Part II — Number Fields

Theorems with proof

Based on lectures by I. Grojnowski

Notes taken by Dexter Chua

Lent 2016

Part IB Groups, Rings and Modules is essential and Part II Galois Theory is desirable

Definition of algebraic number fields, their integers and units. Norms, bases and discriminants. [3]

Ideals, principal and prime ideals, unique factorisation. Norms of ideals. [3]

Minkowski's theorem on convex bodies. Statement of Dirichlet's unit theorem. Determination of units in quadratic fields. [2]

Ideal classes, finiteness of the class group. Calculation of class numbers using statement of the Minkowski bound. [3]

Dedekind's theorem on the factorisation of primes. Application to quadratic fields. [2]

Discussion of the cyclotomic field and the Fermat equation or some other topic chosen by the lecturer. [3]

Contents

0 Introduction

1 Number fields

Lemma. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, i.e. $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$.

Proof. If $\alpha \in \mathbb{Z}$, then $x - \alpha \in \mathbb{Z}[x]$ is a monic polynomial. So $\alpha \in \mathcal{O}_{\mathbb{Q}}$.

On the other hand, let $\alpha \in \mathbb{Q}$. Then there is some coprime $r, s \in \mathbb{Z}$ such that $\alpha = \frac{r}{s}$. If it is an algebraic integer, then there is some

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

with $a_i \in \mathbb{Z}$ such that $f(\alpha) = 0$. Substituting in and multiplying by s^n, we get

$$r^n + \underbrace{a_{n-1}r^{n-1}s + \cdots + a_0 s^n}_{\text{divisible by } s} = 0,$$

So $s \mid r^n$. But if $s \neq 1$, there is a prime p such that $p \mid s$, and hence $p \mid r^n$. Thus $p \mid r$. So p is a common factor of s and r. This is a contradiction. So $s = 1$, and α is an integer. □

Theorem. $\mathcal{O}_L$ is a ring, i.e. if $\alpha, \beta \in \mathcal{O}_L$, then so is $\alpha \pm \beta$ and $\alpha\beta$.

Proposition.

(i) Let $R \subseteq S$ be rings. If $S = R[s]$ and s is integral over R, then S is finitely-generated over R.

(ii) If $S = R[s_1, \cdots, s_n]$ with s_i integral over R, then S is finitely-generated over R.

Proof.

(i) We know S is spanned by $1, s, s^2, \cdots$ over R. However, since s is integral, there exists $a_0, \cdots, a_n \in R$ such that

$$s^n = a_0 + a_1 s + \cdots + a_{n-1}s^{n-1}.$$

So the R-submodule generated by $1, s, \cdots, s^{n-1}$ is stable under multiplication by s. So it contains $s^n, s^{n+1}, s^{n+2}, \cdots$. So it is S.

(ii) Let $S_i = R[s_1, \cdots, s_i]$. So $S_i = S_{i-1}[s_i]$. Since s_i is integral over R, it is integral over S_{i-1}. By the previous part, S_i is finitely-generated over S_{i-1}. To finish, it suffices to show that being finitely-generated is transitive. More precisely, if $A \subseteq B \subseteq C$ are rings, B is finitely generated over A and C is finitely generated over B, then C is finitely generated over A. This is not hard to see, since if $x_1, \cdots, x_n$ generate B over A, and $y_1, \cdots, y_m$ generate C over B, then C is generated by $\{x_i y_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ over A. □

Theorem. If S is finitely-generated over R, then S is integral over R.

Proof. Let $\alpha_1, \cdots, \alpha_n$ generate S as an R-module. wlog take $\alpha_1 = 1 \in S$. For any $s \in S$, write

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

for some $b_{ij} \in R$. We write $B = (b_{ij})$. This is the "matrix of multiplication by S". By construction, we have

$$(sI - B)\begin{pmatrix}\alpha_1\\ \vdots \\ a_n\end{pmatrix} = 0. \qquad (*)$$

Now recall for any matrix X, we have $\mathrm{adj}(X)X = (\det X)I$, where the i, jth entry of $\mathrm{adj}(X)$ is given by the determinant of the matrix obtained by removing the ith row and jth column of X.

We now multiply $(*)$ by $\mathrm{adj}(sI - B)$. So we get

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

In particular, $\det(sI-B)\alpha_1 = 0$. Since we picked $\alpha_1 = 1$, we get $\det(sI-B) = 0$. Hence if $f(x) = \det(xI - B)$, then $f(x) \in R[x]$, and $f(s) = 0$. □

Corollary. Let $L \supseteq \mathbb{Q}$ be a number field. Then $\mathcal{O}_L$ is a ring.

Proof. If $\alpha, \beta \in \mathcal{O}_L$, then $\mathbb{Z}[\alpha, \beta]$ is finitely-generated by the proposition. But then $\mathbb{Z}[\alpha, \beta]$ is integral over $\mathbb{Z}$, by the previous theorem. So $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$. □

Corollary. If $A \subseteq B \subseteq C$ be ring extensions such that B over A and C over B are integral extensions. Then C is integral over A.

Proof. If $c \in C$, let

$$f(x) = \sum_{i=0}^{N} b_i x^i \in B[x]$$

be a monic polynomial such that $f(c) = 0$. Let $B_0 = A[b_0, \cdots, b_N]$ and let $C_0 = B_0[c]$. Then B_0/A is finitely generated as $b_0, \cdots, b_N$ are integral over A. Also, C_0 is finitely-generated over B_0, since c is integral over B_0. Hence C_0 is finitely-generated over A. So c is integral over A. Since c was arbitrary, we know C is integral over A. □

Lemma. If $f \in K[x]$ with $f(\alpha) = 0$, then $p_\alpha \mid f$.

Proof. Write $f = p_\alpha h + r$, with $r \in K[x]$ and $\deg(r) < \deg(p_\alpha)$. Then we have

$$0 = f(\alpha) = p(\alpha)h(\alpha) + r(\alpha) = r(\alpha).$$

So if $r \neq 0$, this contradicts the minimality of $\deg p_\alpha$. □

Proposition. 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 the field extension $\mathbb{Q} \subseteq L$ is in fact in $\mathbb{Z}[x]$.

Proof. $(\Leftarrow)$ is trivial, since this is just the definition of an algebraic integer.

$(\Rightarrow)$ Let $\alpha \in \mathcal{O}_L$ and $p_\alpha \in \mathbb{Q}[x]$ be the minimal polynomial of α, and $h(x) \in \mathbb{Z}[x]$ be a monic polynomial which α satisfies. The idea is to use h to show that the coefficients of p_α are algebraic, thus in fact integers.

Now there exists a bigger field $M \supseteq L$ such that

$$p_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_r)$$

factors in $M[x]$. But by our lemma, $p_\alpha \mid h$. So $h(\alpha_i) = 0$ for all α_i. So $\alpha_i \in \mathcal{O}_M$ is an algebraic integer. But $\mathcal{O}_M$ is a ring, i.e. sums and products of the α_i's are still algebraic integers. So the coefficients of p_α are algebraic integers (in $\mathcal{O}_M$). But they are also in $\mathbb{Q}$. Thus the coefficients must be integers. □

Lemma. We have

$$\operatorname{Frac} \mathcal{O}_L = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in \mathcal{O}_L, \beta \neq 0 \right\} = L.$$

In fact, for any $\alpha \in L$, there is some $n \in \mathbb{Z}$ such that $n\alpha \in \mathcal{O}_L$.

Proof. If $\alpha \in L$, let $g(x) \in \mathbb{Q}[x]$ be its monic minimal polynomial. Then there exists $n \in \mathbb{Z}$ non-zero such that $ng(x) \in \mathbb{Z}[x]$ (pick n to be the least common multiple of the denominators of the coefficients of $g(x)$). Now the magic is to put

$$h(x) = n^{\deg(g)} g\left(\frac{x}{n}\right).$$

Then this is a monic polynomial with integral coefficients — in effect, we have just multiplied the coefficient of x^i by $n^{\deg(g)-i}$! Then $h(n\alpha) = 0$. So $n\alpha$ is integral. □

2 Norm, trace, discriminant, numbers

Proposition. For a field extension L/K and $a, b \in L$, we have $N(ab) = N(a)N(b)$ and $\mathrm{tr}(a+b) = \mathrm{tr}(a) + \mathrm{tr}(b)$.

Proposition. Let $p_\alpha \in K[x]$ be the minimal polynomial of α. Then the characteristic polynomial of m_α is

$$\det(xI - m_\alpha) = p_\alpha^{[L:K(\alpha)]}$$

Hence if $p_\alpha(x)$ splits in some field $L' \supseteq K(\alpha)$, say

$$p_\alpha(x) = (x - \alpha_1)\cdots(x - \alpha_r),$$

then

$$N_{K(\alpha)/K}(\alpha) = \prod \alpha_i, \quad \mathrm{tr}_{K(\alpha)/K}(\alpha) = \sum \alpha_i,$$

and hence

$$N_{L/K}(\alpha) = \left(\prod \alpha_i\right)^{[L:K(\alpha)]}, \quad \mathrm{tr}_{L/K} = [L : K(\alpha)]\left(\sum \alpha_i\right).$$

Corollary. Let $L \supseteq \mathbb{Q}$ be a number field. Then the following are equivalent:

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

(ii) The minimal polynomial p_α is in $\mathbb{Z}[x]$

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

This in particular implies $N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $\mathrm{tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Proof. The equivalence between the first two was already proven. For the equivalence between (ii) and (iii), if $m_\alpha \in \mathbb{Z}[x]$, then $\alpha \in \mathcal{O}_L$ since it vanishes on a monic polynomial in $\mathbb{Z}[x]$. On the other hand, if $p_\alpha \in \mathbb{Z}[x]$, then so is the characteristic polynomial, since it is just p_α^N.

The final implication comes from the fact that the norm and trace are just coefficients of the characteristic polynomial. □

Lemma. Let $L = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is not $0, 1$ and is square-free. Then

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

Proof. We know $x + y\sqrt{\lambda} \in \mathcal{O}_L$ if and only if $2x, x^2 - dy^2 \in \mathbb{Z}$ by the previous example. These imply $4dy^2 \in \mathbb{Z}$. So if $y = \frac{r}{s}$ with r, s coprime, $r, s \in \mathbb{Z}$, then we must have $s^2 \mid 4d$. But d is square-free. So $s = 1$ or 2. So

$$x = \frac{u}{2}, \quad y = \frac{v}{2}$$

for some $u, v \in \mathbb{Z}$. Then we know $u^2 - dv^2 \in 4\mathbb{Z}$, i.e. $u^2 \equiv dv^2 \pmod 4$. But we know the squares mod 4 are always 0 and 1. So if $d \not\equiv 1 \pmod 4$, then $u^2 \equiv dv^2 \pmod 4$ imply that $u^2 = v^2 = 0 \pmod 4$, and hence u, v are even. So $x, y \in \mathbb{Z}$, giving $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$.

On the other hand, if $d \equiv 1 \pmod 4$, then u, v have the same parity mod 2, i.e. we can write $x + y\sqrt{d}$ as a $\mathbb{Z}$-combination of 1 and $\frac{1}{2}(1+\sqrt{d})$.

As a sanity check, we find that the minimal polynomial of $\frac{1}{2}(1+\sqrt{d})$ is $x^2 - x + \frac{1}{4}(1-d)$ which is in $\mathbb{Z}$ if and only if $d \equiv 1 \pmod 4$. □

Theorem (Primitive element theorem)**.** Let $K \subseteq L$ be a separable field extension. Then there exists an $\alpha \in L$ such that $K(\alpha) = L$.

Lemma. The degree $[L : \mathbb{Q}] = n$ of a number field is the number of field embeddings $L \hookrightarrow \mathbb{C}$.

Proof. Let α be a primitive element, and $p_\alpha(x) \in \mathbb{Q}[x]$ its minimal polynomial. Then by we have $\deg p_\alpha = [L : \mathbb{Q}] = n$, as $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is a basis. Moreover,

$$\frac{\mathbb{Q}[x]}{(p_\alpha)} \cong \mathbb{Q}(\alpha) = L.$$

Since $L/\mathbb{Q}$ is separable, we know p_α has n distinct roots in $\mathbb{C}$. Write

$$p_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

Now an embedding $\mathbb{Q}[x]/(p_\alpha) \hookrightarrow \mathbb{C}$ is uniquely determined by the image of x, and x must be sent to one of the roots of p_α. So for each i, the map $x \mapsto \alpha_i$ gives us a field embedding, and these are all. So there are n of them. □

Corollary. Let $L/\mathbb{Q}$ be a number field. If $\sigma_1, \cdots, \sigma_n : L \to \mathbb{C}$ are the different field embeddings and $\beta \in L$, then

$$\mathrm{tr}_{L/\mathbb{Q}}(\beta) = \sum \sigma_i(\beta), \quad N_{L/\mathbb{Q}}(\beta) = \prod_i \sigma_i(\beta).$$

We call $\sigma_1(\beta), \cdots, \sigma_n(\beta)$ the *conjugates* of β in $\mathbb{C}$.

