Number Fields

Cambridge University Mathematical Tripos: Part II

17th May 2024

Contents

1 Number fields

1.1 Algebraic integers

Recall that if K and L are fields and $\dim_K L < \infty$, we write $[L : K]$ for this dimension and say that L/K is a finite extension. If L/K is a finite extension, every element $x \in L$ is algebraic over K.

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

Definition. Let L be a number field. $\alpha \in L$ is an *algebraic integer* if there exists $f \in \mathbb{Z}[x]$ monic such that $f(\alpha) = 0$. We write $\mathcal{O}_L = \{\alpha \in L \mid \alpha \text{ is an algebraic integer}\}$ for the set of *integers of L*.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Q} \arrow[d] \\
\mathcal{O}_L \arrow[r] & L
\end{tikzcd}$$

Lemma. $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

Proof. Clearly if α is an integer, then $f(x) = x - \alpha$ is a monic polynomial such that $f(\alpha) = 0$. Conversely, if α is a rational number, we can let $\alpha = \frac{r}{s}$ where r and s are coprime. Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Clearing denominators, $r^n + a_{n-1}r^{n-1}s + \dots + a_0 s^n = 0$. Hence $s \mid r^n$. If $s \neq 1$, let $p \mid s$ be a prime, then $p \mid r$, so r and s were not coprime. □

We will soon show that $\mathcal{O}_L$ is a ring. In other words, $\alpha, \beta \in \mathcal{O}_L$ implies $\alpha \pm \beta, \alpha\beta \in \mathcal{O}_L$.

Note that $\alpha \in \mathcal{O}_L$ does not in general imply $\frac{1}{\alpha} \in \mathcal{O}_L$. Recall from Galois Theory that if $\alpha, \beta \in L$, and α, β are algebraic over K, then so is $\alpha \pm \beta, \alpha\beta$. The proof from Galois Theory will not work in this case, since that proof does not provide for monic polynomials.

Definition. Let $R \subseteq S$ be commutative rings with a 1.

(i) $\alpha \in S$ is *integral over R* if there exists a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$.

(ii) S is *integral over R* if all $\alpha \in S$ are integral over R.

(iii) S is *finitely generated over R* if there exist elements $\alpha_1, \dots, \alpha_n \in S$ such that any element of S can be written as an R-linear combination of the α_i. Equivalently, the map $R^n \to S$ given by $(r_1, \dots, r_n) \mapsto \sum_{i=1}^n r_i\alpha_i$ is surjective.

Example. Let $\mathbb{Q} \subseteq L$ be a number field. Then $\alpha \in L$ is an algebraic integer if and only if α is integral over $\mathbb{Z}$. $\mathcal{O}_L$ is integral over $\mathbb{Z}$ (once we have proven it is a ring).

If $\alpha_1, \dots, \alpha_r \in S$, we write $R[\alpha_1, \dots, \alpha_r]$ for the subring of S generated by R and the α_i. This is equivalently the image of the polynomial ring $R[x_1, \dots, x_r] \to S$ mapping x_i to α_i.

Proposition. Let $S = R[s]$, where s is integral over R. Then S is finitely generated over R. Further, if $S = R[s_1, \dots, s_n]$ with each s_i integral over R, then S is finitely generated over R.

Proof. S is spanned by $1, s, s^2, \dots$ over R. By assumption, there exists $a_0, \dots, a_{n-1} \in R$ such that $s^n = \sum_{i=0}^{n-1} a_i s^i$. So the R-module spanned by $1, \dots, s^{n-1}$ is stable under multiplication by s, so contains $s^n, s^{n+1}, \dots$ and hence is all of S.

Let $S_i = R[s_1, \dots, s_{i-1}]$. Then $S_{i+1} = S_i[s_{i+1}]$, and s_{i+1} is integral over R, hence is integral over S_i. So S_{i+1} is finitely generated over S_i. Note that if $A \subseteq B \subseteq C$ where B is finitely generated over A and C is finitely generated over B, then C is finitely generated over A. Indeed, if b_i generate B over A and c_j generate C over B, the $b_i c_j$ generate C over A. □

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

Proof. Let $\alpha_1, \dots, \alpha_n$ generate S as an R-module. Without loss of generality, we can assume $\alpha_1 = 1$. Let $s \in S$, and consider the function $m_s : S \to S$ given by $m_s(x) = sx$. Then, $m_s(\alpha_i) = s\alpha_i = \sum b_{ij}\alpha_j$ for some choice of b_{ij}. Let $B = (b_{ij})$. By definition, $(sI - B)(\alpha_1, \dots, \alpha_n)^\intercal = 0$.

Recall that for any matrix X, the adjugate has the property that $\operatorname{adj}(X)X = \det X \cdot I$. Hence, $\det(sI - B)(\alpha_1, \dots, \alpha_n)^\intercal = 0$. In particular, $\det(sI - B)\alpha_1 = \det(sI - B) = 0$. Let $f(t) = \det(tI - B)$, which is a monic polynomial in R. As $f(s) = 0$, s is integral over R. □

Note the similarity to a proof of the Cayley–Hamilton theorem. Note further that this proof is constructive.

Corollary. Let $\mathbb{Q} \subseteq L$ 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 over $\mathbb{Z}$. So this ring is integral. □

Corollary. Let $A \subseteq B \subseteq C$ be ring extensions, where B/A is integral and C/B is integral. Then C/A is integral.

Proof. If $c \in C$, let $f(x) = \sum_{i=0}^{n} b_i x^i$ be the monic polynomial in $B[x]$ it satisfies, and set $B_0 = A[b_0, \dots, b_{n-1}]$, $C_0 = B[c]$. Then B_0 is finitely generated over A as $b_0, \dots, b_{n-1}$ are integral over A, and C_0 is finitely generated over B_0 as c is integral over B_0. C_0 is therefore finitely generated over A. Then the theorem implies that c is integral over A. □

Remark. C could have had infinitely many generators, for instance,

$$C = \{\alpha \in \mathbb{C} \mid \alpha \text{ is an algebraic integer}\}$$

This possibility is why we passed to C_0. This kind of proof is common in commutative algebra, applying a powerful theorem such as the Cayley–Hamilton theorem carefully to find its consequences.

Example. $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$.

1.2 Minimal polynomials

Let $K \subseteq L$ be fields. Recall that the minimal polynomial of $\alpha \in L$ is the monic polynomial $p_\alpha(x) \in K[x]$ of minimum degree such that $p_\alpha(\alpha) = 0$.

Lemma. Let $f(x) \in K[x]$ satisfy $f(\alpha) = 0$. Then $p_\alpha \mid f$.

Proof. By Euclid, $f = p_\alpha h + r$ where $r \in K[x]$ has degree less than that of p. Then $0 = f(\alpha) = p_\alpha(\alpha)h(\alpha) + r(\alpha)$. If $r \neq 0$, this contradicts minimality of $\deg p_\alpha$. □

The converse is obvious, so the lemma implies the uniqueness of p_α.

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

Proof. If p_α has integer coefficients, this holds by definition. Conversely, suppose $\alpha \in \mathcal{O}_L$, where p_α is the minimal polynomial. Let $M \supseteq L$ be a splitting field for p_α, i.e. a field in which p_α splits into linear factors. Let $h(x)$ be a monic polynomial which α satisfies. By the lemma, $p_\alpha \mid h$, so each root α_i of p_α in M is an algebraic integer. By the previous theorem, sums and products of algebraic integers are algebraic. So the coefficients of p_α are algebraic integers. But $p_\alpha \in \mathbb{Q}[x]$, so the coefficients are in $\mathbb{Z}$. □

Remark. One can also show this from the previous result and Gauss' lemma.

Lemma. The field of fractions of $\mathcal{O}_L$ is L. In fact, if $\alpha \in L$, there exists $n \in \mathbb{Z}, n \neq 0$ such that $n\alpha \in \mathcal{O}_L$.

Proof. Let $\alpha \in L$, and g be the minimal polynomial of α. Then g is monic, and there exists an integer $n \in \mathbb{Z}, n \neq 0$ such that $ng \in \mathbb{Z}[x]$. So $h(x) = n^{\deg g} g\left(\frac{x}{n}\right)$ is an integer polynomial which is monic, and this is the minimal polynomial of $n\alpha$, so $n\alpha \in \mathcal{O}_L$. □

1.3 Integral basis

If L/K is a field extension, and $\alpha \in L$, we write $m_\alpha : L \to L$ for the map given by multiplication by α. We define the *norm* of α to be the determinant of m_α, and the *trace* of α to be the trace of m_α. Recall that if $p_\alpha(x)$ is the minimal polynomial of α, then the characteristic polynomial of m_α is $\det(xI - m_\alpha) = p_\alpha^{[L/K(\alpha)]}$. Further, if $p_\alpha(t)$ splits as $(t - \alpha_1) \cdots (t - \alpha_r)$ in some field $L' \supseteq K(\alpha)$, then $N_{K(\alpha)/K}(\alpha) = \prod \alpha_i$ and $\operatorname{Tr}_{K(\alpha)/K}(\alpha) = \sum \alpha_i$, and $N_{L/K}(\alpha) = (\prod \alpha_i)^{[L:K(\alpha)]}, \operatorname{Tr}_{L/K}(\alpha) = [L : K(\alpha)] \sum \alpha_i$.

If L is a number field, then α is an algebraic integer if and only if the minimal polynomial is has integer coefficients, which is the case if and only if the characteristic polynomial of m_α has integer coefficients. In particular, in this case, $N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. If the degree of L over $\mathbb{Q}$ is 2, the norm and trace are integers if and only if α is algebraic, since these values determine the characteristic polynomial.

Example. Let $L = K(\sqrt{d})$ where $d \in K$ is not a square. This has basis $1, \sqrt{d}$. If $\alpha = x + y\sqrt{d}$, the matrix m_α is

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

Then, $\mathrm{Tr}_{L/K}(x + y\sqrt{d}) = 2x = (x + y\sqrt{d}) + (x - y\sqrt{d})$, and $N_{L/K}(x + y\sqrt{d}) = x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$.

Lemma. Let $L = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ a nonzero square-free integer. Such a field is called a *quadratic field*. Then, $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \bmod 4$, and $\mathcal{O}_L = \mathbb{Z}\Big[\frac{1}{2}(1 + \sqrt{d})\Big]$ if $d \equiv 1 \bmod 4$.

