't have distinct roots. □

Finally, two theorems which we do not prove.

Theorem 2.37. With the notation as in (the proof for) Dedekind's criterion, we find that

$$\frac{\mathcal{O}_L}{\mathfrak{p}_i} \simeq \frac{\mathbb{F}_p[x]}{\overline{\phi_i}} \simeq \mathbb{F}_p^{f_i}$$

and

$$\frac{\mathcal{O}_L}{p\mathcal{O}_L} = \bigoplus_{i=1}^{r} \frac{\mathbb{F}_p[x]}{\overline{\phi_i}^{e_i}} \simeq \bigoplus_{i=1}^{r} \frac{\mathbb{F}_{p^{f_i}}[t]}{(t^{e_i})}$$

Theorem 2.38. p ramifies in $\mathcal{O}_L$ if and only if $p \mid D_L$.

3 Geometry of numbers

3.1 Minkowski's lemma

Proposition 3.1. Let $\Lambda \leq \mathbb{R}^n$ be a subgroup. Then the following are equivalent.

(i) Λ is a discrete subgroup of $\mathbb{R}^n$,

(ii) for any $K \subseteq \mathbb{R}^n$ compact, $K \cap \Lambda$ is finite,

(iii) there exists $\varepsilon > 0$ such that $B_\varepsilon(0) \cap \Lambda = \{0\}$,

(iv)
$$\Lambda = \bigoplus_{i=1}^{m} \mathbb{Z}x_i$$
where the x_i are $\mathbb{R}$-linearly independent.

Proof. (i) $\implies$ (iii) follows from the definition of discrete, and (iii) $\implies$ (i) follows from the fact that for every $x \in \Lambda$,

$$B_\varepsilon(x) \cap \Lambda = B_\varepsilon(0) \cap \Lambda + x = \{x\} \tag{*}$$

as Λ is a subgroup.

For (iii) $\implies$ (ii), notice that by compactness,

$$K \subseteq \bigcup_{x \in K} B_{\varepsilon/2}(x) \implies K \subseteq \bigcup_{i=1}^{r} B_{\varepsilon/2}(x_i)$$

and each $B_{\varepsilon/2}(x_i)$ contains at most one element of Λ, by (*). Therefore $K \cap \Lambda$ is finite. Now suppose (iii) doesn't hold. Then we can choose $(x_n) \subseteq \Lambda$ such that $|x_1| < 1$, and $|x_{n+1}| < |x_n|$. So $\overline{B}_1(0) \cap \Lambda$ is finite. Contradiction.

Now suppose (iv) holds. Notice that properties (i)-(v) are all preserved under the action of $g \in \mathrm{GL}_n(\mathbb{R})$. So we can assume without loss of generality that $\Lambda = \mathbb{Z}^m \times 0 \leq \mathbb{R}^m \times \mathbb{R}^{n-m}$, which is clearly discrete.

Finally, suppose (ii) holds. Choose a maximal $\mathbb{R}$-linearly independent subset $y_1, \ldots, y_m$ of Λ. Clearly $m \leq n$, and

$$V = \mathrm{span}\{y_1, \ldots, y_m\} = \mathrm{span}\{\Lambda\}$$

Now let $X = \{\sum_i \lambda_i y_i \mid \lambda_i \in [0,1]\}$, which is a closed bounded subset of $\mathbb{R}^n$, so it is compact. Hence $\Lambda \cap X$ is finite. But we have that $\Lambda \subseteq \bigoplus \mathbb{Z}y_i + X \cap \Lambda$, which means that $|\Lambda / \bigoplus_i \mathbb{Z}y_i| \leq |X \cap \Lambda| < \infty$.

Therefore, if $d = |\Lambda / \bigoplus_i \mathbb{Z}y_i|$, then $d\Lambda \leq \bigoplus \mathbb{Z}y_i$ by Lagrange's theorem, so $\Lambda \subseteq \frac{1}{d} \bigoplus_i \mathbb{Z}y_i$. But then this means that

$$\bigoplus_i \mathbb{Z}y_i \leq \Lambda \leq \frac{1}{d} \bigoplus_i \mathbb{Z}y_i$$

So by the structure theorem for abelian groups, there exists $x_1, \ldots, x_m \in \Lambda$ with $\Lambda = \bigoplus_i \mathbb{Z}x_i$. □

Definition 3.2 (lattice)

A subgroup $\Lambda \leq \mathbb{R}^n$ is called a lattice of $m = n$ in (iv) above.