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

Proof. ($\Rightarrow$) We know $N(ab) = N(a)N(b)$. So if $x \in \mathcal{O}_L^\times$, then there is some $y \in \mathcal{O}_L$ such that $xy = 1$. So $N(x)N(y) = 1$. So $N(x)$ is a unit in $\mathbb{Z}$, i.e. ± 1.

($\Leftarrow$) Let $\sigma_1, \cdots, \sigma_n : L \to \mathbb{C}$ be the n embeddings of L in $\mathbb{C}$. For notational convenience, We suppose that L is already subfield of $\mathbb{C}$, and σ_1 is the inclusion map. Then for each $x \in \mathcal{O}_L$, we have

$$N(x) = x\sigma_2(x) \cdots \sigma_n(x).$$

Now if $N(x) = \pm 1$, then $x^{-1} = \pm\sigma_2(x) \cdots \sigma_n(x)$. So we have $x^{-1} \in \mathcal{O}_L$, since this is a product of algebraic integers. So x is a unit in $\mathcal{O}_L$. □

Corollary. If $x \in \mathcal{O}_L$ is such that $N(x)$ is prime, then x is irreducible.

Proof. If $x = ab$, then $N(a)N(b) = N(x)$. Since $N(x)$ is prime, either $N(a) = \pm 1$ or $N(b) = \pm 1$. So a or b is a unit. □

Proposition. Let L/K be a separable extension. Then a K-bilinear form $L \times L \to K$ defined by $(x, y) \mapsto \mathrm{tr}_{L/K}(xy)$ is non-degenerate. Equivalent, if $\alpha_1, \cdots, \alpha_n$ are a K-basis for L, the Gram matrix $(\mathrm{tr}(\alpha_i\alpha_j))_{i,j=1,\cdots,n}$ has non-zero determinant.

Proof. Let $\sigma_1, \cdots, \sigma_n : L \to \bar{K}$ be the n distinct K-linear field embeddings $L \hookrightarrow \bar{K}$. Put

$$S = (\sigma_i(\alpha_j))_{i,j=1,\cdots,n} = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n). \end{pmatrix}$$

Then

$$S^T S = \left(\sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right)_{i,j=1,\cdots n}.$$

We know σ_k is a field homomorphism. So

$$\sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i\alpha_j) = \mathrm{tr}_{L/K}(\alpha_i\alpha_j).$$

So

$$S^T S = (\mathrm{tr}(\alpha_i\alpha_j))_{i,j=1,\cdots,n}.$$

So we have

$$\Delta(\alpha_1, \cdots, \alpha_n) = \det(S^T S) = \det(S)^2.$$

Now we use the theorem of primitive elements to write $L = K(\theta)$ such that $1, \theta, \cdots, \theta^{n-1}$ is a basis for L over K, with $[L : K] = n$. Now S is just

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

This is a Vandermonde matrix, and so

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

Since the field extension is separable, and hence $\sigma_i \neq \sigma_j$ for all i, j, this implies $\sigma_i(\theta) \neq \sigma_j(\theta)$, since θ generates the field. So the product above is non-zero. □

Theorem. Let $\mathbb{Q}/L$ be a number field. Then there exists an integral basis for $\mathcal{O}_L$. In particular, $\mathcal{O}_L \cong \mathbb{Z}^n$ with $n = [L : \mathbb{Q}]$.

Proof. Let $\alpha_1, \cdots, \alpha_n$ be any basis of L over $\mathbb{Q}$. We have proved that there is some $n_i \in \mathbb{Z}$ such that $n_i\alpha_i \in \mathcal{O}_L$. So wlog $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_L$, and are an basis of L over $\mathbb{Q}$. Since α_i are integral, so are $\alpha_i\alpha_j$, and so all these have integer trace, as we have previously shown. Hence $\Delta(\alpha_1, \cdots, \alpha_n)$, being the determinant of a matrix with integer entries, is an integer.

Now choose a $\mathbb{Q}$-basis $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_L$ such that $\Delta(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z} \setminus \{0\}$ has minimal absolute value. We will show that these are an integral basis.

Let $x \in \mathcal{O}_L$, and write

$$x = \sum \lambda_i \alpha_i$$

for some $\lambda_i \in \mathbb{Q}$. These λ_i are necessarily unique since $\alpha_1, \cdots, \alpha_n$ is a basis.

Suppose some $\lambda_i \notin \mathbb{Z}$. wlog say $\lambda_1 \notin \mathbb{Z}$. We write

$$\lambda_1 = n_1 + \varepsilon_1,$$

for $n_1 \in \mathbb{Z}$ and $0 < \varepsilon_1 < 1$. We put

$$\alpha_1' = x - n_1\alpha_1 = \varepsilon_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n \in \mathcal{O}_L.$$

So $\alpha_1', \alpha_2, \cdots, \alpha_n$ is still a basis for $L/\mathbb{Q}$, and are still in $\mathcal{O}_L$. But then

$$\Delta(\alpha_1', \cdots, \alpha_n) = \varepsilon_1^2 \cdot \Delta(\alpha_1, \cdots, \alpha_n) < \Delta(\alpha_1, \cdots, \alpha_n).$$

This contradicts minimality. So we must have $\lambda_i \in \mathbb{Z}$ for all $\mathbb{Z}$. So this is a basis for $\mathcal{O}_L$. □

3 Multiplicative structure of ideals

Proposition. Let $L/\mathbb{Q}$ be a number field, and $\mathcal{O}_L$ be its ring of integers. Then $\mathcal{O}_L$ is a Dedekind domain.

Proof of (i) to (iii).

(i) Obvious, since $\mathcal{O}_L \subseteq L$.

(ii) We showed that as an abelian group, $\mathcal{O}_L = \mathbb{Z}^n$. So if $\mathfrak{a} \leq \mathcal{O}_L$ is an ideal, then $\mathfrak{a} \leq \mathbb{Z}^n$ as a subgroup. So it is finitely generated as an abelian group, and hence finitely generated as an ideal.

(iii) Note that $\operatorname{Frac} \mathcal{O}_L = L$. If $x \in L$ is integral over $\mathcal{O}_L$, as $\mathcal{O}_L$ is integral over $\mathbb{Z}$, x is also integral over $\mathbb{Z}$. So $x \in \mathcal{O}_L$, by definition of $\mathcal{O}_L$. □

Lemma. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be a non-zero ideal. Then $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$ and $\mathcal{O}_L/\mathfrak{a}$ is finite.

Proof. Let $\alpha \in \mathfrak{a}$ and $\alpha \neq 0$. Let

$$p_\alpha = x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

be its minimal polynomial. Then $p_\alpha \in \mathbb{Z}[x]$. We know $a_0 \neq 0$ as p_α is irreducible.

Since $p_\alpha(\alpha) = 0$, we know

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

We know $\alpha \in \mathfrak{a}$ by assumption, and the mess in the brackets is in $\mathcal{O}_L$. So the whole thing is in $\mathfrak{a}$. But $a_0 \in \mathbb{Z}$. So $a_0 \in \mathbb{Z} \cap \mathfrak{a}$.

Thus, we know $\langle a_0 \rangle \subseteq \mathfrak{a}$. Thus we get a surjection

$$\frac{\mathcal{O}_L}{\langle a_0 \rangle} \to \frac{\mathcal{O}_L}{\mathfrak{a}}.$$

Hence it suffices to show that $\mathcal{O}_L/\langle a_0 \rangle$ is finite. But for every $d \in \mathbb{Z}$, we know

$$\frac{\mathcal{O}_L}{\langle d \rangle} = \frac{\mathbb{Z}^n}{d\mathbb{Z}^n} = \left(\frac{\mathbb{Z}}{d\mathbb{Z}}\right)^n,$$

which is finite. □

Proof of (iv). Let $\mathfrak{p}$ be a prime ideal. Then $\mathcal{O}_L/\mathfrak{p}$ is an integral domain. Since the lemma says $\mathcal{O}_L/\mathfrak{p}$ is finite, we know $\mathcal{O}_L/\mathfrak{p}$ is a field. So $\mathfrak{p}$ is maximal. □

Lemma. Let $\mathfrak{p}$ be a prime ideal in a ring R. Then for $\mathfrak{a}, \mathfrak{b} \lhd R$ ideals, then $\mathfrak{ab} \subseteq \mathfrak{p}$ implies $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

Proof. If not, then there is some $a \in \mathfrak{a} \setminus \mathfrak{p}$ and $b \in \mathfrak{b} \setminus \mathfrak{p}$. Then $ab \in \mathfrak{ab} \subseteq \mathfrak{p}$. But then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Contradiction. □

Lemma. Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$ a non-zero ideal. Then there is a subset of $\mathfrak{a}$ that is a product of prime ideals.

Proof. We are going to use the fact that $\mathcal{O}_L$ is Noetherian. If this does not hold, then there must exist a maximal ideal $\mathfrak{a}$ not containing a product of prime ideals (by which we mean any ideal greater than $\mathfrak{a}$ contains a product of prime ideals, *not* that $\mathfrak{a}$ is itself a maximal ideal). In particular, $\mathfrak{a}$ is not prime. So there are some $x, y \in \mathcal{O}_L$ such that $x, y \notin \mathfrak{a}$ but $xy \in \mathfrak{a}$.

Consider $\mathfrak{a} + \langle x\rangle$. This is an ideal, strictly bigger than $\mathfrak{a}$. So there exists prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a} + \langle x\rangle$, by definition.

Similarly, there exists $\mathfrak{q}_1, \cdots \mathfrak{q}_s$ such that $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{a} + \langle y\rangle$.

But then

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

So $\mathfrak{a}$ contains a product of prime ideals. Contradiction. □

Proposition.

(i) Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$ be an ideal. If $x \in L$ has $x\mathfrak{a} \subseteq \mathfrak{a}$, then $x \in \mathcal{O}_L$.

(ii) Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$ be a *proper* ideal. Then

$$\{y \in L : y\mathfrak{a} \leq \mathcal{O}_L\}$$

contains elements that are not in $\mathcal{O}_L$. In other words,

$$\frac{\{y \in L : y\mathfrak{a} \leq \mathcal{O}_L\}}{\mathcal{O}_L} \neq 0.$$

Proof.

(i) Let $\mathfrak{a} \subseteq \mathcal{O}_L$. Then since $\mathcal{O}_L$ is Noetherian, we know $\mathfrak{a}$ is finitely generated, say by $\alpha_1, \cdots, \alpha_m$. We consider the multiplication-by-x map $m_x : \mathfrak{a} \to \mathfrak{a}$, i.e. write

$$x\alpha_i = \sum a_{ij}\alpha_j,$$

where $A = (a_{ij})$ is a matrix in $\mathcal{O}_L$. So we know

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

By multiplying by the adjugate matrix, this implies $\det(xI - A) = 0$. So x satisfies a monic polynomial with coefficients in $\mathcal{O}_L$, i.e. x is integral over $\mathcal{O}_L$. Since $\mathcal{O}_L$ is integrally closed, $x \in \mathcal{O}_L$.

(ii) It is clear that if the result is true for $\mathfrak{a}$, then it is true for all $\mathfrak{a}' \subseteq \mathfrak{a}$. So it is enough to prove this for $\mathfrak{a} = \mathfrak{p}$, a maximal, and in particular prime, ideal.

Let $\alpha \in \mathfrak{p}$ be non-zero. By the previous lemma, there exists prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle\alpha\rangle$. We also have that $\langle\alpha\rangle \subseteq \mathfrak{p}$ by definition. Assume r is minimal with this property. Since $\mathfrak{p}$ is prime, there is some i such that $\mathfrak{p}_i \subseteq \mathfrak{p}$. wlog, we may as well assume $i = 1$, i.e. $\mathfrak{p}_1 \subseteq \mathfrak{p}$. But $\mathfrak{p}_1$ is a prime ideal, and hence maximal. So $\mathfrak{p}_1 = \mathfrak{p}$.

Also, since r is minimal, we know $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq \langle a\rangle$.

Pick $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus \langle a\rangle$. Then

$$\beta\mathfrak{p} = \beta\mathfrak{p}_1 \subseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \langle \alpha\rangle.$$

Dividing by α, we get $\frac{\beta}{\alpha}\mathfrak{p} \subseteq \mathcal{O}_L$. But $\beta \notin \langle\alpha\rangle$. So we know $\frac{\beta}{\alpha} \notin \mathcal{O}_L$. So done. □

Lemma. An $\mathcal{O}_L$ module $\mathfrak{q} \subseteq L$ is a fractional ideal if and only if there is some $c \in L^\times$ such that $c\mathfrak{q}$ is an ideal in $\mathcal{O}_L$. Moreover, we can pick c such that $c \in \mathbb{Z}$.

Proof.

($\Leftarrow$) We have to prove that $\mathfrak{q}$ is finitely generated. If $\mathfrak{q} \subseteq L^\times$, $c \in L$ non-zero, then $c\mathfrak{q} \cong \mathfrak{q}$ as an $\mathcal{O}_L$ module. Since $\mathcal{O}_L$ is Noetherian, every ideal is finitely-generated. So $c\mathfrak{q}$, and hence $\mathfrak{q}$ is finitely generated.