Proof. $x + y\sqrt{d} \in \mathcal{O}_L$ if and only if $2x, x^2 - dy^2 \in \mathbb{Z}$. This implies that $4dy^2 \in \mathbb{Z}$. If $y = \frac{r}{s}$ with $\gcd(r, s) = 1$, then $s^2 \mid 4d$. But d was square-free, so $s^2 \mid 4$ so $s = \pm 1, \pm 2$. As $2x \in \mathbb{Z}$, we can write $x = \frac{u}{2}$ and $y = \frac{v}{2}$, for $u, v \in \mathbb{Z}$. Therefore, $u^2 - dv^2 \in 4\mathbb{Z}$, so $u^2 \equiv dv^2 \bmod 4$. Note that u^2 must be 0 or 1 mod 4.

So if d is not congruent to 1 mod 4, $u^2 \equiv dv^2$ has a solution, so u^2, v^2 are both zero mod 4, so u, v are even. In this case, $x, y \in \mathbb{Z}$, so any $\alpha \in \mathcal{O}_L$ is a $\mathbb{Z}$-combination of $1, \sqrt{d}$.

On the other hand, if $d \equiv 1$, then u, v have the same parity mod 2, so we can write any such values as a $\mathbb{Z}$-combination of $1, \frac{1}{2}(1 + \sqrt{d})$. □

Example. If $d = -1$, $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$. Note that the minimal polynomial of $\frac{1}{2}(1+\sqrt{d})$ is $t^2 - t + \frac{1}{4}(1-d)$, which has integer coefficients as $d \equiv 1$.

Definition. Let L be a number field. Then, a basis $\alpha_1, \dots, \alpha_n$ of L as a $\mathbb{Q}$-vector space is called an *integral basis* if $\mathcal{O}_L = \left\{ \sum_{i=1}^n m_i \alpha_i \mid m_i \in \mathbb{Z} \right\} = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i$.

Example. $\mathbb{Q}(\sqrt{d})$ has integer basis $1, \frac{1}{2}(1 + \sqrt{d})$ or $1, \sqrt{d}$, depending on the value of d mod 4.

Integral bases are not unique. Given two such bases, there exists a matrix $g \in GL_n(\mathbb{Z})$ which transforms one into the other. We now aim to show that there exists an integral basis for every number field.

Recall that if L/K is a finite separable extension, then there exists $\alpha \in L$ such that $L = K(\alpha)$; this is the primitive element theorem. Note that all extensions in characteristic 0 are separable.

Example. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

This implies that if $L/\mathbb{Q}$ is a number field, then there exists $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$, isomorphic to $\mathbb{Q}[x]\big/_{(p_\alpha(x))}$ where p_α is the minimal polynomial for x. L is a field, so $P_\alpha \lhd \mathbb{Q}[x]$ is a maximal ideal in the principal ideal domain $\mathbb{Q}[x]$, and p_α is irreducible. Let $\deg p_\alpha = [L : \mathbb{Q}] = n$. Then L has basis $1, \alpha, \dots, \alpha^{n-1}$ as a $\mathbb{Q}$-vector space.

Lemma. n is the number of field embeddings of L into $\mathbb{C}$.

Proof. $p_\alpha \in \mathbb{Q}[x]$ is irreducible, so $\gcd(p_\alpha, p'_\alpha) = 1$. So $p_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_n)$ has n distinct roots in $\mathbb{C}$. A field homomorphism ${}^{\mathbb{Q}[x]}\!/\!_{(p_\alpha(x))} \to \mathbb{C}$ is automatically $\mathbb{Q}$-linear, so must map x to a root α_i of $p_\alpha(x)$ in $\mathbb{C}$. Conversely, there exists such a map for each α_i, and they are distinct. □

This allows us to define a new invariant which refines $n = [L : \mathbb{Q}]$.

Definition. Let r be the number of real roots of $p_\alpha(x)$, and let s be the number of complex conjugate pairs of roots of $p_\alpha(x)$. Also, r is the number of field embeddings of L into $\mathbb{R}$, so is independent of the choice of α. s is therefore also an invariant, as $r + 2s = n$.

Lemma. Let $L/\mathbb{Q}$ be a number field. Let $\sigma_1, \dots, \sigma_n : L \to \mathbb{C}$ be the different field embeddings, so $n = [L : \mathbb{Q}]$. If $\beta \in L$, then $\mathrm{Tr}_{L/\mathbb{Q}}(\beta) = \sum \sigma_i(\beta)$ and $N_{L/\mathbb{Q}}(\beta) = \prod \sigma_i(\beta)$. We call the $\sigma_i(\beta)$ the *conjugates* of β in $\mathbb{C}$.

Example. If $L = \mathbb{Q}(\sqrt{d})$ where d is square-free, then $a + b\sqrt{d}$ and $a - b\sqrt{d}$ are conjugates.

Proposition. Let L/K be a finite separable extension. Then, the K-bilinear form $L \times L \to K$ given by $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$, known as the *trace form*, is a nondegenerate inner product. Equivalently, if $\alpha_1, \dots, \alpha_n$ is a basis of L/K, the Gram matrix has nonzero determinant, that is, $\Delta(\alpha_1, \dots, \alpha_n) = \det \mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \neq 0$. Conversely, if L/K is inseparable, the trace form is the zero map.

Proof. Let $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ be the n distinct K-linear field embeddings of L into an algebraic closure $\overline{K}$, which exists by separability. Let S be the matrix $(\sigma_i(\alpha_j))$. Observe that $S^\intercal S$ is the matrix with (i, j) term

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

So $\Delta(\alpha_1, \dots, \alpha_n) = \det S \det S^\intercal = (\det S)^2$. By the primitive element theorem, there exists $\theta \in L$ such that $L = K(\theta)$. Therefore, $1, \theta, \dots, \theta^{n-1}$ forms a basis of L/K. Then

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

This is a Vandermonde matrix, which gives

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

This is nonzero; indeed, if $\sigma_i(\theta) = \sigma_j(\theta)$, then $\sigma_i(\theta^a) = \sigma_j(\theta^a)$ for all a, so $\sigma_i = \sigma_j$, but they are distinct.

Moreover, if $\alpha_1, \dots, \alpha_n$ is any basis of L/K, and $\alpha'_1, \dots, \alpha'_n$ is another basis of L/K, then

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

where $\alpha'_i = \sum a_{ij}\alpha_j$ and $A = (a_{ij})$. Hence, $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$ for any basis. □

Remark. $L = K(\theta)$ and $p_\theta(t) = \prod(t - \sigma_i(\theta))$. The Galois theory notion of the discriminant of p_θ, which is $\prod_{i<j}(\sigma_i(\theta) - \sigma_j(\theta))^2$, is exactly the determinant of the Gram matrix $\Delta(1, \theta, \dots, \theta^{n-1})$, also often called a discriminant.

Remark. Let L be a number field. If $\alpha, \beta \in \mathcal{O}_L$, $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}$. Therefore, the inner product is a function $\mathcal{O}_L \times \mathcal{O}_L \to \mathbb{Z}$. If $\alpha_1, \dots, \alpha_n \in L$ form a basis of L over $\mathbb{Q}$, and $\alpha_1, \dots, \alpha_n$ are algebraic integers, then $\Delta(\alpha_1, \dots, \alpha_n)$ is a nonzero integer.

Theorem. Let $L/\mathbb{Q}$ be a number field. Then there exists an integral basis for $\mathcal{O}_L$: there exist $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ such that $\mathcal{O}_L = \bigoplus \mathbb{Z}\alpha_i \simeq \mathbb{Z}^n$ and $L = \bigoplus \mathbb{Q}\alpha_i \simeq \mathbb{Q}^n$.

Proof. Let $\alpha_1, \dots, \alpha_n$ be any basis for L as a $\mathbb{Q}$-vector space. We have shown that there exists $n_i \in \mathbb{Z}$ such that $n_i\alpha_i \in \mathcal{O}_L$. Therefore, we can assume $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ without loss of generality. Here, $\Delta(\alpha_1, \dots, \alpha_n)$ is a nonzero integer.

Choose $\alpha_1, \dots, \alpha_n$ such that $\Delta(\alpha_1, \dots, \alpha_n)$ has minimum absolute value. Suppose the result is false, so let $x \in \mathcal{O}_L$ and $x = \sum \lambda_i\alpha_i$ where $\lambda_i \in \mathbb{Q}$, and suppose that some λ_i is not an integer. Without loss of generality let $\lambda_1 \notin \mathbb{Z}$. Write $\lambda_1 = n_1 + \varepsilon_1$, and $0 < \varepsilon_1 < 1$. Now, let

$$\alpha_1' = x - n_1\alpha_1 = \varepsilon_1\alpha_1 + \lambda_2\alpha_2 + \dots + \lambda_n\alpha_n$$

Note $\alpha_1' \in \mathcal{O}_L$. Then $\alpha_1', \alpha_2, \dots, \alpha_n$ is a basis of L containing only the elements of $\mathcal{O}_L$. But $\Delta(\alpha_1', \alpha_2, \dots, \alpha_n) = \varepsilon_1^2\Delta(\alpha_1, \dots, \alpha_n)$ contradicting the minimality assumption. □

Remark. If $\alpha_1', \dots, \alpha_n'$ are any other integral basis of $\mathcal{O}_L$, then there exists $g \in GL_n(\mathbb{Z})$ such that $g(\alpha_i') = \alpha_i$. But $\det g \in GL_1(\mathbb{Z}) = \{\pm 1\}$, so $(\det g)^2 = 1$, giving $\Delta(\alpha_1', \dots, \alpha_n') = \Delta(\alpha_1, \dots, \alpha_n)$, so this is an invariant.

Definition. The *discriminant* of a number field $L/\mathbb{Q}$ is the invariant $D_L = \Delta(\alpha_1, \dots, \alpha_n)$.

Example. Let $L = \mathbb{Q}(\sqrt{d})$ where d is square-free. Then, $d \equiv 2, 3 \bmod 4$, then $1, \sqrt{d}$ is an integral basis. If $d \equiv 1 \bmod 4$, then $1, \frac{1}{2}\left(1 + \sqrt{d}\right)$ is an integral basis. Then,

$$D_L = \left[\det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}\right]^2 = 4d; \quad D_L = \left[\det\begin{pmatrix} 1 & \frac{1}{2}\left(1 + \sqrt{d}\right) \\ 1 & \frac{1}{2}\left(1 - \sqrt{d}\right) \end{pmatrix}\right]^2 = d$$

So the discriminant is either $4d$ or d.

Remark. Results on quadratic fields are often phrased more uniformly if written in terms of D_L. Note also that $L = \mathbb{Q}(\sqrt{D_L})$. An integral basis is $1, \frac{\sqrt{D_L}+D_L}{2}$ regardless of the value of d.

2 Ideals

2.1 Ideals in the ring of integers

Lemma. Let $x \in \mathcal{O}_L$, where L is a number field. Then x is a unit in $\mathcal{O}_L$ if and only if $N_{L/\mathbb{Q}}(x) = \pm 1$. We write $\mathcal{O}_L^\star$ for the set of units of $\mathcal{O}_L$.