Definition 3.3 (fundamental domain, covoloume)

Let $\Lambda \leq \mathbb{R}^n$ be a lattice with basis $x_1, \ldots, x_n$. Define

(i) the fundamental fomain
$$P = \left\{ \sum_{i=1}^{n} \lambda_i x_i \mid \lambda_i \in [0,1] \right\}$$

(ii) the covolume of Λ is

$$\mathrm{covol}(\Lambda) = \mathrm{vol}(P) = |\det(A)|$$

where $x_i = \sum_j a_{ij} e_j$, $A = (a_{ij})$.

Proposition 3.4. $\mathrm{covol}(\Lambda)$ is independent of the choice of basis.

Proof. For any $g \in \mathrm{GL}_n(\mathbb{Z})$, $|\det(g)| = 1$. □

Theorem 3.5 (Minkowski's lemma)**.** Let $\Lambda \leq \mathbb{R}^n$ be a lattice, P a fundamental domain, $S \subseteq \mathbb{R}^n$ be measurable. Then

(i) suppose $\mathrm{vol}(S) > \mathrm{covol}(\Lambda)$. Then there exists distinct $x, y \in S$ such that $x - y \in \Lambda$,

(ii) suppose S is symmetric about zero, convex, and either

(a) $\mathrm{vol}(S) > 2^n \, \mathrm{covol}(\Lambda)$,

(b) or $\mathrm{vol}(S) \geq 2^n \, \mathrm{covol}(\Lambda)$ and S is closed,

Then there exists an element $\gamma \in S \cap \Lambda$ with $\gamma \neq 0$.

Proof. (i) We have that $\mathrm{vol}(S) = \sum_{\gamma \in \Lambda} \mathrm{vol}(S \cap (P + \gamma))$ as P is a fundamental domain and volume (i.e. Lebesgue measure) is countably additive, and in the intersections, $\mathrm{vol}(\partial P) = 0$. Sinve the Lebesgue measure is translation invariant, $\mathrm{vol}(S \cap (P + \gamma)) = \mathrm{vol}((S - \gamma) \cap P)$.

Suppose for contradiction that the sets $(S - \gamma) \cap P$ are pairwise disjoint. Then

$$\mathrm{vol}(P) \geq \sum_{\gamma \in \Lambda} \mathrm{vol}((S - \gamma) \cap P) = \sum_{\gamma \in \Lambda} \mathrm{vol}(S \cap (P + \gamma)) = \mathrm{vol}(S)$$

Contradiction. Therefore, there exists $\lambda, \mu \in \Lambda$ distinct such that $(S - \gamma) \cap (S - \mu) \cap P \neq \varnothing$. That is, there exists $x, y \in S$ such that $x - \gamma = y - \mu$, so $x - y = \gamma - \mu \in \Lambda$.

(ii) (a) Suppose $\mathrm{vol}(S) > 2^n \, \mathrm{covol}(\Lambda)$. Let $S' = \frac{1}{2} S$, so $\mathrm{vol}(S') > \mathrm{covol}(\Lambda)$. Hence by (i), there exists $y, z \in S'$ with $y - z \in \Lambda \setminus 0$. But $2y, 2z \in S$, so $-2z \in S$ as S is symmetric about 0. Now convexity implies that $y - z = \frac{1}{2}(2y - 2z) \in S$.

(b) Now suppose $\mathrm{vol}(S) \geq 2^n \, \mathrm{covol}(\Lambda)$, and S is closed. Define $S_m = (1 + \frac{1}{m}) S$ for $m \in \mathbb{N}$. Now we have that $\gamma_m \in S_m \cap \Lambda$ with $\gamma_m \neq 0$ by (a). Convexity implies that $S_m \subseteq S_1$, so $\gamma_1, \gamma_2, \dots \in S_1 \cap \Lambda$, which is a finite set since S_1 is bounded[2]. Hence there exists γ such that $\gamma_m = \gamma$ for infinitely many m. Then

$$\gamma \in \bigcap_m S_m = S$$

as S is closed and bounded. □

3.2 Finiteness of the class group

Let L be a number field, $[L : \mathbb{Q}] = n$. Then we have real embeddings $\sigma_1, \dots, \sigma_r : L \to \mathbb{R}$, and complex embeddings $\sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \dots, \overline{\sigma_{r+s}} : L \to \mathbb{C}$. Define

$$\sigma = (\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \dots, \sigma_{r+s}) : L \to \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^{r+2s} = \mathbb{R}^n$$

where we use the isomorphism $C \simeq \mathbb{R}^2$ as $\mathbb{R}$-vector spaces, given by $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$.