($\Rightarrow$) Suppose $x_1, \cdots, x_n$ generate $\mathfrak{q}$ as an $\mathcal{O}_L$-module. Write $x_i = \frac{y_i}{n_i}$, with $y_i \in \mathcal{O}_L$ and $n_i \in \mathbb{Z}$, $n_i \neq 0$, which we have previously shown is possible.

We let $c = \mathrm{lcm}(n_1, \cdots, n_k)$. Then $c\mathfrak{q} \subseteq \mathcal{O}_L$, and is an $\mathcal{O}_L$-submodule of $\mathcal{O}_L$, i.e. an ideal. □

Corollary. Let $\mathfrak{q}$ be a fractional ideal. Then as an abelian group, $\mathfrak{q} \cong \mathbb{Z}^n$, where $n = [L : \mathbb{Q}]$.

Proof. There is some $c \in L^\times$ such that $c\mathfrak{q} \lhd \mathcal{O}_L$ as an ideal, and $c\mathfrak{q} \cong \mathfrak{q}$ as abelian groups. So it suffices to show that any non-zero ideal $\mathfrak{q} \leq \mathcal{O}_L$ is isomorphic to $\mathbb{Z}^n$. Since $\mathfrak{q} \leq \mathcal{O}_L \cong \mathbb{Z}^n$ as abelian groups, we know $\mathfrak{q} \cong \mathbb{Z}^m$ for some m. But also there is some $a_0 \in \mathbb{Z} \cap \mathfrak{q}$, and $\mathbb{Z}^n \cong \langle a_0\rangle \leq \mathfrak{q}$. So we must have $n = m$, and $\mathfrak{q} \cong \mathbb{Z}^n$. □

Corollary. Let $\mathfrak{a} \leq \mathcal{O}_L$ be a proper ideal. Then $\{x \in L : x\mathfrak{a} \leq \mathcal{O}_L\}$ is a fractional ideal.

Proof. Pick $a \in \mathfrak{a}$. Then $a \cdot \{x \in L : x\mathfrak{a} \leq \mathcal{O}_L\} \subseteq \mathcal{O}_L$ and is an ideal in $\mathcal{O}_L$. □

Proposition. Every non-zero fractional ideal is invertible. The inverse of $\mathfrak{q}$ is

$$\{x \in L : x\mathfrak{q} \subseteq \mathcal{O}_L\}.$$

Proof. Note that for any $n \in \mathcal{O}_L$ non-zero, we know $\mathfrak{q}$ is invertible if and only if $n\mathfrak{q}$ is invertible. So if the proposition is false, there is an integral ideal $\mathfrak{a} \lhd \mathcal{O}_L$ which is not invertible. Moreover, as $\mathcal{O}_L$ is Noetherian, we can assume $\mathfrak{a}$ is maximal with this property, i.e. if $\mathfrak{a} < \mathfrak{a}' < \mathcal{O}_L$, then $\mathfrak{a}'$ is invertible.

Let $\mathfrak{b} = \{x \in L : x\mathfrak{a} \subseteq \mathcal{O}_L\}$, a fractional ideal. We clearly have $\mathcal{O}_L \subseteq \mathfrak{b}$, and by our previous proposition, we know this inclusion is strict.

As $\mathcal{O}_L \subseteq \mathfrak{b}$, we know $\mathfrak{a} \subseteq \mathfrak{ab}$. Again, this inclusion is strict — if $\mathfrak{ab} = \mathfrak{a}$, then for all $x \in \mathfrak{b}$, we have $x\mathfrak{a} \subseteq \mathfrak{a}$, and we have shown that this implies $x \in \mathcal{O}_L$, but we cannot have $\mathfrak{b} \subseteq \mathcal{O}_L$.

So $\mathfrak{a} \subsetneq \mathfrak{ab}$. By assumption, we also have $\mathfrak{ab} \subseteq \mathcal{O}_L$, and since $\mathfrak{a}$ is not invertible, this is strict. But then by definition of $\mathfrak{a}$, we know $\mathfrak{ab}$ is invertible, which implies $\mathfrak{a}$ is invertible (if $\mathfrak{c}$ is an inverse of $\mathfrak{ab}$, then $\mathfrak{bc}$ is an inverse of $\mathfrak{a}$). This is a contradiction. So all fractional ideals must be invertible.

Finally, we have to show that the formula for the inverse holds. We write

$$\mathfrak{c} = \{x \in L : x\mathfrak{q} \subseteq \mathcal{O}_L\}.$$

Then by definition, we know $\mathfrak{q}^{-1} \subseteq \mathfrak{c}$. So

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

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

Corollary. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \lhd \mathcal{O}_L$ be ideals, $\mathfrak{c} \neq 0$. Then

(i) $\mathfrak{b} \subseteq \mathfrak{a}$ if and only if $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}\mathfrak{c}$

(ii) $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a}\mathfrak{c} \mid \mathfrak{b}\mathfrak{c}$

(iii) $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

Proof.

(i) ($\Rightarrow$) is clear, and ($\Leftarrow$) is obtained by multiplying with $\mathfrak{c}^{-1}$.

(ii) ($\Rightarrow$) is clear, and ($\Leftarrow$) is obtained by multiplying with $\mathfrak{c}^{-1}$.

(iii) ($\Rightarrow$) is clear. For the other direction, we notice that the result is easy if $\mathfrak{a} = \langle\alpha\rangle$ is principal. Indeed, if $\mathfrak{b} = \langle\beta_1, \cdots, \beta_r\rangle$, then $\mathfrak{b} \subseteq \langle\alpha\rangle$ means there are some $\beta_a', \cdots, \beta_r' \in \mathcal{O}_L$ such that $\beta_i = \beta_i'\alpha$. But this says

$$\langle\beta_a, \cdots, \beta_r\rangle = \langle\beta_1', \cdots, \beta_r'\rangle\langle\alpha\rangle,$$

So $\langle\alpha\rangle \mid \mathfrak{b}$.

In general, suppose we have $\mathfrak{b} \subseteq \mathfrak{a}$. By the proposition, there exists an ideal $\mathfrak{c} \lhd \mathcal{O}_L$ such that $\mathfrak{a}\mathfrak{c} = \langle\alpha\rangle$ is principal with $\alpha \in \mathcal{O}_L, \alpha \neq 0$. Then

- $\mathfrak{b} \subseteq \mathfrak{a}$ if and only if $\mathfrak{b}\mathfrak{c} \subseteq \langle\alpha\rangle$ by (i); and
- $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\langle\alpha\rangle \mid \mathfrak{b}\mathfrak{c}$ by (ii).

So the result follows. □

Theorem. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be an ideal, $\mathfrak{a} \neq 0$. Then $\mathfrak{a}$ can be written uniquely as a product of prime ideals.

Proof. To show existence, if $\mathfrak{a}$ is prime, then there is nothing to do. Otherwise, if $\mathfrak{a}$ is not prime, then it is not maximal. So there is some $\mathfrak{b} \supsetneq \mathfrak{a}$ with $\mathfrak{b} \lhd \mathcal{O}_L$. Hence $\mathfrak{b} \mid \mathfrak{a}$, i.e. there is some $\mathfrak{c} \lhd \mathcal{O}_L$ with $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, and $\mathfrak{c} \supseteq \mathfrak{a}$. We can continue factoring this way, and it must stop eventually, or else we have an infinite chain of strictly ascending ideals.

We prove uniqueness the usual way. We have shown $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. So if $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, with $\mathfrak{p}_i, \mathfrak{q}_j$ prime, then we know $\mathfrak{p}_1 \mid \mathfrak{q}_1 \cdots \mathfrak{q}_s$, which implies $\mathfrak{p}_1 \mid \mathfrak{q}_i$ for some i, and wlog $i = 1$. So $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. But $\mathfrak{q}_1$ is prime and hence maximal. So $\mathfrak{p}_1 = \mathfrak{q}_1$.

Multiply the equation $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ by $\mathfrak{p}_1^{-1}$, and we get $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Repeat, and we get $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ for all i (after renumbering). □

Corollary. The non-zero fractional ideals form a group under multiplication. We denote this I_L. This is a free abelian group generated by the prime ideals, i.e. any fractional ideal $\mathfrak{q}$ can be written uniquely as $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{q_r}$, with $\mathfrak{p}_i$ distinct prime ideals and $a_i \in \mathbb{Z}$.

Moreover, if $\mathfrak{q}$ is an integral ideal, i.e. $\mathfrak{q} \lhd \mathcal{O}_L$, then $a_i, \cdots, a_r \geq 0$.

Proof. We already have unique factorization of honest ideals. Now take any fractional ideal, and write it as $\mathfrak{q} = \mathfrak{a}\mathfrak{b}^{-1}$, with $\mathfrak{a}, \mathfrak{b} \in \mathcal{O}_L$ (e.g. take $\mathfrak{b} = \langle n \rangle$ for some n), and the result follows. □

Theorem. The following are equivalent:

(i) $\mathcal{O}_L$ is a principal ideal domain

(ii) $\mathcal{O}_L$ is a unique factorization domain

(iii) cl_L is trivial.

Proof. (i) and (iii) are equivalent by definition, while (i) implies (ii) is well-known from IB Groups, Rings and Modules. So the real content is (ii) to (i), which is specific to Dedekind domains.

If $\mathfrak{p} \lhd \mathcal{O}_L$ is prime, and $x \in \mathfrak{p} \setminus \{0\}$, we factor $x = \alpha_1 \cdots \alpha_k$ such that α_i is irreducible in $\mathcal{O}_L$. As $\mathfrak{p}$ is prime, there is some $\alpha_i \in \mathfrak{p}$. But then $\langle \alpha_i \rangle \subseteq \mathfrak{p}$, and $\langle \alpha_i \rangle$ is prime as $\mathcal{O}_L$ is a UFD. So we must have $\langle \alpha_i \rangle = \mathfrak{p}$ as prime ideals are maximal. So $\mathfrak{p}$ is principal. □

4 Norms of ideals

Proposition. For any ideal $\mathfrak{a}$, we have $N(\mathfrak{a}) \in \mathfrak{a} \cap \mathbb{Z}$.

Proof. It suffices to show that $N(\mathfrak{a}) \in \mathfrak{a}$. Viewing $\mathcal{O}_L/\mathfrak{a}$ as an additive group, the order of 1 is a factor of $N(\mathfrak{a})$. So $N(\mathfrak{a}) = N(\mathfrak{a}) \cdot 1 = 0 \in \mathcal{O}_L/\mathfrak{a}$. Hence $N(\mathfrak{a}) \in \mathfrak{a}$. □

Proposition. Let $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$ be ideals. Then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Proof. By the factorization into prime ideals, it suffices to prove this for $\mathfrak{b} = \mathfrak{p}$ prime, i.e.

$$N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p}).$$

In other words, we need to show that

$$\left|\frac{\mathcal{O}_L}{\mathfrak{a}}\right| = \left|\frac{\mathcal{O}_L}{\mathfrak{ap}}\right| \Big/ \left|\frac{\mathcal{O}_L}{\mathfrak{p}}\right|.$$

By the third isomorphism theorem, we already know that

$$\frac{\mathcal{O}_L}{\mathfrak{a}} \cong \left(\frac{\mathcal{O}_L}{\mathfrak{ap}}\right) \Big/ \left(\frac{\mathfrak{a}}{\mathfrak{ap}}\right).$$

So it suffices to show that $\mathcal{O}_L/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$ as abelian groups.

In the case of the integers, we could have, say, $\mathfrak{p} = 7\mathbb{Z}$, $\mathfrak{a} = 12\mathbb{Z}$. We would then simply define

$$\begin{aligned} \frac{\mathbb{Z}}{7\mathbb{Z}} &\longrightarrow \frac{12\mathbb{Z}}{7 \cdot 12\mathbb{Z}} \\ x &\longmapsto 12x \end{aligned}$$

However, in general, we do not know that $\mathfrak{a}$ is principal, but it turns out it doesn't really matter. We can just pick an arbitrary element to multiply with.

By unique factorization, we know $\mathfrak{a} \neq \mathfrak{ap}$. So we can find some $\alpha \in \mathfrak{a} \setminus \mathfrak{ap}$.

We now claim that the homomorphism of abelian groups

$$\begin{aligned} \frac{\mathcal{O}_L}{\mathfrak{p}} &\longrightarrow \frac{\mathfrak{a}}{\mathfrak{ap}} \\ x + \mathfrak{p} &\longmapsto \alpha x + \mathfrak{ap} \end{aligned}$$

is an isomorphism. We first check this is well-defined — if $p \in \mathfrak{p}$, then $\alpha\mathfrak{p} \in \mathfrak{ap}$ since $\alpha \in \mathfrak{a}$. So the image of $x+\mathfrak{p}$ and $(x+p)+\mathfrak{p}$ are equal. So this is well-defined.

To prove our claim, we have to show injectivity and surjectivity. To show injectivity, since $\langle\alpha\rangle \subseteq \mathfrak{a}$, we have $\mathfrak{a} \mid \langle a\rangle$, i.e. there is an ideal $\mathfrak{c} \subseteq \mathcal{O}_L$ such that $\mathfrak{ac} = \langle\alpha\rangle$. If $x \in \mathcal{O}_L$ is in the kernel of the map, then $\alpha x \in \mathfrak{ap}$. So

$$x\mathfrak{ac} \subseteq \mathfrak{ap}.$$

So

$$x\mathfrak{c} \subseteq \mathfrak{p}.$$

As $\mathfrak{p}$ is prime, either $\mathfrak{c} \subseteq \mathfrak{p}$ or $x \in \mathfrak{p}$. But $\mathfrak{c} \subseteq \mathfrak{p}$ implies $\langle\alpha\rangle = \mathfrak{ac} \subseteq \mathfrak{ap}$, contradicting the choice of α. So we must have $x \in \mathfrak{p}$, and the map is injective.