Proof. If x is a unit, then as the norm is multiplicative, $N(xx^{-1}) = 1$ so $N(x)N(x^{-1}) = 1$. So $N(x) = \pm 1$. Conversely, let $\sigma_1, \dots, \sigma_n : L \to \mathbb{C}$ be the distinct field embeddings. Let $L \subseteq \mathbb{C}$ be the containment given by σ_1. If $x \in \mathcal{O}_L$, then $N(x) = x\sigma_2(x) \dots \sigma_n(x)$. So if $N(x) = \pm 1$, we have $\frac{1}{x} = \pm \prod_{i=2}^n \sigma_i(x)$. This is a product of algebraic integers, hence an algebraic integer. So $x^{-1} \in \mathcal{O}_L$. □

Recall that if $x \in \mathcal{O}_L$, it is irreducible if it does not factorise as ab where $a, b \in \mathcal{O}_L$ not units. If $x = uy$ where u is a unit, we say x and y are associate. Many number fields have rings of algebraic integers which are not unique factorisation domains.

Example. Let $L = \mathbb{Q}\left(\sqrt{-5}\right)$. Here, $\mathcal{O}_L = \mathbb{Z}\left[\sqrt{-5}\right]$. Note that $3 \cdot 7 = \left(1 + 2\sqrt{-5}\right)\left(1 - 2\sqrt{-5}\right)$, and $N(3) = 9, N(7) = 49, N\left(1 \pm \sqrt{-5}\right) = 21$. These are not associates. We claim that $3, 7, 1 \pm 2\sqrt{-5}$ are irreducible, so $\mathcal{O}_L$ is not a unique factorisation domain. If this were not the case, $3 = \alpha\overline{\alpha}$, where $\alpha = x + y\sqrt{-5}$, but $N(3) = 9 = N(\alpha)N(\overline{\alpha}) = N(\alpha)^2$ so $N(\alpha) = x^2 + 5y^2 = \pm 3$, but there are no integer solutions to this equation. All of the other factors are similarly irreducible.

Remark. In any number field, one can factorise any $\alpha \in \mathcal{O}_L$ into a product of irreducibles by induction on $|N(\alpha)|$, but this factorisation is not in general unique. An idea due to Kummer is to measure the failure of unique factorisation by studying ideals $\mathfrak{a} \lhd \mathcal{O}_L$.

If $x_1, \dots, x_n \in \mathcal{O}_L$, we write $(x_1, \dots, x_n)$ for the ideal $\sum x_i \mathcal{O}_L$ generated by the x_i. We will consider products of ideals, rather than products of elements.

Definition. If $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$, define

$$\mathfrak{a} + \mathfrak{b} = \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}; \quad \mathfrak{a}\mathfrak{b} = \left\{\sum_i x_i y_i \,\middle|\, x_i \in \mathfrak{a}, y_i \in \mathfrak{b}\right\}$$

One can check that this is an ideal, and that products are associative.

Example. $(x_1, \dots, x_n)(y_1, \dots, y_m) = \left(\{x_i y_j \mid 1 \leq i \leq n, 1 \leq j \leq n\}\right)$. For instance, $(x)(y) = (xy)$, so the product of principal ideals is principal.

Example. Consider $\mathbb{Z}[\sqrt{5}] = \mathcal{O}_L$, and the ideals $\mathfrak{p}_1 = (3, 1 + 2\sqrt{5}), \mathfrak{p}_2 = (3, 1 - 2\sqrt{5})$. We obtain $\mathfrak{p}_1\mathfrak{p}_2 = (9, 3(1 - 2\sqrt{5}), 3(1 + 2\sqrt{5}), 21) = (3)$. So the ideal (3) factors as $\mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_L$. Note that $37 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$, so $\mathbb{Z}[\sqrt{5}]$ is not a unique factorisation domain.

Recall that an ideal $\mathfrak{p} \lhd R$ is *prime* if ${R}/{\mathfrak{p}}$ is an integral domain, so $p \neq R$ and for all $x, y \in R$, $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. In this course, we will also define that a prime ideal is nonzero.

Lemma. If $\mathfrak{a} \lhd \mathcal{O}_K$, it contains an integer, and moreover, ${\mathcal{O}_K}/{\mathfrak{a}}$ is a finite abelian group.

Proof. Let $\alpha \in \mathfrak{a}, \alpha \neq 0$. Let $p_\alpha(x) = x^m + a_{m-1}x^{m-1} + \dots + a_0 \in \mathbb{Z}[x]$ be its minimal polynomial, and $a_0 \neq 0$. Then $a_0 = -\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-1} + \dots + a_2\alpha + a_1)$. But $a_0 \in \mathbb{Z}$, $\alpha \in \mathfrak{a}$, and the other factor lies in $\mathcal{O}_K$. So $a_0 \in \mathfrak{a}$ as $\mathfrak{a}$ is an ideal. Hence $a_0\mathcal{O}_K \subseteq \mathfrak{a}$, so ${}^{\mathcal{O}_K}\!/_{a_0\mathcal{O}_K}$ surjects onto ${}^{\mathcal{O}_K}\!/_{\mathfrak{a}}$. But for any integer d, ${}^{\mathcal{O}_K}\!/_{d\mathcal{O}_K} = {}^{\mathbb{Z}^n}\!/_{d\mathbb{Z}^n} = \left({}^{\mathbb{Z}}\!/_{d\mathbb{Z}}\right)^n$ is a finite set, so ${}^{\mathcal{O}_K}\!/_{\mathfrak{a}}$ is finite. □

Corollary. $\mathfrak{a} \simeq \mathbb{Z}^n$, as $\mathcal{O}_K \simeq \mathbb{Z}^n$ and the quotient is finite.

Therefore, nonzero ideals in $\mathcal{O}_K$ are isomorphic to $\mathbb{Z}^n$ as abelian groups.

Proposition. (i) $\mathcal{O}_K$ is an integral domain.
(ii) $\mathcal{O}_K$ is a Noetherian ring.
(iii) $\mathcal{O}_K$ is *integrally closed* in K (which is the field of fractions of $\mathcal{O}_K$): if $x \in K$ is integral over $\mathcal{O}_K$, it lies in $\mathcal{O}_K$.
(iv) Every (implicitly nonzero) prime ideal is maximal. We say that the *Krull dimension* of $\mathcal{O}_K$ is 1.

Remark. A ring with these four properties is called a *Dedekind domain*. Many of the results in this section hold for all Dedekind domains.

Proof. Part (i). $\mathcal{O}_K \subseteq K$, and K is a field.

Part (ii). We have shown that $\mathcal{O}_K \simeq \mathbb{Z}^n$, where $n = [K : \mathbb{Q}]$, so $\mathcal{O}_K$ is finitely generated as an abelian group, so is certainly finitely generated as a ring.

Part (iii). $\mathcal{O}_K$ is integral over $\mathbb{Z}$ by definition, so if x is integral over $\mathcal{O}_K$, it is integral over $\mathbb{Z}$. So x is an algebraic integer, so lies in $\mathcal{O}_K$.

Part (iv). If $\mathfrak{p}$ is a prime ideal, then by the previous lemma ${}^{\mathcal{O}_K}\!/_{\mathfrak{p}}$ is finite and an integral domain, as $\mathfrak{p}$ is prime. All finite integral domains are fields, hence $\mathfrak{p}$ is maximal. □

Example. Consider $R = \mathbb{C}[X, Y]$. Then (x) is prime but not maximal, since $(x) \subsetneq (x, y)$.

2.2 Unique factorisation of ideals

We aim to show that every ideal in $\mathcal{O}_K$ factors uniquely as a product of prime ideals.

Definition. $\mathfrak{b}$ divides $\mathfrak{a}$ if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. We write $\mathfrak{b} \mid \mathfrak{a}$.

Example. $(5, 1 + 2\sqrt{5}) \mid (3)$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$. $3\mathbb{Z} \mid 6\mathbb{Z}$ as $3\mathbb{Z} \cdot 2\mathbb{Z} = 6\mathbb{Z}$.

Note that $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{b}$, as $\mathfrak{b}$ is an ideal. So if $\mathfrak{b} \mid \mathfrak{a}$, then $\mathfrak{a} \subseteq \mathfrak{b}$. We will show the converse, that $\mathfrak{a} \subseteq \mathfrak{b}$ implies $\mathfrak{b} \mid \mathfrak{a}$. This allows us to prove results about division by using containment. Note that prime ideals are maximal, which allows us to use the containment relation.

Lemma. Let $\mathfrak{p}$ be a prime ideal in a ring R, and let $\mathfrak{a}, \mathfrak{b} \lhd R$ be ideals. Then if $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

Proof. Otherwise, there exists $a \in \mathfrak{a} \setminus \mathfrak{p}$ and $b \in \mathfrak{b} \setminus \mathfrak{p}$, with $ab \in \mathfrak{p}$. But $\mathfrak{p}$ is prime giving a contradiction. □

Lemma. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ be a nonzero ideal. Then $\mathfrak{a}$ contains a product of prime ideals.

Proof. Otherwise, as $\mathcal{O}_K$ is Noetherian, there exists a ideal $\mathfrak{a}$ which is maximal with this property. In particular, $\mathfrak{a}$ is not prime. So there exists $x, y \in \mathcal{O}_K$ with x or y not in $\mathfrak{a}$ but $xy \in \mathfrak{a}$. So $\mathfrak{a} \subsetneq \mathfrak{a} + (x)$. But then, $\mathfrak{a} + (x)$ contains a product of prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ with $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \mathfrak{a} + (x)$. Similarly, there exist prime ideals $\mathfrak{q}_1, \dots \mathfrak{q}_s$ such that $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq \mathfrak{a} + (y)$. Then,

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

But $xy \in \mathfrak{a}$, giving a contradiction. □

The main proof will use the idea that we can formally introduce the group of fractions of the commutative monoid of ideals. The object $\{y \in K \mid y\mathfrak{a} \subseteq \mathcal{O}_K\}$ will represent the inverse of $\mathfrak{a}$.

Lemma. (i) Let $0 \neq \mathfrak{a} \trianglelefteq \mathcal{O}_K$ be an ideal. If $x \in K$ has the property that $x\mathfrak{a} \subseteq \mathfrak{a}$, then $x \in \mathcal{O}_K$.

(ii) Let $0 \neq \mathfrak{a} \triangleleft \mathcal{O}_K$ be a proper ideal. Then, $\mathcal{O}_K \subseteq \{y \in K \mid y\mathfrak{a} \subseteq \mathcal{O}_K\}$ contains elements which are not in $\mathcal{O}_K$. Equivalently, $\{y \in K \mid y\mathfrak{a} \subseteq \mathcal{O}_K\} / \mathcal{O}_K \neq \{1\}$ as abelian groups.