Lemma 3.6. If $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ is an ideal, then $\sigma(\mathfrak{a})$ is a lattice with

[2] Which we can assume, since $0 < \mathrm{vol}(S) < \infty$ implies that S is bounded.

$$\text{covol}(\sigma(\mathfrak{a})) = 2^{-s}|D_L|^{1/2} N(\mathfrak{a})$$

Proof. Recall that $\mathfrak{a}$ has an integral basis, say $\gamma_1, \dots, \gamma_n$, and that $\Delta(\gamma_1, \dots, \gamma_n) = \det\big(\sigma_i(\gamma_j)\big)^2 = N(\mathfrak{a}) D_L$, so $\big|\det\big(\sigma_i(\gamma_j)\big)\big| = N(\mathfrak{a})|D_L|^{1/2}$. The covolume is given by

$$\text{covol}(\sigma(\mathfrak{a})) = \det \begin{pmatrix} \vdots & & \vdots \\ \sigma(\gamma_1) & & \sigma(\gamma_n) \\ \vdots & & \vdots \end{pmatrix}$$

which has the same rows 1 to r as $(\sigma_i(\gamma_j))$, but for the $r+1, \dots, r+2s$ rows, we have

$$\begin{pmatrix} \text{Re}(\sigma_{r+i}(\gamma_j)) \\ \text{Im}(\sigma_{r+i}(\gamma_j)) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} \sigma_{r+i}(\gamma_j) \\ \overline{\sigma_{r+i}(\gamma_j)} \end{pmatrix}$$

Hence the change of basis matrix has absolute value of the determinant being 2^{-s}. ☐

Corollary 3.7. $\sigma(\mathcal{O}_L)$ is a lattice in $\mathbb{R}^n$ with $\text{covol}(\sigma(\mathcal{O}_L)) = 2^{-s}|D_L|^{1/2}$.

Proposition 3.8 (Minkowski bound)**.** Suppose $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ is a nonzero ideal. Then there exists $\alpha \in \mathfrak{a}$ nonzero, with $|N(\alpha)| < C_L N(\mathfrak{a})$, where

$$C_L = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |D_L|^{1/2}$$

is called the Minkowski bound.

Proof. Let

$$B_{r,s}(t) = \left\{ (y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; \sum |y_i| + 2 \sum |z_j| < t \right\}$$

Then $B_{r,s}(t)$ is closed, bounded, measurable, with

$$\text{vol}(B_{r,s}(t)) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$$

Choose t such that $\text{vol}(B_{r,s}(t)) = 2^n \, \text{covol}(\sigma(\mathfrak{a}))$. Then by Minkowski's lemma, we have $\alpha \in \mathfrak{a}$ nonzero, such that $\sigma(\alpha) \in B_{r,s}(t)$. Write $\sigma(\alpha) = (y_1, \dots, y_r, z_1, \dots, z_s)$. Then by the AM-GM inequality, we have that

$$|N(\alpha)|^{1/n} = |y_1 \cdots y_r z_1 \overline{z_1} \cdots z_s \overline{z_s}| \le \frac{1}{n} \left(\sum |y_i| + 2 \sum |z_j| \right) \le \frac{t}{n}$$

Which means that

$$|N(\alpha)| \le \frac{t^n}{n} = C_L N(\mathfrak{a})$$

☐

Corollary 3.9. Every $[\mathfrak{a}] \in \text{Cl}(L)$ has a representative $\mathfrak{a} \trianglelefteq \mathcal{O}_L$, with $N(\mathfrak{a}) \le C_L$.