To show this is surjective, we notice that surjectivity means $\langle\alpha\rangle/\mathfrak{a}\mathfrak{p} = \mathfrak{a}/\mathfrak{a}\mathfrak{p}$, or equivalently $\mathfrak{a}\mathfrak{p} + \langle\alpha\rangle = \mathfrak{a}$.

Using our knowledge of fractional ideals, this is equivalent to saying $(\mathfrak{a}\mathfrak{p} + \langle\alpha\rangle)\mathfrak{a}^{-1} = \mathcal{O}_L$. But we know

$$\mathfrak{a}\mathfrak{p} < \mathfrak{a}\mathfrak{p} + \langle\alpha\rangle \subseteq \mathfrak{a}.$$

We now multiply by $\mathfrak{a}^{-1}$ to obtain

$$\mathfrak{p} < (\mathfrak{a}\mathfrak{p} + \langle\alpha\rangle)\mathfrak{a}^{-1} = \mathfrak{p} + \mathfrak{c} \subseteq \mathcal{O}_L.$$

Since $\mathfrak{p}$ is a prime, and hence maximal ideal, the last inclusion must be an equality. So $\mathfrak{a}\mathfrak{p} + \langle\alpha\rangle = \mathfrak{a}$, and we are done. □

Proof. It is enough to show that $N(\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}) = N(\mathfrak{p}_1)^{a_1}\cdots N(\mathfrak{p}_r)^{a_r}$ by unique factorization.

By the Chinese remainder theorem, we have

$$\frac{\mathcal{O}_L}{\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}} \cong \frac{\mathcal{O}_L}{\mathfrak{p}_1^{a_1}} \times \cdots \times \frac{\mathcal{O}_L}{\mathfrak{p}_r^{a_r}}$$

where $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ are distinct prime ideals.

Next, we show by hand that

$$\left|\frac{\mathcal{O}_L}{\mathfrak{p}^r}\right| = \left|\frac{\mathcal{O}_L}{\mathfrak{p}}\right| \times \left|\frac{\mathfrak{p}}{\mathfrak{p}^2}\right| \times \cdots \times \left|\frac{\mathfrak{p}^{r-1}}{\mathfrak{p}^r}\right| = \left|\frac{\mathcal{O}_L}{\mathfrak{p}}\right|^r,$$

by showing that $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ is a 1-dimensional vector space over the field $\mathcal{O}_L/\mathfrak{p}$. Then the result follows. □

Proposition. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be an ideal, $n = [L : \mathbb{Q}]$. Then

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

$$\mathfrak{a} = \left\{\sum r_i\alpha_i : r_i \in \mathbb{Z}\right\} = \bigoplus_1^n \alpha_i\mathbb{Z},$$

and $\alpha_1, \cdots, \alpha_n$ are a basis of L over $\mathbb{Q}$. In particular, $\mathfrak{a}$ is a free $\mathbb{Z}$-module of n generators.

(ii) For any such $\alpha_1, \cdots, \alpha_n$,

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

Lemma. Let M be a $\mathbb{Z}$-module (i.e. abelian group), and suppose $M \leq \mathbb{Z}^n$. Then $M \cong \mathbb{Z}^r$ for some $0 \leq r \leq n$.

Moreover, if $r = n$, then we can choose a basis $v_1, \cdots, v_n$ of M such that the change of basis matrix $A = (a_{ij}) \in M_{n\times n}(\mathbb{Z})$ is upper triangular, where

$$v_j = \sum a_{ij}e_i,$$

where $e_1, \cdots, e_n$ is the standard basis of $\mathbb{Z}^n$.

In particular,

$$|\mathbb{Z}^n/M| = |a_{11}a_{12}\cdots a_{nn}| = |\det A|.$$

Proof of proposition. Let $d \in \mathfrak{a} \cap \mathbb{Z}$, say $d = N(\alpha)$. Then $d\mathcal{O}_L \subseteq \mathfrak{a} \subseteq \mathcal{O}_L$. As abelian groups, after picking an integral basis $\alpha_1', \cdots, \alpha_n'$ of $\mathcal{O}_L$, we have

$$\mathbb{Z}^n \cong d\mathbb{Z}^n \leq \mathfrak{a} \leq \mathbb{Z}^n.$$

So $\mathfrak{a} \cong \mathbb{Z}^n$. Then the lemma gives us a basis $\alpha_1, \cdots, \alpha_n$ of $\mathfrak{a}$ as a $\mathbb{Z}$-module. As a $\mathbb{Q}$-module, since the α_i are obtained from linear combinations of α_i', by basic linear algebra, $\alpha_1, \cdots, \alpha_n$ is also a basis of L over $\mathbb{Q}$.

Moreover, we know that we have

$$\Delta(\alpha_1, \cdots, \alpha_n) = \det(A)^2 \Delta(\alpha_1', \cdots, \alpha_n').$$

Since $\det(A)^2 = |\mathcal{O}_L/\mathfrak{a}|^2 = N(\mathfrak{a})$ and $D_L = \Delta(\alpha_1', \cdots, \alpha_n')$ by definition, the second part follows. □

Corollary. Suppose $\mathfrak{a} \lhd \mathcal{O}_L$ has basis $\alpha_1, \cdots, \alpha_n$, and $\Delta(\alpha_1, \cdots, \alpha_n)$ is square-free. Then $\mathfrak{a} = \mathcal{O}_L$ (and D_L is square-free).

Proof. Immediate, since this forces $N(\mathfrak{a})^2 = 1$. □

Lemma. If $\alpha \in \mathcal{O}_L$, then

$$N(\langle\alpha\rangle) = |N_{L/\mathbb{Q}}(\alpha)|.$$

Proof. Let $\alpha_1, \cdots, \alpha_n$ be an integral basis of $\mathcal{O}_L$. Then $\alpha\alpha_1, .., \alpha\alpha_n$ is an integral basis of $\langle\alpha\rangle$. So by the previous lemma,

$$\Delta(\alpha\alpha_1, \cdots, \alpha\alpha_n) = N(\langle\alpha\rangle)^2 D_L.$$

But

$$\begin{aligned}
\Delta(\alpha\alpha_1, \cdots, \alpha\alpha_n) &= \det(\sigma_i(\alpha\alpha_j)_{ij})^2 \\
&= \det(\sigma_i(\alpha)\sigma_i(\alpha_j))^2 \\
&= \left(\prod_{i=1}^n \sigma_i(\alpha)\right)^2 \Delta(\alpha_1, \cdots, \alpha_n) \\
&= N_{L/\mathbb{Q}}(\alpha)^2 D_L.
\end{aligned}$$

So

$$N_{L/\mathbb{Q}}(\alpha)^2 = N(\langle\alpha\rangle)^2.$$

But $N(\langle\alpha\rangle)$ is positive. So the result follows. □

5 Structure of prime ideals

Lemma. Let $\mathfrak{p} \lhd \mathcal{O}_L$ be a prime ideal. Then there exists a unique $p \in \mathbb{Z}$, p prime, with $\mathfrak{p} \mid \langle p \rangle$. Moreover, $N(\mathfrak{p}) = p^f$ for some $1 \leq f \leq n$.

Proof. Well $\mathfrak{p} \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$, and hence principal. So $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some $p \in \mathbb{Z}$.

We now claim p is a prime integer. If $p = ab$ with $ab \in \mathbb{Z}$. Then since $p \in \mathfrak{p}$, either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. So $a \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ or $b \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. So $p \mid a$ or $p \mid b$.

Since $\langle p \rangle \subseteq \mathfrak{p}$, we know $\langle p \rangle = \mathfrak{p}\mathfrak{a}$ for some ideal $\mathfrak{a}$ by factorization. Taking norms, we get

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

So the result follows. □

Theorem (Dedekind's criterion)**.** Let $\alpha \in \mathcal{O}_L$ and $g(x) \in \mathbb{Z}[x]$ be its minimal polynomial. Suppose $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ has finite index, coprime to p (i.e. $p \nmid |\mathcal{O}_L/\mathbb{Z}[\alpha]|$). We write

$$\bar{g}(x) = g(x) \pmod{p},$$

so $\bar{g}(x) \in \mathbb{F}_p[x]$. We factor

$$\bar{g}(x) = \varphi_1^{e_1} \cdots \varphi_m^{e_m}$$

into distinct irreducibles in $\mathbb{F}_p[x]$. We define the ideal

$$\mathfrak{p}_i = \langle p, \tilde{\varphi}_i(\alpha) \rangle \lhd \mathcal{O}_L,$$

generated by p and $\tilde{\varphi}_i$, where $\tilde{\varphi}_i$ is any polynomial in $\mathbb{Z}[x]$ such that $\tilde{\varphi}_i \bmod p = \varphi_i$. Notice that if $\tilde{\varphi}'$ is another such polynomial, then $p \mid (\tilde{\varphi}_i - \varphi_i)$, so $\langle p, \tilde{\varphi}'(\alpha) \rangle = \langle p, \tilde{\varphi}(\alpha) \rangle$.

Then the $\mathfrak{p}_i$ are prime, and

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}.$$

Moreover, $f_i = \deg \varphi_i$, so $N(\mathfrak{a}) = p^{\deg \varphi_i}$.

Lemma. In $L = \mathbb{Q}(\sqrt{d})$,

(i) 2 splits in L if and only if $d \equiv 1 \pmod 8$;

(ii) 2 is inert in L if and only if $d \equiv 5 \pmod 8$;

(iii) 2 ramifies in L if $d \equiv 2, 3 \pmod 4$.

Proof.

– If $d \equiv 1 \pmod 4$, then then $\mathcal{O}_L = \mathbb{Z}[\alpha]$, where $\alpha = \frac{1}{2}(1 + \sqrt{d})$. This has minimal polynomial

$$x^2 - x + \frac{1}{4}(1 - d).$$

We reduce this mod 2.

- If $d \equiv 1 \pmod 8$, we get $x(x + 1)$. So 2 splits.
- If $d \equiv 5 \pmod 8$, then we get $x^2 + x + 1$, which is irreducible. So $\langle 2 \rangle$ is prime, hence 2 is inert.

– If $d \equiv 2, 3 \pmod 4$, then $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$, and $x^2 - d$ is the minimal polynomial. Taking mod 2, we get x^2 or $x^2 + 1 = (x+1)^2$. In both cases, 2 ramifies. □

Proof of Dedekind's criterion. The key claim is that

Claim. We have
$$\frac{\mathcal{O}_L}{\mathfrak{p}_i} \cong \frac{\mathbb{F}_p[x]}{\langle \varphi_i \rangle}.$$

Suppose this is true. Then since φ_i is irreducible, we know $\frac{\mathbb{F}_p[x]}{\langle \varphi_i \rangle}$ is a field. So $\mathfrak{p}_i$ is maximal, hence prime.

Next notice that
$$\mathfrak{p}_1^{e_1} = \langle p, \tilde{\varphi}_i(\alpha) \rangle^{e_i} \subseteq \langle p, \tilde{\varphi}_i(\alpha)^{e_i} \rangle.$$

So we have
$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m} \subseteq \langle p, \tilde{\varphi}_1(\alpha)^{e_1} \cdots \tilde{\varphi}_m(\alpha)^{e_m} \rangle = \langle p, g(\alpha) \rangle = \langle p \rangle,$$
using the fact that $g(\alpha) = 0$.

So to prove equality, we notice that if we put $f_i = \deg \varphi_i$, then $N(\mathfrak{p}_i) = p^{f_i}$, and
$$N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_m)^{e_m} = p^{\sum e_i f_i} = p^{\deg g}.$$
Since $N(\langle p \rangle) = p^n$, it suffices to show that $\deg g = n$. Since $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ has finite index, we know $\mathbb{Z}[\alpha] \cong \mathbb{Z}^n$. So $1, \alpha, \cdots, \alpha^{n-1}$ are independent over $\mathbb{Z}$, hence $\mathbb{Q}$. So $\deg g = [\mathbb{Q}(\alpha) : \mathbb{Q}] = n = [L : \mathbb{Q}]$, and we are done.

So it remains to prove that
$$\frac{\mathcal{O}_L}{\mathfrak{p}_i} \cong \frac{\mathbb{Z}[\alpha]}{\mathfrak{p}_i \cap \mathbb{Z}[\alpha]} \cong \frac{\mathbb{F}_p[x]}{\langle \varphi_i \rangle}.$$

The second isomorphism is clear, since
$$\frac{\mathbb{Z}[\alpha]}{\langle p, \tilde{\varphi}_i(\alpha) \rangle} \cong \frac{\mathbb{Z}[x]}{\langle p, \tilde{\varphi}_i(x), g(x) \rangle} \cong \frac{\mathbb{F}_p[x]}{\langle \tilde{\varphi}_i(x), g(x) \rangle} = \frac{\mathbb{F}_p[x]}{\langle \varphi_i(x), \bar{g}(x) \rangle} = \frac{\mathbb{F}_p[x]}{\langle \varphi_i \rangle}.$$

To prove the first isomorphism, it suffices to show that the following map is an isomorphism:
$$\begin{aligned} \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]} &\to \frac{\mathcal{O}_L}{p\mathcal{O}_L} \\ x + p\mathbb{Z}[\alpha] &\mapsto x + p\mathcal{O}_L \end{aligned} \tag{$*$}$$

If this is true, then quotienting further by $\tilde{\varphi}_i$ gives the desired isomorphism.