Example. Let $\mathcal{O}_K = \mathbb{Z}$ and $\mathfrak{a} = 3\mathbb{Z}$. Then, part (i) shows that if $\frac{a}{b} \cdot 3 \in 3\mathbb{Z}$, then $\frac{a}{b} \in \mathbb{Z}$. Part (ii) shows that if $\frac{a}{b} \cdot 3 \in \mathbb{Z}$ then $\frac{a}{b} \in \frac{1}{3}\mathbb{Z}$; for instance, if $\frac{a}{b} = \frac{1}{3}$, we have $\frac{1}{3}\mathbb{Z} / \mathbb{Z} = \mathbb{Z} / 3\mathbb{Z} \neq \{1\}$.

Proof. Part (i). $\mathfrak{a} \subseteq \mathcal{O}_K$ is finitely generated as an abelian group, as it is isomorphic to $\mathbb{Z}^n$. Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Consider $m_x : \mathfrak{a} \to \mathfrak{a}$ given by multiplication by $x \in K$. We write $x\alpha_i = \sum a_{ij}\alpha_j$, where by assumption, a_{ij} are integers. Hence,

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

where $A = (a_{ij})$. So $\det(xI - A) = 0$, so x is integral over $\mathbb{Z}$; that is, $x \in \mathcal{O}_K$.

Part (ii). If this holds for $\mathfrak{a}$, it certainly holds for all ideals $\mathfrak{a}' \subseteq \mathfrak{a}$. So without loss of generality, let $\mathfrak{a}$ be maximal, so $\mathfrak{a} = \mathfrak{p}$ is a prime ideal. Let $\alpha \in \mathfrak{p}$ be nonzero. By the previous lemma, there exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}$. Suppose that r is minimal. By the first lemma in this subsection, there exists i such that $\mathfrak{p}_i \subseteq \mathfrak{p}$, and without loss of generality $i = 1$. So $\mathfrak{p}_1 \subseteq \mathfrak{p}$. But $\mathfrak{p}_1$ is maximal, so $\mathfrak{p}_1 = \mathfrak{p}$.

Since r is minimal, $\mathfrak{p}_2 \dots \mathfrak{p}_r \subsetneq (\alpha)$. Fix $\beta \in \mathfrak{p}_2 \dots \mathfrak{p}_r \setminus (\alpha)$. Then $\beta\mathfrak{p} \subseteq \mathfrak{p}(\mathfrak{p}_2 \dots \mathfrak{p}_r) \subseteq (\alpha)$, but $\beta \in (\alpha)$. So, dividing by α, we obtain $\frac{\beta}{\alpha}\mathfrak{p} \subseteq (1) = \mathcal{O}_K$, but $\frac{\beta}{\alpha} \notin \mathcal{O}_K$. □

Definition. A *fractional ideal* is an $\mathcal{O}_K$-module X such that $X \subseteq K$ and X is finitely generated.

$X = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}$ is an $\mathcal{O}_K$-module. If $\alpha \in \mathfrak{a} \setminus \{0\}$, then $\alpha X \subseteq \mathcal{O}_K = \mathbb{Z}^n$ where $n = [K : \mathbb{Q}]$. Multiplication by α is an isomorphism $X \to \alpha X$, and submodules of $\mathbb{Z}^n$ are finitely generated abelian groups, so X is finitely generated as an abelian group, hence as an $\mathcal{O}_K$-module. Hence X is a fractional ideal.

Lemma. $\mathfrak{q} \subseteq K$ is a fractional ideal if and only if there exists a nonzero constant $c \in K$ such that $c\mathfrak{q}$ is an ideal in $\mathcal{O}_K$.

Proof. Suppose $c\mathfrak{q}$ is an ideal. Then $\mathfrak{q} \subseteq K$, and multiplication by c is an isomorphism $\mathfrak{q} \to c\mathfrak{q}$ as $\mathcal{O}_K$-modules, so it is finitely generated as $\mathfrak{q}$ is.

Suppose $\mathfrak{q}$ is a fractional ideal. Then, $x_1, \dots, x_r$ generate $\mathfrak{q}$ as an $\mathcal{O}_K$-module. But $x_i \in K$ so $x_i = \frac{y_i}{n_i}$ where $y_i \in \mathcal{O}_K$, $n_i \in \mathbb{Z}$. Let c be the least common multiple of the n_i, and then $cq \subseteq \mathcal{O}_K$, and is a submodule of $\mathcal{O}_K$, and hence is an ideal. □

Corollary. $\mathfrak{q}$ is isomorphic to $\mathbb{Z}^n$ as an abelian group.

Proof. We have shown that all nonzero ideals in $\mathcal{O}_K$ are isomorphic to $\mathbb{Z}^n$ as abelian groups, where $n = [K : \mathbb{Q}]$, and multiplication by c is an isomorphism $\mathfrak{q} \to c\mathfrak{q}$. □

Ideals are sometimes called *integral ideals* to distinguish from fractional ideals. One can define multiplication of fractional ideals in the same way that we defined it for integral ideals.

Definition. A fractional ideal $\mathfrak{q}$ is *invertible* if there exists a fractional ideal $\mathfrak{r}$ such that $\mathfrak{q}\mathfrak{r} = (1) = \mathcal{O}_K$.

Proposition. Every nonzero fractional ideal $\mathfrak{q}$ is invertible, and its inverse is

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

Remark. $\mathfrak{q} = \frac{1}{n}\mathfrak{a}, \mathfrak{r} = \frac{1}{m}\mathfrak{b}$ where $\mathfrak{a}, \mathfrak{b}$ are integral ideals in $\mathcal{O}_K$, and $n, m \in K^\star$. Then $\mathfrak{q}\mathfrak{r} = 1$ if and only if $\mathfrak{a}\mathfrak{b} = (nm)$. Therefore, the proposition is equivalent to the statement that for every $\mathfrak{a} \trianglelefteq \mathcal{O}_K$, there exists an ideal $\mathfrak{b} \trianglelefteq \mathcal{O}_K$ such that $\mathfrak{a}\mathfrak{b}$ is principal.

Proof. $\mathfrak{q}$ is invertible if and only if $\mathfrak{a}$ is invertible, where $n\mathfrak{q} = \mathfrak{a}$ as above. So, without loss of generality, let $\mathfrak{q}$ be an integral ideal. If the proposition is false, there exists some integral ideal in $\mathcal{O}_K$. As $\mathcal{O}_K$ is Noetherian, there exists a maximal such ideal $\mathfrak{a} \neq \mathcal{O}_K$. So every ideal $\mathfrak{a}' \supsetneq \mathfrak{a}$ is invertible. Let $\mathfrak{b} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}$, which is a fractional ideal. $\mathcal{O}_K \subseteq \mathfrak{b}$ hence $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{b}$. If $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$, then part (i) of a previous lemma implies that $\mathfrak{b} \subseteq \mathcal{O}_K$. Part (ii) of the same lemma implies $\mathfrak{b} \setminus \mathcal{O}_K \neq \varnothing$, which is a contradiction. So $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{b} \subsetneq \mathcal{O}_K$. Then $\mathfrak{a}\mathfrak{b}$ is invertible by assumption, so $\mathfrak{a}$ is invertible, giving a contradiction. Finally, $\mathfrak{q}^{-1} \subseteq \{x \in K \mid x\mathfrak{q} \subseteq \mathcal{O}_K\} = X$, so $\mathfrak{q}\mathfrak{q}^{-1} = \mathcal{O}_K \subseteq \mathfrak{q}X \subseteq \mathcal{O}_K$, so we have equality: $\mathfrak{q}^{-1} = X$. □

Corollary. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \lhd \mathcal{O}_K$ be integral ideals, and let $\mathfrak{c} \neq (0)$. 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. The forward direction of parts (i) and (ii) are clear; the backward direction follows from multiplication by $\mathfrak{c}^{-1}$. The forward direction of part (iii) has already been seen. Now, suppose $\mathfrak{b} \subseteq \mathfrak{a}$. By the proposition above, there exists $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c} = (\alpha)$ is principal. Then, $\mathfrak{b} \subseteq \mathfrak{a}$ if and only if $\mathfrak{b}\mathfrak{c} \subseteq (\alpha)$ by part (i). $\mathfrak{a} \mid \mathfrak{b}$ if and only if $(\alpha) \mid \mathfrak{b}\mathfrak{c}$ by part (ii). But if $\mathfrak{b}\mathfrak{c}$ is generated by $\beta_1, \dots, \beta_r$, $\mathfrak{b}\mathfrak{c} \subseteq (\alpha)$ means that each β_i is divisible by α. More precisely, $\beta_i = \beta_i'\alpha$ for some $\beta_i' \in \mathcal{O}_K$. So $(\beta_1, \dots, \beta_r) = (\beta_1', \dots, \beta_r')(\alpha)$ proving part (iii). □

Remark. Part (iii) is straightforward if $\mathfrak{a}$ is principal, and invertibility via fractional ideals allows us to reduce to this case.

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

Proof. If $\mathfrak{a}$ is not prime, it is not maximal. Let $\mathfrak{b} \supsetneq \mathfrak{a}$ be an ideal in $\mathcal{O}_K$. Then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c}$ containing $\mathfrak{a}$ by part (iii) of the previous corollary. We continue factoring in this way. As the ring is Noetherian, this process will always terminate, as we produce an ascending chain.

For uniqueness, we have shown that $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. So if $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$ with $\mathfrak{p}_i, \mathfrak{q}_i$ prime, we have $\mathfrak{p}_1 \mid \mathfrak{q}_i$ for some i. So let $i = 1$ without loss of generality, so $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. But $\mathfrak{q}_1$ is maximal, so $\mathfrak{q}_1 = \mathfrak{p}_1$. Multiply by $\mathfrak{p}_1^{-1}$ to obtain $\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$, then by induction, the $\mathfrak{p}_i$ and $\mathfrak{q}_i$ match. □

Corollary. The nonzero fractional ideals form a group I_K under multiplication. I_K is the free abelian group generated by the prime ideals $\mathfrak{p} \lhd \mathcal{O}_K$. In other words, any $\mathfrak{q} \in I_K$ can be written uniquely as a product of prime ideals and their inverses. $\mathfrak{q} \in I_K$ is an integral ideal if and only if all of the exponents are nonnegative.

Proof. Follows from the previous theorem after writing $\mathfrak{q} = \mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_K$. □

2.3 Class group

Observe that we have a map $K^\star \to I_K$ mapping x to the principal ideal (x). This map is a group homomorphism, as $\alpha\beta \mapsto (\alpha)(\beta)$. Its kernel is the set of $\alpha \in K^\star$ such that $(\alpha) = (1) = \mathcal{O}_K$, which is the set $\mathcal{O}_K^\star$ of invertible elements of $\mathcal{O}_K$. The image is the set of principal ideals P_K.