Proof. Let $\alpha \in \mathfrak{a}^{-1}$ be such that $|N(\alpha)| \le C_L N(\mathfrak{a}^{-1})$. Then $\mathfrak{a}^{-1} \mid (\alpha)$, so we must have $\mathfrak{a}^{-1}\mathfrak{b} = (\alpha)$, for some ideal $\mathfrak{b}$. Taking norms, we find

$$N(\mathfrak{a}^{-1}) N(\mathfrak{b}) = |N(\alpha)| \le C_L N(\mathfrak{a}^{-1})$$

so $N(\mathfrak{b}) \le C_L$. Furthermore, in the class group, we have that $[\mathfrak{b}] = [\mathfrak{a}]$. ☐

Theorem 3.10. $\mathrm{Cl}(L)$ is a finite group, and it is generated by $[\mathfrak{p}]$, where the $\mathfrak{p}$ are prime ideals with $N(\mathfrak{p}) \leq C_L$.

Proof. By the previous corollary, let $[\mathfrak{a}] \in \mathrm{Cl}(L)$, with $N(\mathfrak{a}) \leq C_L$. Then if we factor $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, then each $N(\mathfrak{p}_i) \leq C_L$. □

Corollary 3.11. $\mathrm{Cl}(L)$ is generated by the prime factors of $p\mathcal{O}_L$, for primes $p \leq C_L$.

Theorem 3.12 (Hermite, Minkowski)**.** If $n \geq 2$, then

$$|D_L| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$$

So there are primes which ramify in L.

Proof. Consider the class $[\mathcal{O}_L] \in \mathrm{Cl}(L)$. Then we have an ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ such that $1 \leq N(\mathfrak{a}) \leq C_L$. This implies $C_L \geq 1$, so

$$|D_L|^{1/2} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!} =: a_n^{1/2}$$

The result follows by induction as

$$a_2 = \frac{\pi^2}{4} \quad \text{and} \quad \frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} > \frac{\pi}{4}(1+2) = \frac{3\pi}{4}$$

by the binomial theorem. □

3.3 Dirichlet's unit theorem

The final result in the course is Dirichlet's unit theorem.

Theorem 3.13 (Dirichlet's unit theorem)**.**

$$\mathcal{O}_L^\times \simeq \mu_L \times \mathbb{Z}^{r+s-1}$$

as abelian groups, where

$$\mu_L = \{\alpha \in L \mid \alpha^m = 1 \text{ for some } m > 0\}$$

is the group of roots of unity in L, which is a finite cyclic group.

Let $\sigma_1, \ldots, \sigma_r : L \to \mathbb{R}$ be the real embeddings, and $\sigma_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}} : L \to \mathbb{C}$ be the complex embeddings, as before. Define $\ell : \mathcal{O}_L^\times \to \mathbb{R}^{r+s}$ by

$$\ell(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha), 2\log|\sigma_{r+1}(\alpha)||, \ldots, 2\log|\sigma_{r+s}(\alpha)|)$$

Lemma 3.14.

(i) $\mathrm{im}(\ell) \leq \mathbb{R}^{r+s}$ is a discrete subgroup,

(ii) $\ker(\ell) = \mu_L$ is a finite group.

Proof. (i) As $\log|ab| = \log|a| + \log|b|$, ℓ is a group homomorphism, and so its image is a subgroup of $\mathbb{R}^{r+s}$. We want to show that it is discrete. Equivalently, it suffices to show that for every $R > 0$, $\mathrm{im}(\ell) \cap [-R, R]^{r+s}$ is finite. But we have that $\ell = j \circ \sigma$,

$$\mathcal{O}_L^\times \hookrightarrow \mathcal{O}_L \xrightarrow{\sigma} \mathbb{R}^r \times \mathbb{C}^s \xrightarrow{j} \mathbb{R}^{r+s}$$

where $j(y_1, \dots, y_r, z_1, \dots, z_s) = (\log|y_1|, \dots, \log|y_r|, 2\log|z_1|, \dots, 2\log|z_s|)$. We have that

$$j^{-1}([-R, R]^{r+s}) = \left\{(y_i, z_j) \mid e^{-R} \le y_i \le e^R, e^{-R} \le 2\left|z_j\right| \le e^R\right\}$$

which is compact. But $\sigma(\mathcal{O}_L)$ is a lattice, so $\sigma(\mathcal{O}_L) \cap j^{-1}([-R, R]^{r+s})$ is finite.