To prove the claim, we consider a slightly different map. We notice $p \nmid |\mathcal{O}_L/\mathbb{Z}[\alpha]|$ means the "multiplication by p" map
$$\frac{\mathcal{O}_L}{\mathbb{Z}[\alpha]} \xrightarrow{\ p\ } \frac{\mathcal{O}_L}{\mathbb{Z}[\alpha]} \tag{$\dagger$}$$

is injective. But $\mathcal{O}_L/\mathbb{Z}[\alpha]$ is a finite abelian group. So the map is an isomorphism.

By injectivity of ($\dagger$), we have $\mathbb{Z}[\alpha] \cap p\mathcal{O}_L = p\mathbb{Z}[\alpha]$. By surjectivity, we have $\mathbb{Z}[\alpha] + p\mathcal{O}_L = \mathcal{O}_L$. It thus follows that ($*$) is injective and surjective respectively.

So it is an isomorphism. We have basically applied the snake lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}[\alpha] & \hookrightarrow & \mathcal{O}_L & \twoheadrightarrow & \frac{\mathcal{O}_L}{\mathbb{Z}[\alpha]} & \longrightarrow & 0 \\ & & \downarrow p & & \downarrow p & & \downarrow p & & \\ 0 & \longrightarrow & \mathbb{Z}[\alpha] & \hookrightarrow & \mathcal{O}_L & \twoheadrightarrow & \frac{\mathcal{O}_L}{\mathbb{Z}[\alpha]} & \longrightarrow & 0 \end{array}$$

□

Corollary. If p is prime and $p < n = [L : \mathbb{Q}]$, and $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ has finite index coprime to p, then p does *not* split completely in $\mathcal{O}_L$.

Proof. By Dedekind's theorem, if $g(x)$ is the minimal polynomial of α, then the factorization of $\bar{g}(x) = g(x) \bmod p$ determines the factorization of $\langle p \rangle$ into prime ideals. In particular, p splits completely if and only if $\bar{g}$ factors into distinct linear factors, i.e.

$$\bar{g}(x) = (x - \alpha_1) \cdots (x - \alpha_n),$$

where $\alpha_i \in \mathbb{F}_p$ and α_i are distinct. But if $p < n$, then there aren't n distinct elements of $\mathbb{F}_p$! □

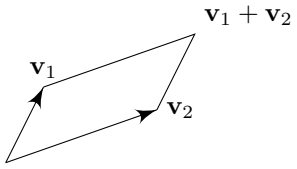
Theorem. $p \mid D_L$ if and only if p ramifies in $\mathcal{O}_L$.

6 Minkowski bound and finiteness of class group

Lemma (Minskowski's lemma)**.** Let $\Lambda = \mathbb{Z}\mathbf{v}_1 + \mathbb{Z}\mathbf{v}_2 \subseteq \mathbb{R}^2$ be a lattice, with $\mathbf{v}_1, \mathbf{v}_2$ linearly independent in $\mathbb{R}$ (i.e. $\mathbb{R}\mathbf{v}_1 + \mathbb{R}\mathbf{v}_2 = \mathbb{R}^2$). We write $\mathbf{v}_i = a_i\mathbf{e}_1 + b_i\mathbf{e}_2$. Then let

$$A(\Lambda) = \text{area of fundamental parallelogram} = \left|\det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}\right|,$$

where the fundamental parallelogram is the following:



Then a closed disc S around 0 contains a non-zero point of Λ if

$$\text{area}(S) \geq 4A(\Lambda).$$

In particular, there exists an $\alpha \in \Lambda$ with $\alpha \neq 0$, such that

$$0 < |\alpha|^2 \leq \frac{4A(\Lambda)}{\pi}.$$

Proof. We will prove a general result in any dimensions later. □

Proposition.

(i) If $\alpha = a + b\sqrt{\lambda}$, then as a complex number,

$$|\alpha|^2 = (a + b\sqrt{\lambda})(a - b\sqrt{\lambda}) = N(\alpha).$$

(ii) For $\mathcal{O}_L$, we have

$$A(\mathcal{O}_L) = \frac{1}{2}\sqrt{|D_L|}.$$

(iii) In general, we have

$$A(\mathfrak{a}) = \frac{1}{2}\sqrt{|\Delta(\alpha_1, \alpha_2)|},$$

where α_1, α_2 are the integral basis of $\mathfrak{a}$.

(iv) We have

$$A(\mathfrak{a}) = N(\mathfrak{a})A(\mathcal{O}_L).$$

Proof.

(i) This is clear.

(ii) We know $\mathcal{O}_L$ has basis $1, \alpha$, where again

$$\alpha = \begin{cases} \sqrt{d} & d \equiv 2, 3 \pmod 4 \\ \frac{1}{2}(1 + \sqrt{d}) & d \equiv 1 \pmod 4 \end{cases}.$$

So we can just look at the picture of the lattice, and compute to get

$$A(\mathcal{O}_L) = \begin{cases} \sqrt{|d|} & d \equiv 2, 3 \pmod 4 \\ \frac{1}{2}\sqrt{|d|} & d \equiv 1 \pmod 4 \end{cases} = \frac{1}{2}\sqrt{|D_L|}.$$

(iii) If α_1, α_2 are the integral basis of $\mathfrak{a}$, then the lattice of $\mathfrak{a}$ is in fact spanned by the vectors $\alpha_1 = a + bi, \alpha_2 = a' + b'i$. This has area

$$A(\mathfrak{a}) = \det \begin{pmatrix} a & b \\ a' & b' \end{pmatrix},$$

whereas we have

$$\begin{aligned} \Delta(\alpha_1, \alpha_2) &= \det \begin{pmatrix} \alpha_1 & \bar{\alpha}_1 \\ \alpha_2 & \bar{\alpha}_2 \end{pmatrix}^2 \\ &= (\alpha_1\bar{\alpha}_2 - \alpha_2\bar{\alpha}_1)^2 \\ &= \operatorname{Im}(2\alpha_1\bar{\alpha}_2)^2 \\ &= 4(a'b - ab')^2 \\ &= 4A(\mathfrak{a})^2. \end{aligned}$$

(iv) This follows from (ii) and (iii), as

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

in general. □

Proposition (Minkowski bound)**.** For all $[\mathfrak{a}] \in \mathrm{cl}_L$, there is a representative $\mathfrak{b}$ of $[\mathfrak{a}]$ (i.e. an ideal $\mathfrak{b} \leq \mathcal{O}_L$ such that $[\mathfrak{b}] = [\mathfrak{a}]$) such that

$$N(\mathfrak{b}) \leq c_L = \frac{2\sqrt{|D_L|}}{\pi}.$$

Proof. Find the $\mathfrak{b}$ such that $[\mathfrak{b}] = [(\mathfrak{a}^{-1})^{-1}]$ and $N(\mathfrak{b}) \leq c_L$. □

Lemma. For every $n \in \mathbb{Z}$, there are only finitely many ideals $\mathfrak{a} \leq \mathcal{O}_L$ with $N(\mathfrak{a}) = m$.

Proof. If $N(\mathfrak{a}) = m$, then by definition $|\mathcal{O}_L/\mathfrak{a}| = m$. So $m \in \mathfrak{a}$ by Lagrange's theorem. So $\langle m \rangle \subseteq \mathfrak{a}$, i.e. $\mathfrak{a} \mid \langle m \rangle$. Hence $\mathfrak{a}$ is a factor of $\langle m \rangle$. By unique factorization of prime ideals, there are only finitely many such ideals. □

Proof. Each ideal bijects with an ideal in $\mathcal{O}_L/m\mathcal{O}_L = (\mathbb{Z}/m)^n$. So there are only finitely many. □

Theorem. The class group cl_L is a finite group, and the divisors of ideals of the form $\langle p \rangle$ for $p \in \mathbb{Z}$, p a prime, and $0 < p < c_L$, collectively generate cl_L.

Proof.

(i) Each element is represented by an ideal of norm less than $2\sqrt{|D_L|}/\pi$, and there are only finitely many ideals of each norm.

(ii) Given any element of cl_L, we pick a representative $\mathfrak{a}$ such that $N(\mathfrak{a}) < c_L$. We factorize

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Then

$$N(\mathfrak{p}_i) \leq N(\mathfrak{a}) < c_L.$$

Suppose $\mathfrak{p}_i \mid \langle p \rangle$. Then $N(\mathfrak{p})$ is a power of p, and is thus at least p. So $p < c_L$. □

Theorem. Let $L = \mathbb{Q}(\sqrt{d})$ with $d < 0$. Then $\mathcal{O}_L$ is a UFD if

$$-d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Moreover, this is actually an "if and only if".

Proposition. Suppose $\Lambda \subseteq \mathbb{R}^n$ is a subgroup. Then Λ is a discrete subgroup of $(\mathbb{R}^n, +)$ if and only if

$$\Lambda = \left\{\sum_1^m n_i \mathbf{x}_i : n_i \in \mathbb{Z}\right\}$$

for some $\mathbf{x}_1, \cdots, \mathbf{x}_m$ linearly independent over $\mathbb{R}$.

Proof. Suppose Λ is generated by $\mathbf{x}_1, \cdots, \mathbf{x}_m$. By linear independence, there is some $g \in \mathrm{GL}_n(\mathbb{R})$ such that $g\mathbf{x}_i = \mathbf{e}_i$ for all $1 \leq i \leq m$, where $\mathbf{e}_1, \cdots, \mathbf{e}_n$ is the standard basis. We know acting by g preserves discreteness, since it is a homeomorphism, and $g\Lambda = \mathbb{Z}^m \subseteq \mathbb{R}^m \times \mathbb{R}^{n-m}$ is clearly discrete (take $\varepsilon = \frac{1}{2}$). So this direction follows.

For the other direction, suppose Λ is discrete. We pick $\mathbf{y}_1, \cdots, \mathbf{y}_m \in \Lambda$ which are linearly independent over $\mathbb{R}$, with m maximal (so $m \leq n$). Then by maximality, we know

$$\left\{\sum_{i=1}^m \lambda_i \mathbf{y}_i : \lambda_i \in \mathbb{R}\right\} = \left\{\sum_1^m \lambda_i \mathbf{z}_i : \lambda_i \in \mathbb{R}, \mathbf{z}_i \in \Lambda\right\},$$

and this is the smallest vector subspace of $\mathbb{R}^n$ containing Λ. We now let

$$X = \left\{\sum_{i=1}^m \lambda_i \mathbf{y}_i : \lambda_i \in [0, 1]\right\} \cong [0, 1]^m.$$

This is closed and bounded, and hence compact. So $X \cap \Lambda$ is finite.

Also, we know

$$\bigoplus \mathbb{Z}\mathbf{y}_i = \mathbb{Z}^m \subseteq \Lambda,$$

and if γ is any element of Λ, we can write it as $\gamma = \gamma_0 + \gamma_1$, where $\gamma_0 \in X$ and $\gamma_1 \in \mathbb{Z}^m$. So

$$\left|\frac{\Lambda}{\mathbb{Z}^m}\right| \leq |X \cap \Lambda| < \infty.$$

So let $d = |\Lambda/\mathbb{Z}^m|$. Then $d\Lambda \subseteq \mathbb{Z}^m$, i.e. $\Lambda \subseteq \frac{1}{d}\mathbb{Z}^m$. So

$$\mathbb{Z}^m \subseteq \Lambda \subseteq \frac{1}{d}\mathbb{Z}^m.$$

So Λ is a free abelian group of rank m. So there exists $\mathbf{x}_1, \cdots, \mathbf{x}_m \in \frac{1}{d}\mathbb{Z}^m$ which is an integral basis of Λ and are linearly independent over $\mathbb{R}$. □

Theorem (Minkowski's theorem)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, and P be a fundamental domain. We let $S \subseteq \mathbb{R}^n$ be a measurable set, i.e. one for which $\mathrm{vol}(S)$ is defined.

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

(ii) Suppose $\mathbf{0} \in S$, and S is symmetric around 0, i.e. $\mathbf{s} \in S$ if and only if $-\mathbf{s} \in S$, and S is convex, i.e. for all $\mathbf{x}, \mathbf{y} \in S$ and $\lambda \in [0, 1]$, then

$$\lambda \mathbf{x} + (1 - \lambda)\mathbf{y} \in S.$$

Then suppose either

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

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

Then S contains a $\gamma \in \Lambda$ with $\gamma \neq 0$.

Proof.