Definition. The *class group* of a number field K is $\mathrm{Cl}_K = {}^{I_K}\!/_{P_K}$, the cokernel of the map $K^\star \to I_K$.

If $\mathfrak{a} \in I_K$, we write $[\mathfrak{a}]$ for its equivalence class in the class group, so $[\mathfrak{a}] = [\mathfrak{b}]$ if and only if there exists $\gamma \in K^\star$ such that $\gamma\mathfrak{a} = \mathfrak{b}$.

Theorem. The following are equivalent.

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

(ii) $\mathcal{O}_K$ is a unique factorisation domain;

(iii) Cl_K is trivial.

Proof. (i) holds if and only if (iii) holds by definition. (i) implies (ii) is a general fact from IB Groups, Rings and Modules. The proof that (ii) implies (i) remains. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, and $x \in \mathfrak{p}$ a nonzero element of this ideal. We can factorise x into irreducibles $x = \alpha_1 \dots \alpha_r$ uniquely by assumption. As $\mathfrak{p}$ is prime, some α_i lies in $\mathfrak{p}$. Then $(\alpha_i) \subseteq \mathfrak{p}$, and as $\mathcal{O}_K$ is a unique factorisation domain and α_i is irreducible, (α_i) is prime. But prime ideals are maximal, so $(\alpha_i) = \mathfrak{p}$ as required. □

The following sequence is exact.

$$\begin{tikzcd} 1 \arrow[r] & \mathcal{O}_K^\star \arrow[r] & K^\star \arrow[r] & I_K \arrow[r] & \mathrm{Cl}_K \arrow[r] & 1 \end{tikzcd}$$

We can now state the main theorems of the course, which are:

(i) the class group is finite;

(ii) $\mathcal{O}_K^\star$ is the direct product of the roots of unity in K with $\mathbb{Z}^{r+s-1}$.

Example. $(3, 1 + 2\sqrt{5})(3, 1 - 2\sqrt{5}) = (3)$, so $(3, 1 + 2\sqrt{5})$ and $(3, 1 - 2\sqrt{5})$ are inverse in the class group.

Example. Let $[L : \mathbb{Q}] = 2$, so $L = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$, and $d \not\equiv 1 \bmod 4$. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$, so $\mathfrak{a} \simeq \mathbb{Z}^2$ giving $\mathfrak{a} = (\alpha, \beta)$ as an $\mathcal{O}_L$-module. We can always assume $\beta \in \mathbb{Z}$. Indeed, write $\alpha = a + b\sqrt{d}$ and $\beta = a' + b'\sqrt{d}$. Assume $|a| + |a'|$ is minimal, so without loss of generality $a \geq a' \geq 0$, and if $a' \neq 0$, $\alpha - \beta, \beta$ has smaller $|a| + |a'|$.

Example. In a quadratic field $\mathfrak{a} = (\alpha, b)$ where $b \in \mathbb{Z}$. Then $(b, \alpha)(b, \overline{\alpha})$ is principal.

$$\mathfrak{a}\overline{\mathfrak{a}} = (b^2, b\alpha, b\overline{\alpha}, \alpha\overline{\alpha}) = (b^2, b\alpha, b\underbrace{(\alpha + \overline{\alpha})}_{\mathrm{Tr}(\alpha)}, N(\alpha)) = (b\alpha, c)$$

where $c = \gcd(b^2, \mathrm{Tr}(\alpha), N(\alpha))$. Let $x = \frac{b\alpha}{c} \in L^\star$. $\mathrm{Tr}(x) = \frac{b\,\mathrm{Tr}(\alpha)}{c} \in \mathbb{Z}$, and $N(c) = N\left(\frac{b\alpha}{c}\right) = \frac{b^2 N(\alpha)}{c^2} = \frac{b^2}{c}\frac{N(\alpha)}{c} \in \mathbb{Z}$, so $x \in \mathcal{O}_L$, giving $c \mid b\alpha$, so $\mathfrak{a}\overline{\mathfrak{a}} = (c)$. In particular, $(b, \alpha), (b, \overline{\alpha})$ are inverse in the class group.

2.4 Norms of ideals

Definition. Let L be a number field, and let $[L : \mathbb{Q}] = n$. Let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ be a nonzero ideal. The *norm* of $\mathfrak{a}$ is $\left|\mathcal{O}_L/\mathfrak{a}\right|$.

By Lagrange's theorem, $N(\mathfrak{a}) \cdot 1 = 0$ in $\mathcal{O}_L/\mathfrak{a}$. Hence $N(\mathfrak{a}) \in \mathfrak{a} \cap \mathbb{Z}$.

Example. Let p be a prime. $N((p)) = \left|\mathbb{Z}^n/(p\mathbb{Z})^n\right| = p^n$.

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

Remark. By unique factorisation of ideals, it suffices to show that

$$N(\mathfrak{p}_1^{a_1} \dots \mathfrak{p}_n^{a_n}) = N(\mathfrak{p}_1)^{a_1} \dots N(\mathfrak{p}_n)^{a_n}$$

for $\mathfrak{p}_i$ distinct prime ideals. To show this, we need that

(i) ${}^{\mathcal{O}_L}\!/_{\mathfrak{p}_1^{a_1} \dots \mathfrak{p}_n^{a_n}} \simeq {}^{\mathcal{O}_L}\!/_{\mathfrak{p}_1^{a_1}} \dots {}^{\mathcal{O}_L}\!/_{\mathfrak{p}_n^{a_n}}$ by the Chinese remainder theorem.

(ii) $\left|{}^{\mathcal{O}_L}\!/_{\mathfrak{p}^e}\right| = \left|{}^{\mathcal{O}_L}\!/_{\mathfrak{p}}\right| \cdot \left|{}^{\mathfrak{p}}\!/_{\mathfrak{p}^2}\right| \cdots \left|{}^{\mathfrak{p}^{e-1}}\!/_{\mathfrak{p}^e}\right|$ which is a general fact, and this is equal to $\left|{}^{\mathcal{O}_L}\!/_{\mathfrak{p}}\right|^e$ as ${}^{\mathfrak{p}^a}\!/_{\mathfrak{p}^{a+1}}$ is a one-dimensional vector space over the field ${}^{\mathcal{O}_L}\!/_{\mathfrak{p}}$. This fact is specific to number fields (or more generally, Dedekind domains). For a counterexample, consider $\mathbb{F}_p[X, Y]$ and $\mathfrak{p} = (x, y)$.

The following proof uses the above approach obscurely but quickly.

Proof. By unique factorisation it suffices to show the result for $\mathfrak{b} = \mathfrak{p}$ where $\mathfrak{p}$ is prime. $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}$ by unique factorisation, so let $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}$. We claim that the homomorphism of abelian groups ${}^{\mathcal{O}_L}\!/_{\mathfrak{p}} \to {}^{\mathfrak{a}}\!/_{\mathfrak{a}\mathfrak{p}}$ mapping $x \mapsto \alpha x$ is an isomorphism. Then,

$${}^{\mathcal{O}_L}\!/_{\mathfrak{a}} \simeq {}^{\left({}^{\mathcal{O}_L}\!/_{\mathfrak{a}\mathfrak{p}}\right)}\!/_{\left({}^{\mathfrak{a}}\!/_{\mathfrak{a}\mathfrak{p}}\right)}$$

so

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

but $\left|{}^{\mathfrak{a}}\!/_{\mathfrak{a}\mathfrak{p}}\right| = \left|{}^{\mathcal{O}_L}\!/_{\mathfrak{p}}\right| = N(\mathfrak{p})$ by the claim, proving the proposition. We now prove the claim.

We show the homomorphism is injective. $(\alpha) \subseteq \mathfrak{a}$ so $(\alpha) = \mathfrak{a}\mathfrak{c}$ for some $\mathfrak{c} \vartriangleleft \mathcal{O}_L$. Suppose x has $\alpha x \in \mathfrak{a}\mathfrak{p}$, so $x + \mathfrak{p}$ is in the kernel. Then, $x\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}\mathfrak{p}$. Dividing by $\mathfrak{a}$, $x\mathfrak{c} \subseteq \mathfrak{p}$. But $\mathfrak{p}$ is prime, so $x \in p$ or $\mathfrak{c} \subseteq \mathfrak{p}$. But $\mathfrak{c} \subseteq \mathfrak{p}$ implies $\alpha \in \mathfrak{a}\mathfrak{p}$, contradicting our choice of α. So $x \in \mathfrak{p}$, so the map is injective as required.

We show the homomorphism is surjective. We want to show $(\alpha) + \mathfrak{a}\mathfrak{p} = \mathfrak{a}$. We know that $\mathfrak{a}\mathfrak{p} \subsetneq (\alpha) + \mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a}$. Multiplying by $\mathfrak{a}^{-1}$, we obtain

$$\mathfrak{p} \subsetneq ((\alpha) + \mathfrak{a}\mathfrak{p})\mathfrak{a}^{-1} \subseteq \mathcal{O}_L$$

But $\mathfrak{p}$ is a prime and hence maximal. Therefore, $((\alpha) + \mathfrak{a}\mathfrak{p})\mathfrak{a}^{-1} = \mathcal{O}_L$, so $(\alpha) + p = \mathfrak{a}$, so the map is surjective. □

Lemma. Let $M \subseteq \mathbb{Z}^n$ be a subgroup. Then $M \simeq \mathbb{Z}^r$ for some $0 \leq r \leq n$. Suppose further that $r = n$. Let $e_1, \dots, e_n$ be a basis of $\mathbb{Z}^n$ and $v_1, \dots, v_n$ be a basis of M over $\mathbb{Z}$. Then, $\left|{}^{\mathbb{Z}^n}\!/_{M}\right| = \det A$ where $A = (a_{ij})$ and $v_j = \sum a_{ij} e_i$.

Proof. We can choose a basis $v_1, \dots, v_n$ of M such that A is upper triangular. Then, $|\det A| = |a_{11} \dots a_{nn}|$. □

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

(i) There exist $\alpha_1, \dots, \alpha_n \in \mathfrak{a}$ such that $\mathfrak{a} = \left\{\sum_{i=1}^n r_i\alpha_i \mid r_i \in \mathbb{Z}\right\}$, and $\alpha_1, \dots, \alpha_n$ are a basis of $L/\mathbb{Q}$.

(ii) For any such $\alpha_1, \dots, \alpha_n \in \mathfrak{a}$, $\Delta(\alpha_1, \dots, \alpha_n) = N(\mathfrak{a})^2 D_L$ where D_L is the discriminant of L, and where $\Delta(\alpha_1, \dots, \alpha_n) = \det \operatorname{Tr}(\alpha_i\alpha_j) = \left(\det(\sigma_i\alpha_j)\right)^2$.