(ii) Note that if $\alpha \in \ker(\ell)$, then $\sigma(\alpha) \in \sigma(\mathcal{O}_L) \cap j^{-1}([-R, R]^{r+s})$ for all $R > 0$. In particular, as σ is injective, $\ker(\ell)$ is a finite group. So each element has finite order, hence it is a root of unity. Thus, $\ker(\ell) = \mu_L$. □

Lemma 3.15.

$$\mathrm{im}(\ell) \le \left\{(y_1, \dots, y_{r+s}) \;\middle|\; \sum y_i = 0\right\}$$

Proof. If $\alpha \in \mathcal{O}_L^\times$, then

$$0 = \log|N(\alpha)| = \sum_{i=1}^{r} \log|\sigma_i(\alpha)| + 2\sum_{i=r+1}^{r+s} |\sigma_i(\alpha)|$$

□

Corollary 3.16. $\mathrm{im}(\ell)$ is isomorphic to a discrete subgroup of $\mathbb{R}^{r+s-1}$, so it must be $\mathbb{Z}^a$ for some $0 \le a \le r + s - 1$.

Lemma 3.17. Fix k with $1 \le k \le r + x$, $\alpha \in \mathcal{O}_L$ nonzero. Write $\ell(\alpha) = (a_1, \dots, a_{r+s})$. Then there exists $\beta \in \mathcal{O}_L$ nonzero with

(i) $|N(\beta)| \le \left(\frac{2}{\pi}\right)^s |D_L|^{1/2}$,

(ii) if we write $\ell(\beta) = (b_1, \dots, b_{r+s})$, then $b_i < a_i$ for every $\ne k$.

Proof. Let

$$S = \left\{(y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid |y_i| \le c_i, \left|z_j\right|^2 \le c_{r+j}\right\}$$

for soem constants $c_1, \dots, c_{r+s}$. Then S is closed, convex and symmetric around zero, with $\mathrm{vol}(S) = 2^r \pi^s c_1 \cdots c_{r+s}$. If we choose c_i such that $0 < c_i < e^{a_i}$ for all $i \ne k$, and c_k such that

$$\mathrm{vol}(S) = 2^n \,\mathrm{covol}(\sigma(\mathcal{O}_L))$$

by Minkowski's lemma, there exists $\beta \in \sigma(\mathcal{O}_L) \cap S$. □

Lemma 3.18. If $\alpha = \beta + m\gamma$, with $\alpha, \beta, \gamma \in \mathcal{O}_L$, and $N(\alpha) = N(\beta) = m$, then $\alpha/\beta \in \mathcal{O}_L^\times$.

Proof. Notice that $N(\beta)/\beta \in L$ is a product of algebraic elements, since

$$N(\beta) = \prod_i \sigma_i(\beta)$$

so $N(\beta)/\beta \in \mathcal{O}_L$. □

Lemma 3.19. Let $A \in M_m(\mathbb{R})$ be such that $a_{ii} > 0$ for all i, $a_{ij} < 0$ for $i \neq j$, $\sum_j a_{ij} \geq 0$ for all i. Then $\text{rank}(A) \geq m - 1$.

Proof. Some basic linear algebra. Any $m - 1$ columns of A are linearly independent. □

Lemma 3.20. The short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow \mathbb{Z}^m \longrightarrow 0$$

of abelian groups splits. That is, $B \simeq A \oplus \mathbb{Z}^m$, with the map $B \to \mathbb{Z}^m$ being the projection map.

Proof. Easy homological algebra. □

Proof of Dirichlet's unit theorem. Fix $1 \leq k \leq r + s$. Then we have a sequence $\alpha_1, \alpha_2, \ldots$ such that $N(\alpha_t)$ bounded, and for $i \neq k$, the i-th coordinate of $\ell(\alpha_1), \ell(\alpha_2), \ldots$ is a strictly decreasing sequence. Now by the Pigeonhole principle, there exists $t < t'$ such that

1. $N(\alpha_t) = N(\alpha_{t'}) = m$,
2. $\alpha_t \equiv \alpha_{t'} \mod m\mathcal{O}_L$

Then $u_k = \alpha_t / \alpha_{t'} \in \mathcal{O}_L^\times$. Furthermore, we have that

$$\ell(u_k) = \ell(\alpha_t) - \ell(\alpha_t)' = (y_1, \ldots, y_{r+s})$$

and we have that $y_i < 0$ if $i \neq k$, $y_1 + \cdots + y_{r+s} = 0$, and $y_k > 0$. But then this means that $u_1, \ldots, u_{r+s-1}$ are linearly independent, so the rank of $\ell(\mathcal{O}_L^\times)$ is $r + s - 1$. □

4 Quadratic number fields

In this section, we collect the implications of the theorems in this course for quadratic number fields. That is, $[L : \mathbb{Q}] = 2$. By some basic field theory, we can see that all such L must be of the form $L = \mathbb{Q}(\sqrt{d})$, where we can assume wlog that d is squarefree, $d \neq 0, 1$. Throughout, assume $L = \mathbb{Q}(\sqrt{d})$.