(i) Suppose $\mathrm{vol}(S) > \operatorname{covol}(\Lambda) = \mathrm{vol}(P)$. Since $P \subseteq \mathbb{R}^n$ is a fundamental domain, we have

$$\mathrm{vol}(S) = \mathrm{vol}(S \cap \mathbb{R}^n) = \mathrm{vol}\left(S \cap \sum_{\gamma \in \Lambda} (P + \gamma)\right) = \sum_{\gamma \in \Lambda} \mathrm{vol}(S \cap (P + \gamma)).$$

Also, we know

$$\mathrm{vol}(S \cap (P + \gamma)) = \mathrm{vol}((S - \gamma) \cap P),$$

as volume is translation invariant. We now claim the sets $(S - \gamma) \cap P$ for $\gamma \in \Lambda$ are *not* pairwise disjoint. If they were, then

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

contradicting our assumption.

Then in particular, there are some distinct γ and μ such that $(S - \gamma)$ and $(S - \mu)$ are not disjoint. In other words, there are $\mathbf{x}, \mathbf{y} \in S$ such that $\mathbf{x} - \gamma = \mathbf{y} - \mu$, i.e. $\mathbf{x} - \mathbf{y} = \gamma - \mu \in \Lambda \neq 0$.

(ii) We now let

$$S' = \frac{1}{2} S = \left\{ \frac{1}{2} s : s \in S \right\}.$$

So we have

$$\mathrm{vol}(S') = 2^{-n} \mathrm{vol}(S) > \operatorname{covol}(\Lambda),$$

by assumption.

(a) So there exists some distinct $\mathbf{y}, \mathbf{z} \in S'$ such that $\mathbf{y} - \mathbf{z} \in \Lambda \setminus \{0\}$. We now write

$$\mathbf{y} - \mathbf{z} = \frac{1}{2}(2\mathbf{y} + (-2\mathbf{z})),$$

Since $2\mathbf{z} \in S$ implies $-2\mathbf{z} \in S$ by symmetry around $\mathbf{0}$, so we know $\mathbf{y} - \mathbf{z} \in S$ by convexity.

(b) We apply the previous part to $S_m = \left(1 + \frac{1}{m}\right) S$ for all $m \in \mathbb{N}$, $m > 0$. So we get a non-zero $\gamma_m \in S_m \cap \Lambda$.

By convexity, we know $S_m \subseteq S_1 = 2S$ for all m. So $\gamma_1, \gamma_2, \cdots \in S_1 \cap \Lambda$. But S_1 is compact set. So $S_1 \cap \Lambda$ is finite. So there exists γ such that γ_m is γ infinitely often. So

$$\gamma \in \bigcap_{m \geq 0} S_m = S.$$

So $\gamma \in S$. □

Lemma.

(i) $\sigma(\mathcal{O}_L)$ is a lattice in $\mathbb{R}^n$ of covolume $2^{-s}|D_L|^{\frac{1}{2}}$.

(ii) More generally, if $\mathfrak{a} \lhd \mathcal{O}_L$ is an ideal, then $\sigma(\mathfrak{a})$ is a lattice and the covolume

$$\operatorname{covol}(\sigma(\mathfrak{a})) = 2^{-s}|D_L|^{\frac{1}{2}} N(\mathfrak{a}).$$

Proof. Obviously (ii) implies (i). So we just prove (ii). Recall that $\mathfrak{a}$ has an integral basis $\gamma_1, \cdots, \gamma_n$. Then $\mathfrak{a}$ is the integer span of the vectors

$$(\sigma_1(\gamma_i), \sigma_2(\gamma_i), \cdots, \sigma_{r+s}(\gamma_i))$$

for $i = 1, \cdots, n$, and they are independent as we will soon see when we compute the determinant. So it is a lattice.

We also know that

$$\Delta(\gamma_1, \cdots, \gamma_n) = \det(\sigma_i(\gamma_j))^2 = N(\mathfrak{a})^2 D_L,$$

where the σ_i run over all $\sigma_1, \cdots, \sigma_r, \sigma_{r+1}, \cdots, \sigma_{r+s}, \bar{\sigma}_{r+1}, \cdots \bar{\sigma}_{r+s}$.

So we know

$$|\det(\sigma_i(\gamma_j))| = N(\mathfrak{a})|D_L|^{\frac{1}{2}}.$$

So what we have to do is to relate $\det(\sigma_i(\gamma_j))$ to the covolume of $\sigma(\mathfrak{a})$. But these two expressions are very similar.

In the $\sigma_i(\gamma_j)$ matrix, we have columns that look like

$$\begin{pmatrix} \sigma_{r+i}(\gamma_j) & \bar{\sigma}_{r+i}(\gamma_j) \end{pmatrix} = \begin{pmatrix} z & \bar{z} \end{pmatrix}.$$

On the other hand, the matrix of $\sigma(\gamma)$ has corresponding entries

$$\begin{pmatrix} \operatorname{Re}(z) & \operatorname{Im}(z) \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(z + \bar{z}) & \frac{i}{2}(\bar{z} - z) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \begin{pmatrix} z \\ \bar{z} \end{pmatrix}$$

We call the last matrix $A = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$. We can compute the determinant as

$$|\det A| = \left| \det \frac{1}{2} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \right| = \frac{1}{2}.$$

Hence the change of basis matrix from $(\sigma_i(\gamma_j))$ to $\sigma(\gamma)$ is s diagonal copies of A, so has determinant 2^{-s}. So this proves the lemma. □

Proposition. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be an ideal. Then there exists an $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$ such that

$$|N(\alpha)| \leq c_L N(\mathfrak{a}),$$

where

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

Proof. Let

$$B_{r,s}(t) = \left\{(y_1, \cdots, y_r, z_1, \cdots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : \sum |y_i| + 2\sum |z_i| \leq t\right\}.$$

This

(i) is closed and bounded;

(ii) is measurable (it is defined by polynomial inequalities);

(iii) has volume

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

(iv) is convex and symmetric about 0.

Only (iii) requires proof, and it is on the second example sheet, i.e. we are not doing it here. It is just doing the integral.

We now choose t so that

$$\mathrm{vol}\, B_{r,s}(t) = 2^n \,\mathrm{covol}(\sigma(\mathfrak{a})).$$

Explicitly, we let

$$t^n = \left(\frac{4}{\pi}\right)^s n! |D_L|^{1/2} N(\mathfrak{a}).$$

Then by Minkowski's lemma, there is some $\alpha \in \mathfrak{a}$ non-zero such that $\sigma(\alpha) \in B_{r,s}(t)$. We write

$$\sigma(\alpha) = (y_1, \cdots, y_r, z_1, \cdots, z_s).$$

Then we observe

$$N(\alpha) = y_1 \cdots y_r z_1 \bar{z}_1 z_2 \bar{z}_2 \cdots z_s \bar{z}_s = \prod y_i \prod |z_j|^2.$$

By the AM-GM inequality, we know

$$|N(\alpha)|^{1/n} \leq \frac{1}{n}\left(\sum y_i + 2\sum |z_j|\right) \leq \frac{t}{n},$$

as we know $\sigma(\mathfrak{a}) \in B_{r,s}(t)$. So we get

$$|N(\alpha)| \leq \frac{t^n}{n^n} = c_L N(\mathfrak{a}). \qquad \square$$

Corollary. Every $[\mathfrak{a}] \in \mathrm{cl}_L$ has a representative $\mathfrak{a} \in \mathcal{O}_L$ with $N(\mathfrak{a}) \leq c_L$.

Theorem (Dirichlet)**.** The class group cl_L is finite, and is generated by prime ideals of norm $\leq c_L$.

Proof. Just as the case for imaginary quadratic fields. $\square$

7 Dirichlet's unit theorem

Theorem (Dirichlet unit theorem)**.** We have the isomorphism

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

where

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

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

Theorem (Pell's equation)**.** There are infinitely many $x + y\sqrt{d} \in \mathcal{O}_L$ such that $x^2 - dy^2 = \pm 1$.

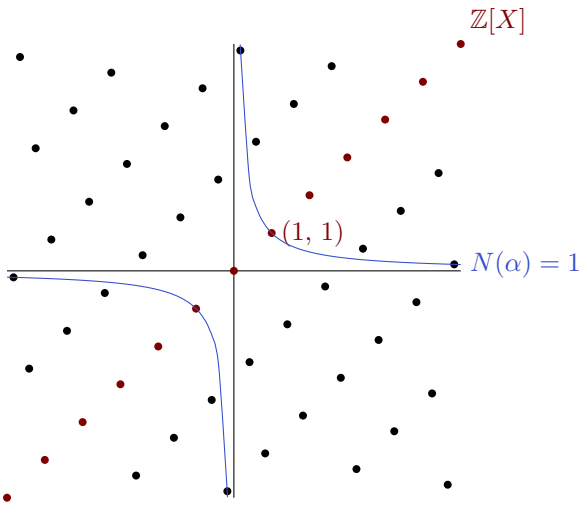
Proof. Recall that $\sigma : \mathcal{O}_L \to \mathbb{R}^2$ sends

$$\alpha = x + y\sqrt{d} \mapsto (\sigma_1(\alpha), \sigma_2(\alpha)) = (x + y\sqrt{d}, x - y\sqrt{d}).$$

(in the domain, $\sqrt{d}$ is a formal symbol, while in the codomain, it is a real number, namely the positive square root of d)

Also, we know

$$\operatorname{covol}(\sigma(\mathcal{O}_L)) = |D_L|^{\frac{1}{2}}.$$



Consider

$$s_t = \left\{(y_1, y_2) \in \mathbb{R}^2 : |y_1| \le t, |y_2| \le \frac{|D_L|^{1/2}}{t}\right\}.$$

So

$$\operatorname{vol}(s_t) = 4|D_L|^{\frac{1}{2}} = 2^n \operatorname{covol}(\mathcal{O}_L),$$

as $n = [L : \mathbb{Q}] = 2$. Now Minkowski implies there is an $\alpha \in \mathcal{O}_L$ non-zero such that $\sigma(\alpha) \in s_t$. Also, if we write

$$\sigma(\alpha) = (y_1, y_2),$$

then

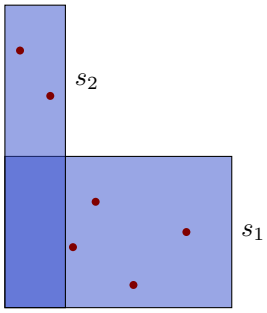
$$N(\alpha) = y_1 y_2.$$

So such an α will satisfy

$$1 \leq |N(\alpha)| \leq |D_L|^{1/2}.$$

This is not quite what we want, since we need $|N(\alpha)| = 1$ exactly. Nevertheless, this is a good start. So let's try to find infinitely such elements.

First notice that no points on the lattice (apart from the origin) hits the x or y axis, since any such point must satisfy $x \pm y\sqrt{d} = 0$, but $\sqrt{d}$ is not rational. Also, s_t is compact. So $s_t \cap \sigma(\mathcal{O}_L)$ contains finitely many points. So we can find a t_2 such that for each $(y_1, y_2) \in s_t \cap \mathcal{O}_L$, we have $|y_1| > t_2$. In particular, s_{t_2} does not contain any point in $s_t \cap \sigma(\mathcal{O}_L)$. So we get a new set of points $\alpha \in s_{t_2} \cap \mathcal{O}_L$ such that $1 \leq |N(\alpha)| \leq |D_L|^{1/2}$.



We can do the same thing for s_{t_2} and get a new t_3. In general, given $t_1 > \cdots > t_n$, pick t_{n+1} be such that

$$0 < t_{n+1} < \min\left\{|y_1| : (y_1, y_2) \in \bigcup_{i=1}^{n} s_{t_i} \cap \sigma(\mathcal{O}_L)\right\},$$

and the minimum is finite since s_t is compact and hence contains finitely many lattice points on $\sigma(\mathcal{O}_L)$.

Then we get an infinite sequence of t_i such that $s_{t_i} \cap \sigma(\mathcal{O}_L)$ are disjoint for different i. Since each must contain at least one point, we have got infinitely many points in $\mathcal{O}_L$ satisfying $1 \leq |N(\alpha)| \leq |D_L|^{1/2}$.

Since there are only finitely many integers between 1 and $|D_L|^{1/2}$, we can apply the pigeonhole principle, and get that there is some integer satisfying $1 \leq |m| \leq |D_L|^{1/2}$ such that there exists infinitely many $\alpha \in \mathcal{O}_L$ with $N(\alpha) = m$.

This is not quite good enough. We consider

$$\mathcal{O}_L/m\mathcal{O}_L \cong (\mathbb{Z}/m\mathbb{Z})^{[L:\mathbb{Q}]},$$

another finite set. We notice that each $\alpha \in \mathcal{O}_L$ must fall into one of finitely many the cosets of $m\mathcal{O}_L$ in $\mathcal{O}_L$. In particular, each α such that $N(\alpha) = m$ must belong to one of these cosets.

So again by the pigeonhole principle, there exists a $\beta \in \mathcal{O}_L$ with $N(\beta) = m$, and infinitely many $\alpha \in \mathcal{O}_L$ with $N(\alpha) = m$ and $\alpha = \beta \pmod{m\mathcal{O}_L}$.