Proof. Part (i). The result holds for $\mathcal{O}_L$, and if $d \in \mathfrak{a}$ is an integer, such as $d = N(\mathfrak{a})$, then $d\mathcal{O}_L \subseteq \mathfrak{a} \subseteq \mathcal{O}_L$, so as abelian groups, $(d\mathbb{Z})^n \subseteq \mathfrak{a} \subseteq \mathbb{Z}^n$, so $\mathfrak{a} \simeq \mathbb{Z}^n$.

Part (ii). Let $\alpha_1', \dots, \alpha_n'$ be an integral basis of $\mathcal{O}_L$. Let A be the change of basis matrix from $\alpha_1, \dots, \alpha_n$ to $\alpha_1', \dots, \alpha_n'$. Then $\Delta(\alpha_1, \dots, \alpha_n) = (\det A)^2 \Delta(\alpha_1', \dots, \alpha_n') = \left|{}^{\mathcal{O}_L}\!/\!_{\mathfrak{a}}\right|^2 D_L$ by the lemma. □

Corollary. If $\alpha_1, \dots, \alpha_n$ generating $\mathfrak{a}$ as a $\mathbb{Z}$-module has $\Delta(\alpha_1, \dots, \alpha_n)$ square-free, then $\mathfrak{a} = \mathcal{O}_L$ and D_L is square-free. In particular, if $L = \mathbb{Q}(\alpha)$ and $\alpha \in \mathcal{O}_L$ where the discriminant $\operatorname{disc}(\alpha) = \Delta(1, \alpha, \dots, \alpha^{n-1})$ is square-free, then $\mathbb{Z}[\alpha] = \mathcal{O}_L$. More generally, if $\alpha \in \mathcal{O}_L$ and $L = \mathbb{Q}(\alpha)$, and $d \in \mathbb{Z}$ is a maximal integer such that $d^2 \mid \operatorname{disc}(\alpha)$, then $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L \subseteq \frac{1}{d}\mathbb{Z}[\alpha]$.

Lemma. Let $\alpha \in \mathcal{O}_L$ be a nonzero algebraic integer. Then $N((\alpha)) = |N_{L/\mathbb{Q}}(\alpha)|$.

Proof. Let $\alpha_1, \dots, \alpha_n$ be an integral basis of $\mathcal{O}_L$. Consider

$$\begin{aligned}\Delta(\alpha_1\alpha, \dots, \alpha_n\alpha) &= \left(\det(\sigma_i(\alpha_j\alpha))\right)^2 \\ &= \left(\det((\sigma_i\alpha_j)(\sigma_i\alpha))\right)^2 \\ &= \left(\prod_{i=1}^n \sigma_i(\alpha) \cdot \det(\sigma_i\alpha_j)\right)^2 \\ &= N(\alpha)^2 \Delta(\alpha_1, \dots, \alpha_n) \\ &= N(\alpha)^2 D_L\end{aligned}$$

But $\alpha_1\alpha, \dots, \alpha_n\alpha$ is a basis of (α), hence this is equal to $N((\alpha))^2 D_L$. So $N((\alpha))^2 = N_{L/\mathbb{Q}}(\alpha)^2$, but $N((\alpha)) > 0$, giving the result as required. □

2.5 Prime ideals

Lemma. Let $\mathfrak{p} \lhd \mathcal{O}_L$ be a prime ideal. Then there exists a unique prime $p \in \mathbb{Z}$ such that $\mathfrak{p} \mid (p) = p\mathcal{O}_L$. Moreover, $N(\mathfrak{p}) = p^f$ for some integer $1 \leq f \leq n = [L : \mathbb{Q}]$.

Proof. $\mathfrak{p} \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$, hence principal. So for some $p \in \mathbb{Z}$, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$; we claim p is prime. If $p = ab$ with $a, b \in \mathbb{Z}$, then as $p \in \mathfrak{p}$, a or b lie in $\mathfrak{p} \cap \mathbb{Z}$, so a or b lie in $p\mathbb{Z}$, so $p \mid a$ or $p \mid b$. By factorisation of ideals, $(p) = \mathfrak{p}\mathfrak{a}$ for some $\mathfrak{a} \trianglelefteq \mathcal{O}_L$. Taking norms, $N((p)) = N(\mathfrak{p})N(\mathfrak{a})$. But $N((p)) = p^n$, so $N(\mathfrak{p}) = p^f$ for $1 \leq f \leq n$. □

Remark. Every prime ideal in $\mathcal{O}_L$ is a factor of $(p) \lhd \mathbb{Z}$ where p is a prime. Hence, we can factorise (p) as $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ for each prime $p \in \mathbb{Z}$ to identify all prime ideals in $\mathcal{O}_L$.

Let $p \in \mathbb{Z}$ be a prime. Consider the map $q : \mathcal{O}_L \to {}^{\mathcal{O}_L}\!/_{p\mathcal{O}_L}$, which is a surjection. By the isomorphism theorem, there is a bijection $I \mapsto q^{-1}(I)$ with inverse $J \mapsto {}^{J}\!/_{(p)}$ between the set of ideals in ${}^{\mathcal{O}_L}\!/_{p\mathcal{O}_L}$ and ideals of $\mathcal{O}_L$ containing $p\mathcal{O}_L$, or equivalently, ideals $\mathfrak{p} \lhd \mathcal{O}_L$ with $\mathfrak{p} \mid (p)$. The bijection maps prime ideals to prime ideals.

Under certain assumptions, we can determine the prime ideals in ${}^{\mathcal{O}_L}\!/_{(p)}$ exactly.

> **Theorem** (Dedekind's criteria). Let $\alpha \in \mathcal{O}_L$ have minimal polynomial $g(x) \in \mathbb{Z}[x]$. Suppose that $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ has finite index $\left|{}^{\mathcal{O}_L}\!/_{\mathbb{Z}[\alpha]}\right|$ not divisible by p. Let $\overline{g}(x) = g(x) \bmod p \in \mathbb{F}_p[x]$. Let $\overline{g}(x) = \overline{\varphi}_1^{e_1} \dots \overline{\varphi}_r^{e_r}$ be the factorisation of $g(x)$ into irreducibles in $\mathbb{F}_p[x]$. Then $p\mathcal{O}_L = (p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i = (p, \varphi_i(\alpha))$ is the prime ideal in $\mathcal{O}_L$ where we choose any monic polynomial $\varphi_i(x) \in \mathbb{Z}[x]$ which has reduction mod p equal to $\overline{\varphi}_i(x)$.

Proof. First, we show that each factor $\overline{\varphi}_i$ defines a prime ideal in ${}^{\mathbb{Z}[\alpha]}\!/_{p\mathbb{Z}[\alpha]}$. We will then relate this to prime ideals in ${}^{\mathcal{O}_L}\!/_{p\mathcal{O}_L}$. We have a surjective ring homomorphism $\mathbb{Z}[x] \to {}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i}$.

We claim that the kernel of this homomorphism is the ideal generated by p, φ_i. We can factor the map as $\mathbb{Z}[\alpha] \to \mathbb{F}_p[x] \to {}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i}$. It is clear that p, φ_i lie in the kernel. If $f \mapsto 0$, then $\overline{\varphi}_i \mid \overline{f}$ so there exists $\overline{h} \in \mathbb{F}_p[x]$ such that $\overline{f} = \overline{\varphi}_i \overline{h}$, so $f = \varphi_i h + ps$ for any lift h of $\overline{h}$ of the same degree. So the kernel is precisely (p, φ_i).

We can alternatively factor the map as $\mathbb{Z}[\alpha] \to {}^{\mathbb{Z}[x]}\!/_{g(x)\mathbb{Z}[x]} \to {}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i}$. We claim that the kernel of the map $\mathbb{Z}[\alpha] \to \mathbb{F}_p[\alpha] = {}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i}$ is the ideal $\mathfrak{q}_i \lhd \mathbb{Z}[\alpha]$ generated by $p, \varphi_i(\alpha)$. The proof of this claim is left as an exercise. Therefore, ${}^{\mathbb{Z}[\alpha]}\!/_{\mathfrak{q}_i} \simeq {}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i(x)}$. But $\overline{\varphi}_i(x)$ is irreducible by hypothesis, so ${}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i(x)}$ is a field, hence $\mathfrak{q}_i$ is a prime ideal. Therefore, ${}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i} \simeq \mathbb{F}_q$ where $q = p^{f_i}$ is some power of p. In particular, $\left|{}^{\mathbb{Z}[\alpha]}\!/_{\mathfrak{q}_i}\right| = \left|{}^{\mathbb{F}_p[x]}\!/_{\overline{\varphi}_i(x)}\right| = p^{f_i}$ where $f_i = \deg \overline{\varphi}_i$.

Now, if $\mathbb{Z}[\alpha] = \mathcal{O}_L$ the first part implies that $\mathfrak{p}_i = \mathfrak{q}_i$ is a prime ideal containing p, and $N(\mathfrak{p}_i) = p^{f_i}$. Suppose $p \nmid \left|{}^{\mathcal{O}_L}\!/_{\mathbb{Z}[\alpha]}\right|$. We claim that the inclusion map defines an isomorphism $\iota : {}^{\mathbb{Z}[\alpha]}\!/_{p\mathbb{Z}[\alpha]} \to {}^{\mathcal{O}_L}\!/_{p\mathcal{O}_L}$. This implies that there is a bijection between ideals of ${}^{\mathbb{Z}[\alpha]}\!/_{p\mathbb{Z}[\alpha]}$ and ideals of ${}^{\mathcal{O}_L}\!/_{p\mathcal{O}_L}$. Hence, there is a bijection between ideals of $\mathbb{Z}[\alpha]$ containing p and ideals of $\mathcal{O}_L$ containing p, where this bijection maps an ideal $(p, y) \trianglelefteq \mathbb{Z}[\alpha]$ to $\mathfrak{p} \trianglelefteq \mathcal{O}_L$ generated by the same elements under the inclusion map. In other words, it maps an ideal $\mathfrak{q}$ to $\mathfrak{q}\mathcal{O}_L$. The inverse bijection maps $\mathfrak{p}$ to $\mathfrak{p} \cap \mathbb{Z}[\alpha]$. Moreover, ${}^{\mathcal{O}_L}\!/_{\mathfrak{p}} \simeq {}^{\mathbb{Z}[\alpha]}\!/_{\mathfrak{p} \cap \mathbb{Z}[\alpha]}$ hence $N(\mathfrak{p}_i) = p^{\deg \overline{\varphi}_i} = p^{f_i}$ for $\mathfrak{p}_i$ as above.