Integral basis and discriminant

Lemma 4.1.

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[(1 + \sqrt{d})/2] & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4 \end{cases}$$

Proof. $L/\mathbb{Q}$ has basis $1, \sqrt{d}$. So if $\alpha = x + y\sqrt{d}$, then the matrix of m_α in this basis is

$$\begin{pmatrix} x & dy \\ y & x \end{pmatrix}$$

which has minimal polynomial $t^2 - 2x + (x^2 - dy^2)$. Hence $\alpha \in \mathcal{O}_L$ if and only if $2x, x^2 - dy^2 \in \mathbb{Z}$. Notice that this implies that $4dy^2 \in \mathbb{Z}$. If $y = r/s \in \mathbb{Q}$, with r, s coprime, then $s^2 \mid 4d$. But d is squarefree, so $s^2 \mid 4$, so $s = \pm 1$ or ± 2. Hence we have that

$$x = \frac{u}{2}, y = \frac{v}{2}, u, v \in \mathbb{Z} \quad \text{with} \quad u^2 \equiv dv^2 \pmod 4$$

Now the quadratic residues mod 4 are $0, 1$, so if $d \not\equiv 1 \pmod 4$, then the equation has a solution if and only if $u^2, B^2 \equiv 0 \pmod 4$. That is, u, v are even. So $x, y \in \mathbb{Z}$. That is, $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$.

On the other hand, if $d \equiv 1 \pmod 4$, then the equation implies that u, v have the same parity, so we can write α as a $\mathbb{Z}$ linear combination of $1, (1 + \sqrt{d})/2$. □

Note that the minimal polynomials are

- $t^2 - t + (1-d)/4$ for $(1+\sqrt{d})/2$
- $t^2 - d$ for $\sqrt{d}$

Corollary 4.2. *L has integral basis*

$$\begin{cases} 1, (1+\sqrt{d})/2 & \text{if } d \equiv 1 \pmod 4 \\ 1, \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4 \end{cases}$$

Corollary 4.3. *L has discriminant*

$$\begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2,3 \pmod 4 \end{cases}$$

Ideals

Lemma 4.4. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ be an ideal, then there exists $\alpha \in \mathcal{O}_L$, $b \in \mathbb{Z}$ such that $\mathfrak{a} = \langle \alpha, b \rangle$.

Proof. Since $\mathfrak{a} \simeq \mathbb{Z}^2$ as abelian groups, we can choose $\alpha, \beta \in \mathcal{O}_L$ such that $\mathfrak{a} = \langle \alpha, \beta \rangle$. We will handle the $d \equiv 1 \pmod 4$ and $d \equiv 2,3 \pmod 4$ cases together. We can write

$$\alpha = \frac{u + v\sqrt{d}}{2}, \beta = \frac{x + y\sqrt{d}}{2}$$

where $u, v, x, y \in \mathbb{Z}$, with $u \equiv v \pmod 2$ and $x \equiv y \pmod 2$. Let $\ell = \gcd(y, v) = mv + ny$, and we the have that

$$\beta' = \beta - \frac{y(m\alpha + n\beta)}{\ell} = \frac{m}{\ell}\left(\frac{vx - uy}{2}\right)$$

But $vx - uy \equiv 0 \pmod 2$, so $\beta' \in \mathbb{Z}$. It is easy to see that $\langle \alpha, \beta \rangle = \langle \alpha, \beta' \rangle$, so we are done. □

Proposition 4.5. Let $\mathfrak{a} = \langle \alpha, b \rangle$ with $\alpha \in \mathcal{O}_L, b \in \mathbb{Z}$. Then

$$\mathfrak{a}\overline{\mathfrak{a}} = \langle b, \alpha \rangle \langle b, \overline{\alpha} \rangle$$

is principal.