Now of course α and β are not necessarily units, if $m \neq 1$. However, we will show that α/β is. The hard part is of course showing that it is in $\mathcal{O}_L$ itself, because it is clear that α/β has norm 1 (alternatively, by symmetry, β/α is in $\mathcal{O}_L$, so an inverse exists).

Hence all it remains is to prove the general fact that if

$$\alpha = \beta + m\gamma,$$

where $\alpha, \beta, \gamma \in \mathcal{O}_L$ and $N(\alpha) = N(\beta) = m$, then $\alpha/\beta \in \mathcal{O}_L$.

To show this, we just have to compute

$$\frac{\alpha}{\beta} = 1 + \frac{m}{\beta}\gamma = 1 + \frac{N(\beta)}{\beta}\gamma = 1 + \bar{\beta}\gamma \in \mathcal{O}_L,$$

since $N(\beta) = \beta\bar{\beta}$. So done. □

Theorem (Dirchlet's unit theorem for real quadratic fields)**.** Let $L = \mathbb{Q}(\sqrt{d})$. Then there is some $\varepsilon_0 \in \mathcal{O}_L^\times$ such that

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

We call such an ε_0 a *fundamental unit* (which is not unique). So

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

Proof. We have just proved the really powerful theorem that there are infinitely many ε with $N(\varepsilon) = 1$. We are not going to need the full theorem. All we need is that there are three — in particular, something that is not ± 1.

We pick some $\varepsilon \in \mathcal{O}_L^\times$ with $\varepsilon \neq \pm 1$. This exists by what we just proved. Then we know

$$|\sigma_1(\varepsilon)| \neq 1,$$

as $|\sigma_1(\varepsilon)| = 1$ if and only if $\varepsilon = \pm 1$. Replacing by ε^{-1} if necessary, we wlog $E = |\sigma_1(\varepsilon)| > 1$. Now consider

$$\{\alpha \in \mathcal{O}_L : N(\alpha) = \pm 1, 1 \leq |\sigma_1(\alpha)| \leq E\}.$$

This is again finite, since it is specified by a compact subset of the $\mathcal{O}_L$-lattice. So we pick ε_0 in this set with $\varepsilon_0 \neq \pm 1$ and $|\sigma_1(\varepsilon_0)|$ minimal (> 1). Replacing ε_0 by $-\varepsilon_0$ if necessary, we can assume $\sigma_1(\varepsilon) > 1$.

Finally, we claim that if $\varepsilon \in \mathcal{O}_L^\times$ and $\sigma_1(\varepsilon) > 0$, then $\varepsilon = \varepsilon_0^N$ for some $N \in \mathbb{Z}$. This is obvious if we have addition instead of multiplication. So we take logs.

Suppose

$$\frac{\log \varepsilon}{\log \varepsilon_0} = N + \gamma,$$

where $N \in \mathbb{Z}$ and $0 \leq \gamma < 1$. Then we know

$$\varepsilon\varepsilon_0^{-N} = \varepsilon_0^\gamma \in \mathcal{O}_L^\times,$$

but $|\varepsilon_0^\gamma| = |\varepsilon_0|^\gamma < |\varepsilon_0|$, as $|\varepsilon_0| > 1$. By our choice of ε_0, we must have $\gamma = 0$. So done. □

Theorem (Dirichlet unit theorem)**.** We have the isomorphism

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

where

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

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

Proof. We do the proof in the opposite order. We throw in the logarithm at the very beginning. We define

$$\ell : \mathcal{O}_L^\times \to \mathbb{R}^{r+s}$$

by

$$x \mapsto (\log|\sigma_1(x)|, \cdots, \log|\sigma_r(x)|, 2\log|\sigma_{r+1}(x)|, \cdots, 2\log|\sigma_{r+s}(x)|).$$

Note that $|\sigma_{r+i}(x)| = |\overline{\sigma_{r+\ell}(x)}|$. So this is independent of the choice of one of $\sigma_{r+i}, \bar{\sigma}_{r+i}$.

Claim. We now claim that $\operatorname{im}\ell$ is a discrete group in $\mathbb{R}^{r+s}$ and $\ker\ell = \mu_L$ is a finite cyclic group.

We note that

$$\log|ab| = \log|a| + \log|b|.$$

So this is a group homomorphism, and the image is a subgroup. To prove the first part, it suffices to show that $\operatorname{im}\ell \cap [-A, A]^{r+s}$ is finite for all $A > 0$. We notice ℓ factors as

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

where σ maps $\alpha \mapsto (\sigma_1(\alpha), \cdots, \sigma_{r+s}(\alpha))$, and

$$j : (y_1, \cdots, y_r, z_1, \cdots, z_s) \mapsto (\log|y_1|, \cdots, \log|y_r|, 2\log|z_1|, \cdots, 2\log|z_2|).$$

We see

$$j^{-1}([-A, A]^{r+s}) = \{(y_i, z_j) : e^{-A} \le |y_i| \le e^A, e^{-A} \le 2|z_j| \le e^A\}$$

is a compact set, and $\sigma(\mathcal{O}_L)$ is a lattice, in particular discrete. So $\sigma(\mathcal{O}_L) \cap j^{-1}([-A, A]^{r+s})$ is finite. This also shows the kernel is finite, since the kernel is the inverse image of a compact set.

Now as $\ker\ell$ is finite, all elements are of finite order. So $\ker\ell \subseteq \mu_L$. Conversely, it is clear that $\mu_L \subseteq \ker\ell$. So it remains to show that μ_L is cyclic. Since L embeds in $\mathbb{C}$, we know μ_L is contained in the roots of unity in $\mathbb{C}$. Since μ_L is finite, we know L is generated by a root of unity with the smallest argument (from, say, IA Groups).

Claim. We claim that

$$\operatorname{im}\ell \subseteq \left\{(y_1, \cdots, y_{r+s}) : \sum y_i = 0\right\} \cong \mathbb{R}^{r+s-1}.$$

To show this, note that if $\alpha \in \mathcal{O}_L^\times$, then

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \prod_{\ell=1}^{s} \sigma_{r+\ell}(\alpha)\bar{\sigma}_{r+\ell} = \pm 1.$$

Taking the log of the absolute values, we get

$$0 = \sum \log|\sigma_i(\alpha)| + 2\sum \log|\sigma_{r+i}(\alpha)|.$$

So we know $\operatorname{im} \ell \subseteq \mathbb{R}^{r+s-1}$ as a discrete subgroup. So it is isomorphic to $\mathbb{Z}^a$ for some $a \leq r+s-1$. Then what we want to show is that $\operatorname{im} \ell \subseteq \mathbb{R}^{r+s-1}$ is a lattice, i.e. it is congruent to $\mathbb{Z}^{r+s-1}$.

Note that so far what we have done is the second part of what we did for the real quadratic fields. We took the logarithm to show that these form a discrete subgroup. Next, we want to find $r+s-1$ independent elements to show it is a lattice.

Claim. Fix a k such that $1 \leq k \leq r+s$ and $\alpha \in \mathcal{O}_L$ with $\alpha \neq 0$. Then there exists a $\beta \in \mathcal{O}_L$ such that

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

and moreover if we write

$$\begin{aligned} \ell(\alpha) &= (a_1, \cdots, a_{r+s}) \\ \ell(\beta) &= (b_1, \cdots, b_{r+s}), \end{aligned}$$

then we have $b_i < a_i$ for all $i \neq k$.

We can apply Minkowski to the region

$$S = \{(y_1, \cdots, y_r, z_1, \cdots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |y_i| \leq c_i, |z_j| \leq c_{r+j}\}$$

(we will decide what values of c_i to take later). Then this has volume

$$\operatorname{vol}(S) = 2^r \pi^s c_1 \cdots c_{r+s}.$$

We notice S is convex and symmetric around 0. So if we choose $0 < c_i < e^{a_i}$ for $i \neq k$, and choose

$$c_k = \left(\frac{2}{\pi}\right)^s |D_L|^{1/2} \frac{1}{c_1 \cdots \hat{c}_k \cdots c_{r+s}}.$$

Then Minkowski gives $\beta \in \sigma(\mathcal{O}_L) \cap S$, satisfying the two conditions above.

Claim. For any $k = 1, \cdots, r+s$, there is a unit $u_k \in \mathcal{O}_L^\times$ such that if $\ell(u_k) = (y_1, \cdots, y_{r+s}$, then $y_i < 0$ for all $i \neq k$ (and hence $y_k > 0$ since $\sum y_i = 0$).

This is just as in the proof for the real quadratic case. We can repeatedly apply the previous claim to get a sequence $\alpha_1, \alpha_2, \cdots \in \mathcal{O}_L$ such that $N(\alpha_t)$ is bounded for all t, and for all $i \neq k$, the ith coordinate of $\ell(\alpha_1), \ell(\alpha_2), \cdots$ is strictly decreasing. But then as with real quadratic fields, the pigeonhole principle implies we can find t, t' such that

$$N(\alpha_t) = N(\alpha_{t'}) = m,$$

say, *and*

$$\alpha_t \equiv \alpha_{t'} \pmod{m\mathcal{O}_L},$$

i.e. $\alpha_t = \alpha_{t'}$ in $\mathcal{O}_L/m\mathcal{O}_L$. Hence for each k, we get a unit $u_k = \alpha_t/\alpha_{t'}$ such that

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

has $y_i < 0$ if $i \neq k$ (and hence $y_k > 0$, since $\sum y_i = 0$). We need a final trick to show the following:

Claim. The units $u_1, \cdots, u_{r+s-1}$ are linearly independent in $\mathbb{R}^{r+s-1}$. Hence the rank of $\ell(\mathcal{O}_L^\times) = r + s - 1$, and Dirichlet's theorem is proved.

We let A be the $(r+s) \times (r+s)$ matrix whose jth row is $\ell(u_j)$, and apply the following lemma:

Claim. Let $A \in \mathrm{Mat}_m(\mathbb{R})$ be such that $a_{ii} > 0$ for all i and $a_{ij} < 0$ for all $i \neq j$, and $\sum_j a_{ij} \geq 0$ for each i. Then $\mathrm{rank}(A) \geq m - 1$.

To show this, we let $\mathbf{v}_i$ be the ith column of A. We show that $\mathbf{v}_1, \cdots, \mathbf{v}_{m-1}$ are linearly independent. If not, there exists a sequence $t_i \in \mathbb{R}$ such that

$$\sum_{i=1}^{m-1} t_i \mathbf{v}_i = 0, \tag{$*$}$$

with not all of the t_i non-zero. We choose k so that $|t_k|$ is maximal among the $t_1, \cdots, t_{m-1}$'s. We divide the whole equation by t_k. So we can wlog assume $t_k = 1$, $t_i \leq 1$ for all i.

Now consider the kth row of $(*)$. We get

$$0 = \sum_{i=1}^{m-1} t_i a_{ki} \geq \sum_{i=1}^{m-1} a_{ki},$$

as $a < 0$ and $t \leq 1$ implies $at \geq a$. Moreover, we know $a_{mi} > 0$ strictly. So we get

$$0 > \sum_{i=1}^{m} a_{ki} \geq 0.$$

This is a contradiction. So done. □

Lemma.

(i) If $d = -1$, then $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \mathbb{Z}/4\mathbb{Z}$.

(ii) If $d = -3$, then let $\omega = \frac{1}{2}(1 + \sqrt{d})$, and we have $\omega^6 = 1$. So $\mathbb{Z}[\omega]^\times = \{1, \omega, \cdots, \omega^5\} \cong \mathbb{Z}/6\mathbb{Z}$.

(iii) For any other $d < 0$, we have $\mathcal{O}_L^\times = \{\pm 1\}$.

Proof. This is just a direct check.

If $d \equiv 2, 3 \pmod 4$, then by looking at the solution of $x^2 - dy^2 = \pm 1$ in the integers, we get (i) and (iii).

If $d \equiv 1 \pmod 4$, then by looking at the solutions to $\left(x + \frac{y}{2}\right)^2 - \frac{d}{4}y^2 = \pm 1$ in the integers, we get (ii) and (iii). □

8 L-functions, Dirichlet series*

Theorem (Euclid)**.** There are infinitely many primes.

Proof. Consider the function

$$\prod_{p \text{ primes}} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \text{ prime}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \sum_{n>0} \frac{1}{n}.$$

This is since every $n = p_1^{e_1} \cdots p_r^{e_r}$ factors uniquely as a product of primes, and each such product appears exactly once in this. If there were finitely many primes, as $\sum \frac{1}{p^n}$ converges to $\left(1 - \frac{1}{p}\right)^{-1}$, the sum

$$\sum_{n \geq 1} \frac{1}{n} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)$$

must be finite. But the harmonic series diverges. This is a contradiction. □

Theorem (Dirichlet's theorem)**.** Let $a, q \in \mathbb{Z}$ be coprime. Then there exists infinitely many primes in the sequence

$$a, a + q, a + 2q, \cdots,$$

i.e. there are infinitely many primes in any such arithmetic progression.

Proposition.

(i) The Riemann zeta function $\zeta(s)$ converges for $\mathrm{Re}(s) > 1$.

(ii) The function

$$\zeta(s) - \frac{1}{s-1}$$

extends to a holomorphic function when $\mathrm{Re}(s) > 0$.