We now prove the claim. The map ${}^{\mathcal{O}_L}\!/_{\mathbb{Z}[\alpha]} \to {}^{\mathcal{O}_L}\!/_{\mathbb{Z}[\alpha]}$ given by multiplication by p is an isomorphism. It is injective as the kernel is a p-group so must be trivial, and ${}^{\mathcal{O}_L}\!/_{\mathbb{Z}[\alpha]}$ is a finite abelian group, so this is an isomorphism. But the kernel of the map $\iota : {}^{\mathbb{Z}[\alpha]}\!/_{p\mathbb{Z}[\alpha]} \to {}^{\mathcal{O}_L}\!/_{p\mathcal{O}_L}$ is ${}^{\mathbb{Z}[\alpha] \cap p\mathcal{O}_L}\!/_{p\mathbb{Z}[\alpha]}$, which is precisely the kernel of the map given by multiplication by p. So ι is injective.

ι is surjective if $\mathcal{O}_L = \mathbb{Z}[\alpha] + p\mathcal{O}_L$. The map given by multiplication by p is surjective, so ι is indeed surjective, and hence an isomorphism as required.

We have now constructed prime ideals $\mathfrak{p}_i = (p, \varphi_i(\alpha)) \lhd \mathcal{O}_L$ containing p with norm $N(\mathfrak{p}_i) = p^{f_i}$ with $f_i = \deg \overline{\varphi}_i$. We must now show that there are no other ideals containing p. Now, $\mathfrak{p}_i^{e_i} = (p, \varphi_i(\alpha))^{e_i} \subseteq (p, \varphi_i(\alpha)^{e_i})$, so

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \subseteq (p, \varphi_1(\alpha)^{e_1}) \dots (p, \varphi_r(\alpha)^{e_r}) \subseteq (p, \varphi_1(\alpha)^{e_1} \dots \varphi_r(\alpha)^{e_r})$$

But $\overline{\varphi_1^{e_1} \dots \varphi_r^{e_r}} = \overline{g}$, so $\varphi_1^{e_1} \dots \varphi_r^{e_r} = g + ps$. So $(p, \varphi_1(\alpha)^{e_1} \dots \varphi_r(\alpha)^{e_r}) = (p, g(\alpha)) = (p)$ as $g(\alpha) = 0$. So $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \subseteq (p)$. But $[L : \mathbb{Q}] = n = \deg g = \deg \overline{g} = \sum_{i=1}^r e_i \deg \overline{\varphi}_i = \sum_{i=1}^r e_i f_i$. Taking norms,

$$N(\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}) = \prod_{i=1}^r N(\mathfrak{p}_i)^{e_i} = p^{e_1 f_1 + \dots + e_r f_r} = p^n = N((p))$$

One can show that if $\mathfrak{a} \subseteq \mathfrak{b}$ and $N(\mathfrak{a}) = N(\mathfrak{b})$, then $\mathfrak{a} = \mathfrak{b}$. So the two ideals are equal.

Note that if $i \neq j$, $\overline{\varphi}_i, \overline{\varphi}_j$ are coprime in $\mathbb{F}_p[x]$, so $\mathfrak{p}_i + \mathfrak{p}_j = (p, \varphi_i(\alpha), \varphi_j(\alpha)) \neq \mathfrak{p}_i$, so $\mathfrak{p}_i \neq \mathfrak{p}_j$. □

Note that since we choose a monic polynomial, $\deg \varphi_i(x) = \deg \overline{\varphi}_i(x)$. Different choices of $\varphi_i(x)$ give the same ideal as p is in the ideal. $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$, and $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ is the factorisation of (p) into irreducibles.

Remark. Most $\alpha \in \mathcal{O}_L$ have ${}^{\mathcal{O}_L}\!/\!{}_{\mathbb{Z}[\alpha]}$ finite, but the condition that $p \nmid \left| {}^{\mathcal{O}_L}\!/\!{}_{\mathbb{Z}[\alpha]} \right|$ is restrictive.

Example. Let $L = \mathbb{Q}(\sqrt{-11})$, and let us factorise $(5) \subseteq \mathcal{O}_L$. As $-11 \equiv 1 \bmod 4$, $\mathbb{Z}[\sqrt{-11}] \neq \mathcal{O}_L$. So $\mathbb{Z}[\sqrt{-11}]$ has index 2 in $\mathcal{O}_L$, and $5 \nmid 2$, so Dedekind's theorem applies. Modulo 5, $x^2+1 = (x-2)(x+2)$, so $(5) = (5, -2 + \sqrt{-11})(5, -2 - \sqrt{-11})$.

Example. In general, let $L = \mathbb{Q}(\sqrt{d})$ where d is square free and not equal to zero or one. Let p be an odd prime. Then, $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_L$ has index 1 or 2, and both are coprime to p. Factorising $x^2 - d$ modulo p, there are three cases.

- Suppose there are two distinct roots modulo p of $x^2 - d$. Then, using the Legendre symbol, $\left(\frac{d}{p}\right) = 1$. In this case, $x^2 - d = (x - r)(x + r)$ for some $r \in \mathbb{Z}$. By Dedekind's theorem, $p = \mathfrak{p}_1 \mathfrak{p}_2$ where $\mathfrak{p}_1 = (p, \sqrt{d} - r)$ and $\mathfrak{p}_2 = (p, \sqrt{d} + r)$. In this case, $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$; we say p *splits* in $L/\mathbb{Q}$.
- Suppose $x^2 - d$ is irreducible modulo p. Then $\left(\frac{d}{p}\right) = -1$. $(p) = \mathfrak{p}$ is prime; we say p is *inert* in L.
- Suppose $x^2 - d$ has a repeated root, so $d \equiv 0$ modulo p. Then $\left(\frac{d}{p}\right) = 0$. In this case, Dedekind's theorem gives $(p) = \mathfrak{p}^2$ where $\mathfrak{p} = (p, \sqrt{d})$. We say that p *ramifies* in L.

Now consider the case $p = 2$.

Lemma. 2 splits in L if and only if $d \equiv 1 \bmod 8$. 2 is inert in L if and only if $d \equiv 5 \bmod 8$. 2 ramifies in L if and only if $d \equiv 2, 3 \bmod 4$.

Proof. If $d \equiv 1 \bmod 4$, then $\mathcal{O}_L = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1}{2}(1+\sqrt{d})$. The minimal polynomial of α is $x^2 - x + \frac{1}{4}(1-d)$. Reducing modulo 2, if $d \equiv 1 \bmod 8$ then this is $x(x+1)$ so 2 splits. If $d \equiv 5 \bmod 8$ then this gives x^2+x+1 which is irreducible, so 2 is inert. If $d \equiv 2, 3 \bmod 4$, then $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$ and $x^2 - d$ is either x^2 or $(x-1)^2$, which ramifies. □

Recall that $D_L = 4d$ if $d \equiv 2, 3 \bmod 4$, and $D_L = d$ if $d \equiv 1 \bmod 4$.

Corollary. Let $L = \mathbb{Q}(\sqrt{d})$. $p \mid D_L$ if and only if p ramifies in L.

Proof. Case analysis. □

Definition. Let $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ be the factorisation of (p) into irreducibles in $\mathcal{O}_L$, where $p^{f_i} = N(\mathfrak{p}_i)$. We say that

- p *ramifies* if some e_i is greater than 1;
- p *is inert* if $r = 1$ and $e_1 = 1$, so (p) remains prime;
- p *splits* or *splits completely* if $r = n$ and $e_i = f_i = \dots = e_n = f_n = 1$.

Corollary. Let p be a prime and $p < n = [L : \mathbb{Q}]$. Let $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ have finite index coprime to p. Then p does not split completely.

Proof. Let g be the minimal polynomial of α. Suppose p splits, so g has n distinct roots in $\mathbb{F}_p$ by Dedekind's theorem. But $n > p$, so this is not possible. □

Example. Let $L = \mathbb{Q}(\alpha)$ and α has minimal polynomial $x^3 - x^2 - 2x - 8$. On an example sheet, we show that 2 splits completely in $\mathcal{O}_L$. Hence, for all $\beta \in \mathcal{O}_L \setminus \mathbb{Z}$, $\mathbb{Z}[\beta] \subseteq \mathcal{O}_L$ has even index.

Note that Dedekind's theorem allows for the factorisation of (p) for all but finitely many p, as if $\alpha \in \mathcal{O}_L$ with ${}^{\mathcal{O}_L}\!/\!_{\mathbb{Z}[\alpha]}$ finite, only finitely many primes p divide its order.

Theorem. For all primes p, we have $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ with ${}^{\mathcal{O}_L}\!/\!_{\mathfrak{p}_i} = {}^{\mathbb{F}_p[x]}\!/\!_{\overline{\varphi}_i(x)}$ where $\overline{\varphi}_i \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree f_i and $N(\mathfrak{p}_i) = p^{f_i}$, and ${}^{\mathcal{O}_L}\!/\!_{p\mathcal{O}_L} \simeq \prod_{i=1}^r {}^{\mathbb{F}_p[x]}\!/\!_{\overline{\varphi}_i(x)} = \prod_{i=1}^r \mathbb{F}_{p^{f_i}}$.

Dedekind's theorem implies that this holds if there exists $\alpha \in \mathcal{O}_L$ with $p \nmid \left| {}^{\mathcal{O}_L}\!/\!_{\mathbb{Z}[\alpha]} \right| < \infty$.

Theorem. p ramifies in L if and only if $p \mid D_L$.

3 Geometry of numbers

3.1 Imaginary quadratic fields

Let $L = \mathbb{Q}(\sqrt{d})$ where d is square-free and $d < 0$. $\mathcal{O}_L = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1}{2}(1 + \sqrt{d})$ or $\alpha = \sqrt{d}$. Choose a square root of d in $\mathbb{C}$ to construct an embedding of $\mathcal{O}_L$ into $\mathbb{C}$.

Suppose $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 \subseteq \mathbb{R}^2$ where $\mathbb{R}^2$ is equipped with the Euclidean norm, and v_1, v_2 are linearly independent over $\mathbb{R}$. Let $A(\Lambda)$ be the area of the parallelogram generated by v_1 and v_2. If $v_i = a_i e_1 + b_i e_2$, we have

$$A(\Lambda) = \left|\det\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}\right|$$

Minkowski's lemma is that a closed disk S around zero contains a nonzero point of Λ whenever the area of S is at least $4A(\Lambda)$. More precisely, there exists $\alpha \in \Lambda$ such that $0 < |\alpha|^2 < \frac{4A(\Lambda)}{\pi}$. Note that this condition depends only on the area of the parallelogram, not its shape. This will be proven shortly.