Proof.

$$\mathfrak{a}\overline{\mathfrak{a}} = \left\langle b^2, b\alpha, b\overline{\alpha}, \alpha\overline{\alpha} \right\rangle = \left\langle b^2, b\alpha, b\operatorname{Tr}(\alpha), N(\alpha) \right\rangle$$

Let $c = \gcd(b^2, b\operatorname{Tr}(\alpha), N(\alpha))$. Then $\mathfrak{a}\overline{\mathfrak{a}} = \langle b\alpha, c \rangle$. Let $x = b\alpha/c$. Then $Tr(x), N(x) \in \mathbb{Z}$, so $x \in \mathcal{O}_L$, and so $c \mid b\alpha$ in $\mathcal{O}_L$. Thus $\mathfrak{a}\overline{\mathfrak{a}} = \langle c \rangle$ is principal. □

Dedekind and primes

First of all, we consider the behaviour of odd primes. Let p be an odd prime, then $\mathbb{Z}[\sqrt{d}] \leq \mathcal{O}_L$ has index 1 or 2, which is coprime to p. Hence by Dedekind's criterion, we must factor $x^2 - d \mod p$. We have three possibilities.

(i) if $(\frac{d}{p}) = 1$, then there are two distinct roots modulo p, so p splits completely.

(ii) if $(\frac{d}{p}) = 0$, i.e. $p \mid d$, then p ramifies.

(iii) if $(\frac{d}{p}) = -1$, then $x^2 - d$ is irreducible, so p is inert.

Lemma 4.6.

$$2\begin{cases}\text{splits completely} & \iff d\equiv 1 \pmod 8\\ \text{is inert} & \iff d\equiv 5 \pmod 8\\ \text{ramifies} & \iff d\equiv 2,3 \pmod 4\end{cases}$$

Proof. First we handle the case $d \equiv 1 \pmod 4$. In this case, $\mathcal{O}_L = \mathbb{Z}[\alpha]$, where $\alpha = (1+\sqrt{d})/2$ has minimal polynomial $g = x^2 - x + (1-d)/4$. So if $d \equiv 1 \pmod 8$, then $\overline{g} = x^2 + x = x(x+1)$, so 2 splits by Dedekind. If $d \equiv 5 \pmod 8$, then $\overline{g} = x^2 + x + 1$, which is irreducible.

Finally, if $d \equiv 2, 3 \pmod 4$, then $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$, and $g(x) = x^2 - d$ is the minimal polynomial. Modulo 2 this is x^2 or $x^2 - 1 = (x-1)^2$, so 2 ramifies. □

Minkowski bound

For imaginary quadratic fields, that is, $\mathbb{Q}(\sqrt{d})$ with $d < 0$ squarefree, we have that $n = 2, r = 0, s = 1$, so the Minkowski bound is

$$C_L = \frac{2}{\pi}|D_L|^{1/2}$$

and for real quadratic fields, we have $n = 2, r = 2, s = 0$, so the Minkowski bound is

$$C_L = \frac{1}{2}|D_L|^{1/2}$$

Dirichlet's unit theorem

For a real quadratic number field, $\mu_L = \{\pm 1\}$, $n = 2, r = 2, s = 0$, so we have that

$$\mathcal{O}_L^\times \simeq \{\pm 1\} \times \mathbb{Z}$$

More concretely, we have

Corollary 4.7 (Dirichlet's unit theorem for real quadratic number fields)**.**

$$\mathcal{O}_L^\times = \{\pm \varepsilon_0^n \mid n \in \mathbb{Z}\}$$

for some $\varepsilon_0 \in \mathcal{O}_L^\times$, called a fundamental unit.

Proof. Choose $\varepsilon_0 \in \mathcal{O}_L^\times$, with $1 < |\sigma_1(\varepsilon_0)|$ minimal. Then ε_0 is a fundamental unit. □

For an imaginary quadratic number field, $n = 2, r = 0, s = 1$, so $r + s - 1 = 0$. Hence by Dirichlet's unit theorem, $\mathcal{O}_L^\times = \mu_L$ is a finite group. In particular,

Lemma 4.8.

1. if $d = -1$, then $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$,
2. if $d = -3$, $\omega = (1+\sqrt{-3})/2$, $\mathbb{Z}[\omega]^\times = \{1, \omega, \ldots, \omega^5\}$,
3. for all other $d < 0$, $\mathcal{O}_L^\times = \{\pm 1\}$.

Proof. Just solve $N(x + y\sqrt{d}) = x^2 - dy^2 = \pm 1$. □