In other words, $\zeta(s)$ extends to a meromorphic function on $\mathrm{Re}(s) > 0$ with a simple pole at 1 with residue 1.

(iii) We have the expression

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

for $\mathrm{Re}(s) > 1$, and the product is absolutely convergent. This is the *Euler product*.

Lemma. If there is a real number $r \in \mathbb{R}$ such that

$$a_1 + \cdots + a_N = O(N^r),$$

then

$$\sum a_n n^{-s}$$

converges for $\mathrm{Re}(s) > r$, and is a holomorphic function there.

Proof. This is just IA Analysis. Suppose $\mathrm{Re}(s) > r$. Then we can write

$$\sum_{n=1}^{N} a_n n^{-s} = a_1(1^{-s} - 2^{-s}) + (a_1 + a_2)(2^{-s} - 3^{-s}) + \cdots \\ + (a_1 + \cdots + a_{N-1})((N-1)^{-s} - N^{-s}) + R_N,$$

where

$$R_N = \frac{a_1 + \cdots + a_N}{N^s}.$$

This is getting annoying, so let's write

$$T(N) = a_1 + \cdots + a_N.$$

We know

$$\left|\frac{T(N)}{N^s}\right| = \left|\frac{T(N)}{N^r}\right| \frac{1}{N^{\mathrm{Re}(s)-r}} \to 0$$

as $N \to \infty$, by assumption. Thus we have

$$\sum_{n\geq 1} a_n n^{-s} = \sum_{n\geq 1} T(n)(n^{-s} - (n+1)^{-s})$$

if $\mathrm{Re}(s) > r$. But again by assumption, $T(n) \leq B \cdot n^r$ for some constant B and all n. So it is enough to show that

$$\sum_n n^r(n^{-s} - (n+1)^{-s})$$

converges. But

$$n^{-s} - (n+1)^{-s} = \int_n^{n+1} \frac{s}{x^{s+1}}\,\mathrm{d}x,$$

and if $x \in [n, n+1]$, then $n^r \leq x^r$. So we have

$$n^r(n^{-s} - (n+1)^{-s}) \leq \int_n^{n+1} x^r \frac{s}{x^{s+1}}\,\mathrm{d}x = s\int_n^{n+1} \frac{\mathrm{d}x}{x^{s+1-r}}.$$

It thus suffices to show that

$$\int_1^n \frac{\mathrm{d}x}{x^{s+1-r}}$$

converges, which it does (to $\frac{s}{s-r}$). □

Theorem.

(i) $\zeta_L(s)$ converges to a holomorphic function if $\mathrm{Re}(s) > 1$.

(ii) *Analytic class number formula*: $\zeta_L(s)$ is a meromorphic function if $\mathrm{Re}(s) > 1 - \frac{1}{n}$ and has a simple pole at $s = 1$ with residue

$$\frac{|\operatorname{cl}_L| 2^r (2\pi)^s R_L}{|D_L|^{1/2} |\mu_L|},$$

where cl_L is the class group, r and s are the number of real and complex embeddings, you know what π is, R_L is the regulator, D_L is the discriminant and μ_L is the roots of unity in L.

(iii)
$$\zeta_L(s) = \prod_{\mathfrak{p} \lhd \mathcal{O}_L \text{ prime ideal}} (1 - N(\mathfrak{p})^{-s})^{-1}.$$
This is again known as the *Euler product*.

Proposition. χ_D, as defined for $L = \mathbb{Q}(\sqrt{d})$ is a Dirichlet character of modulus D.

Proof. We must show that
$$\chi_D(p + Da) = \chi_D(p)$$
for all p, a.

(i) If $d \equiv 3 \pmod 4$, then $D = 4d$. Then
$$\chi_D(2) = 0,$$
as (2) ramifies. So $\chi_D(\text{even}) = 0$. For $p > 2$, we have
$$\chi_D(p) = \left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{p}{d}\right)(-1)^{\frac{p-1}{2}}$$
as $\frac{d-1}{2} \equiv 1 \pmod 2$, by quadratic reciprocity. So
$$\chi_D(p + Da) = \left(\frac{p + Da}{d}\right)(-1)^{\frac{p-1}{2}}(-1)^{4da/2} = \chi_D(p).$$

(ii) If $d \equiv 1, 2 \pmod 4$, see example sheet. □

Lemma. Let χ be any non-trivial Dirichlet character. Then $L(\chi, s)$ is holomorphic for $\text{Re}(s) > 0$.

Proof. By our lemma on convergence of Dirichlet series, we have to show that
$$\sum_{i=1}^{N} \chi(i) = O(1),$$
i.e. it is bounded. Recall from Representation Theory that distinct irreducible characters of a finite group G are orthogonal, i.e.
$$\frac{1}{|G|} \sum_{g \in G} \overline{\chi_1(g)}\chi_2(g) = \begin{cases} 1 & \chi_1 = \chi_2 \\ 0 & \text{otherwise} \end{cases}.$$
We apply this to $G = (\mathbb{Z}/D\mathbb{Z})^\times$, where χ_1 is trivial and $\chi_2 = \chi$. So orthogonality gives
$$\sum_{aD < i \leq (a+1)D} \chi(i) = \sum_{i \in (\mathbb{Z}/D\mathbb{Z})^\times} \chi(i) = 0,$$
using that $\chi(i) = 0$ if i is not coprime to D. So we are done. □

Corollary. For quadratic characters χ_D, we have
$$L(\chi_D, 1) \neq 0.$$

Proof. We have shown that

$$\zeta_{\mathbb{Q}(\sqrt{d})}(s) = \zeta_{\mathbb{Q}}(s)L(\chi_D, s).$$

Note that $\zeta_{\mathbb{Q}(\sqrt{d})}(s)$ and $\zeta_{\mathbb{Q}}(s)$ have simple poles at $s = 1$, while $L(\chi_D, s)$ is holomorphic at $s = 1$.

Since the residue of $\zeta_{\mathbb{Q}}(s)$ at $s = 1$ is 1, while the residue of $\zeta_{\mathbb{Q}(\sqrt{D})}$ at $s = 1$ is non-zero by the analytic class number formula. So $L(\chi_D, 1)$ is non-zero, and given by the analytic class number formula. □

Proposition.

(i) We have $[L : \mathbb{Q}] = \varphi(q)$, where

$$\varphi(q) = |(\mathbb{Z}/q\mathbb{Z})^\times|.$$

(ii) $L \supseteq \mathbb{Q}$ is a Galois extension, with

$$\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times,$$

where if $r \in (\mathbb{Z}/q\mathbb{Z})^\times$, then r acts on $\mathbb{Q}(w_Q)$ by sending $\omega_q \mapsto \omega_q^r$. This is what plays the role of quadratic reciprocity for cyclotomic fields.

(iii) The ring of integers is

$$\mathcal{O}_L = \mathbb{Z}[\omega_q] = \mathbb{Z}[x]/\Phi_q(x),$$

where

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

is the qth cyclotomic polynomial.

(iv) Let p be a prime. Then p ramifies in $\mathcal{O}_L$ if and only if $p \mid D_L$, if and only if $p \mid q$. So while D might be messy, the prime factors of D are the prime factors of q.

(v) Let p be a prime and $p \nmid q$. Then $\langle p \rangle$ factors as a product of $\varphi(q)/f$ distinct prime ideals, each of norm p^f, where f is the order of p in $(\mathbb{Z}/q\mathbb{Z})^\times$.

Proof.

(i) In the Galois theory course.

(ii) In the Galois theory course.

(iii) In the example sheet.

(iv) In the example sheet.

(v) Requires proof, but is easy Galois theory, and is omitted. □

Proposition. We have

$$\zeta_{\mathbb{Q}(\omega_q)}(s) = \prod_{i=1}^{\varphi(q)} L(\chi_i, s) \cdot (\text{corr. factor}) = \zeta_{\mathbb{Q}}(s) \prod_{i=2}^{\varphi(q)} L(\chi_i, s) \cdot (\text{corr. factor})$$

where the correction factor is a finite product coming from the primes that divide q.

Proof. Our analysis covered all primes $p \nmid q$, and the correction factor is just to include the terms with $p \mid q$. The second part is just saying that

$$\zeta_{\mathbb{Q}}(s) = L(\chi_1, s)\prod_{p|q}(1-p^{-s})^{-1}. \qquad \square$$

Corollary. If χ is any non-trivial Dirichlet character, then $L(\chi, 1) \neq 0$.

Proof. By definition, Dirichlet characters come from representations of some $(\mathbb{Z}/q\mathbb{Z})^\times$, so they appear in the formula of the ζ function of some cyclotomic extension.

Consider the formula

$$\zeta_{\mathbb{Q}(\omega_q)}(s) = \zeta_{\mathbb{Q}}(s)\prod_{i=2}^{\varphi(q)} L(\chi_i, s)\cdot(\text{corr. factor})$$

at $s = 1$. We know that the $L(\chi_i, s)$ are all holomorphic at $s = 1$. Moreover, both $\zeta_{\mathbb{Q}(\omega_q)}$ and $\zeta_{\mathbb{Q}}$ have a simple pole at 0. Since the correction terms are finite, it must be the case that all $L(\chi_i, s)$ are non-zero. $\square$

Theorem (Dirichlet, 1839)**.** Let $a, q \in \mathbb{N}$ be coprime, i.e. $\gcd(a, q) = 1$. Then there are infinitely many primes in the arithmetic progression

$$a, a+q, a+2q, a+3q, \cdots.$$

Proof. As before, let

$$\omega_1, \cdots, \omega_{\varphi(q)} : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$$

be the irreducible characters, and let

$$\chi_1, \cdots, \chi_{\varphi(q)} : \mathbb{Z} \to \mathbb{C}$$

be the corresponding Dirichlet character, with ω_1 the trivial one.

Recall the orthogonality of columns of the character table, which says that if $\gcd(p, q) = 1$, then

$$\frac{1}{\varphi(q)}\sum_i \overline{\omega_i(a)}\omega_i(p) = \begin{cases} 1 & a \equiv p \pmod q \\ 0 & \text{otherwise} \end{cases}.$$

Hence we know

$$\frac{1}{\varphi(q)}\sum_i \overline{\chi_i(a)}\chi_i(p) = \begin{cases} 1 & a \equiv p \pmod q \\ 0 & \text{otherwise} \end{cases},$$

even if $\gcd(p, q) \neq 1$, as then $\chi_i(p) = 0$. So

$$\sum_{\substack{p \equiv a \bmod q \\ p \text{ prime}}} p^{-s} = \frac{1}{\varphi(q)}\sum_i \overline{\chi_i(a)} \sum_{\text{all primes } p} \chi_i(p)p^{-s}. \qquad (\ddagger)$$

We want to show this has a pole at $s = 1$, as in Euclid's proof.

To do so, we show that $\sum_p \chi_i(p)p^{-s}$ is "essentially" $\log L(\chi_i, s)$, up to some bounded terms. We Taylor expand

$$\log L(\chi, s) = -\sum \log(1 - \chi(p)p^{-s}) = \sum_{\substack{n\geq 1\\ p \text{ prime}}} \frac{\chi(p)^n}{np^{ns}} = \sum_{\substack{n\geq 1\\ p \text{ prime}}} \frac{\chi(p^n)}{np^{ns}}.$$

What we care about is the $n = 1$ term. So we claim that

$$\sum_{n\geq 2, p \text{ prime}} \frac{\chi(p^n)}{np^{ns}}$$

converges at $s = 1$. This follows from the geometric sum

$$\left|\sum_p \sum_{n\geq 2} \frac{\chi(p^n)}{np^{ns}}\right| \leq \sum_p \sum_{n\geq 2} p^{-ns} = \sum_{p \text{ prime}} \frac{1}{p^s(p^s - 1)} \leq \sum_{n\geq 2} \frac{1}{n^s(n^s - 1)} < \infty.$$

Hence we know

$$\log L(\chi, s) = \sum_p \chi_i(p)p^{-s} + \text{bounded stuff}$$

near $s = 1$.

So at $s = 1$, we have

$$(\ddagger) \sim \frac{1}{\varphi(q)} \sum_i \overline{\chi_i(a)} \log L(\chi_i, s).$$

and we have to show that the right hand side has a pole at $s = 1$.

We know that for $i \neq 1$, i.e. χ_i non-trivial, $L(\chi_i, s)$ is holomorphic and non-zero at $s = 1$. So we just have to show that $\log L(\chi_1, s)$ has a pole. Note that $L(\chi_1, s)$ is essentially $\zeta_{\mathbb{Q}}(s)$. Precisely, we have

$$L(\chi_1, s) = \zeta_{\mathbb{Q}}(s) \prod_{p|q} (1 - p^{-s}).$$

Moreover, we already know that $\zeta_{\mathbb{Q}}(s)$ blows up at $s = 1$. We have

$$\begin{aligned}\zeta_{\mathbb{Q}}(s) &= \frac{1}{s-1} + \text{holomorphic function}\\ &= \frac{1}{s-1}(1 + (s-1)(\text{holomorphic function})).\end{aligned}$$

So we know

$$\log L(\chi_1, s) \sim \log \zeta_{\mathbb{Q}}(s) \sim \log\left(\frac{1}{s-1}\right),$$

and this does blow up at $s = 1$. □