We will apply this to $\Lambda = \mathfrak{a} \trianglelefteq \mathcal{O}_L$ for $L = \mathbb{Q}(\sqrt{d})$, $d < 0$ square-free. Let $\sqrt{d} \in \mathbb{C}$ be chosen with positive imaginary part to embed $\mathcal{O}_L$ in $\mathbb{C}$.

Lemma. (i) if $\alpha = a + b\sqrt{d} \in \mathcal{O}_L$, then $|\alpha|^2 = (a + b\sqrt{d})(a - b\sqrt{d}) = N(\alpha)$;

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

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

(iv) $A(\mathfrak{a}) = \frac{1}{2}|\Delta(\alpha_1, \alpha_2)|^{\frac{1}{2}}$ where α_1, α_2 are an integral basis for $\mathfrak{a}$.

Proof. Part (i) is clear. (iv) implies (ii) and (iii). We will prove (iv) later in a more general setting, giving the justification for the coefficient $\frac{1}{2}$.

We now prove (ii) and (iii) manually, without appealing to (iv). For part (ii), $\mathcal{O}_L$ has basis $1, \alpha$. Therefore, $A(\mathcal{O}_L) = \frac{1}{2}\sqrt{d}$ or $\sqrt{d}$, which is exactly $\frac{1}{2}\sqrt{|D_L|}$. Part (iii) is a variant of the fact that $\Delta(\alpha_1, \dots, \alpha_n) = N(\mathfrak{a})^2 D_L$. □

Minkowski's lemma implies that there exists $\alpha \in \mathfrak{a}$ with $N(\alpha) \leq \frac{4A(\mathfrak{a})}{\pi} = N(\mathfrak{a})C_L$ where $C_L = \frac{2\sqrt{|D_L|}}{\pi}$ is Minkowski's constant. Since $\alpha \in \mathfrak{a}$, $(\alpha) \subseteq \mathfrak{a}$. Hence $(\alpha) = \mathfrak{a}\mathfrak{b}$ for some $\mathfrak{b} \trianglelefteq \mathcal{O}_L$. So $N(\alpha) = N((\alpha)) = N(\mathfrak{a})N(\mathfrak{b})$, so $N(\mathfrak{b}) \leq C_L$.

Recall that the class group of L is ${}^{I_L}\!/\!{}_{P_L}$, the quotient of fractional ideals over principal ideals. Then, $[\mathfrak{b}] = [\mathfrak{a}^{-1}] \in \mathrm{Cl}_L$. Replacing $\mathfrak{a}$ with $\mathfrak{a}^{-1}$, we have shown that for all $[\mathfrak{a}] \in \mathrm{Cl}_L$, there exists a representative $\mathfrak{b}$ of $[\mathfrak{a}]$ which is an ideal with $N(\mathfrak{b}) \leq \frac{2\sqrt{|D_L|}}{\pi} = C_L$. But for all $m \in \mathbb{Z}$, the number of ideals $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ with $N(\mathfrak{a}) = m$ is finite; indeed, if $N(\mathfrak{a}) = m$, then $m \in \mathfrak{a}$ so $\mathfrak{a} \mid (m)$, but there are only finitely many ideals dividing (m), as they biject with ideals in ${}^{\mathcal{O}_L}\!/\!{}_{m\mathcal{O}_L} \simeq \left({}^{\mathbb{Z}}\!/\!{}_{m\mathbb{Z}}\right)^n$.

Therefore, we have shown that Cl_L is finite, and generated by the class of prime ideals dividing (p), for p a prime integer less than $\frac{2\sqrt{|D_L|}}{\pi} = C_L$. Indeed, if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ with $N(\mathfrak{a}) < C_L$, then $N(\mathfrak{p}_i) < C_L$.

Example. Let $d = -7$. Then $D_L = -7$, and $\frac{2\sqrt{7}}{\pi} < 2$. So there are no primes $p < C_L$, giving $\mathrm{Cl}_L = \{1\}$. In particular, $\mathcal{O}_L$ is a unique factorisation domain. Similarly, $d = -1, -2, -3$ give unique factorisation domains.

Example. Let $d = -5$. Here, $D_L = -20$, and $2 < \frac{4\sqrt{5}}{\pi} < 3$. Hence, Cl_L is generated by prime ideals dividing (2). Note that $(2) = (2, 1 + \sqrt{-5})^2$ by Dedekind's theorem.

We now must check if $(2, 1 + \sqrt{-5})$ is principal. If $(2, 1 + \sqrt{-5}) = (\beta)$, then $N(\beta) = 2$. But $\beta = a + b\sqrt{-5}$, so $N(\beta) = a^2 + 5b^2$, which is not satisfiable by integers. So $(2, 1 + \sqrt{-5})$ is principal but its square is, so $\mathrm{Cl}_L = \mathbb{Z}/2\mathbb{Z}$.

Example. Let $d = -17$, then $5 < C_L < 6$. Cl_L is generated by prime ideals dividing $(2), (3), (5)$. Modulo 2, $x^2 + 17 = x^2 + 1 = (x + 1)^2$, so $(2) = \mathfrak{p}^2$ where $\mathfrak{p} = (2, 1 + \sqrt{-17})$. Modulo 3, $x^2 + 17 = x^2 - 1 = (x + 1)(x - 1)$, giving $(3) = \mathfrak{q}\overline{\mathfrak{q}}$ where $\mathfrak{q} = (3, 1 + \sqrt{-17}), \overline{\mathfrak{q}} = (3, 1 - \sqrt{-17})$. Modulo 5, $x^2 + 17 = x^2 + 2$ which is irreducible, so (5) is inert, so is trivial in the class group.

Hence $\mathrm{Cl}_L = (\mathfrak{p}, \mathfrak{q}, \overline{\mathfrak{q}}) = (\mathfrak{p}, \mathfrak{q})$. We could compute powers of $\mathfrak{p}$ and $\mathfrak{q}$ until we obtain all nontrivial relations between them. A more efficient way to compute Cl_L in this case is to find principal ideals of small norm which are multiples of 2 and 3 to find the relations. Consider $(1 + \sqrt{-17})$, which has norm $N(1 + \sqrt{-17}) = 18 = 2 \cdot 3^2$. Note that $1 + \sqrt{-17} \in \mathfrak{p} \cap \mathfrak{q}$ so $(1 + \sqrt{-17}) = \mathfrak{p}\mathfrak{q}\mathfrak{r}$ where $\mathfrak{r} \in (\mathfrak{p}, \mathfrak{q})$. We can show that $\mathfrak{r} = \mathfrak{q}$. This shows that $[\mathfrak{p}] = [\mathfrak{q}]^{-2}$ in Cl_L. So Cl_L is generated by $[\mathfrak{q}]$. So it is cyclic, and we can show $[\mathfrak{q}]^2 \neq 1$, as $\mathfrak{p}$ is not principal, but $[\mathfrak{q}]^4 = [\mathfrak{p}^2]^{-1} = 1$. So $\mathrm{Cl}_L = \mathbb{Z}/4\mathbb{Z}$.

Theorem. Let $L = \mathbb{Q}(\sqrt{-d})$ with $d > 0$.
(i) $\mathcal{O}_L$ is a unique factorisation domain if $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$;
(ii) there are no others.

3.2 Lattices

Definition. A subset $X \subseteq \mathbb{R}^n$ is called *discrete* if for all $K \subseteq \mathbb{R}^n$ compact, $K \cap X$ is finite. Equivalently, for all $x \in X$ there exists $\varepsilon > 0$ with $B_\varepsilon(x) \cap X = \{x\}$.

Recall that $K \subseteq \mathbb{R}^n$ is compact if and only if it is closed and bounded.

Proposition. Let $\Lambda \subseteq \mathbb{R}^n$. Then the following are equivalent.
(i) Λ is a discrete subgroup of $(\mathbb{R}^n, +)$;
(ii) $\Lambda = \left\{\sum_{i=1}^m n_i x_i \mid n_i \in \mathbb{Z}\right\}$ where $x_1, \dots, x_m$ are linearly independent over $\mathbb{R}$.

Example. $\mathbb{Z}\sqrt{2} + \mathbb{Z}\sqrt{3} \subseteq \mathbb{R}$ is not discrete. If $\Lambda = \mathfrak{a} \trianglelefteq O_L$ is an ideal where $L = \mathbb{Q}(\sqrt{-d})$ and $d > 0$, Λ is discrete.

Proof. (ii) implies (i). Observe that if $g \in GL_n(\mathbb{R})$, then $g\Lambda$ is discrete if Λ is. $g\Lambda$ satisfies (ii) if and only if Λ does. Suppose property (ii) holds, so $\Lambda = \left\{\sum_{i=1}^m n_i x_i \mid n_i \in \mathbb{Z}\right\}$. There exists $g \in GL_n(\mathbb{R})$ such that $g x_i = e_i$ where the e_i form the standard basis of $\mathbb{R}^n$. Clearly, $\bigoplus_{i=1}^m \mathbb{Z}e_i$ is discrete.

(i) implies (ii). Let $y_1, \dots, y_m \in \Lambda$ which are $\mathbb{R}$-linearly independent such that m is maximal. Note that $m \leq n$. Also,

$$\left\{ \sum_{i=1}^{m} \lambda_i y_i \,\middle|\, \lambda_i \in \mathbb{R} \right\} = \left\{ \sum_{i=1}^{N} \lambda_\alpha z_\alpha \,\middle|\, \lambda_\alpha \in \mathbb{R}, z_\alpha \in \Lambda, N \geq 0 \right\}$$

This is the smallest $\mathbb{R}$-vector subspace of $\mathbb{R}^n$ containing Λ. Let $X = \left\{ \sum_{i=1}^m \lambda_i y_i \mid \lambda_i \in [0,1] \right\}$. This is closed and bounded, hence compact. Λ is discrete, so $X \cap \Lambda$ is finite.

Consider the subgroup $\mathbb{Z}^m = \bigoplus_{i=1}^m \mathbb{Z} y_i \subseteq \Lambda$. We can write $\lambda \in \Lambda$ as $\lambda = \lambda_0 + \lambda_1$ where $\lambda_0 \in X \cap \Lambda$ is the integral part and $\lambda_1 \in \mathbb{Z}^m = \bigoplus_{i=1}^m \mathbb{Z} y_i$ is the fractional part. Hence, $\left|{}^{\Lambda}\!/\!_{\mathbb{Z}^m}\right| \leq |X \cap \Lambda|$ is finite. Let $d = \left|{}^{\Lambda}\!/\!_{\mathbb{Z}^m}\right|$, so by Lagrange's theorem, $d = 0$ in ${}^{\Lambda}\!/\!_{\mathbb{Z}^m}$, so $d\Lambda \subseteq \mathbb{Z}^m$. In particular, $\mathbb{Z}^m \subseteq \Lambda \subseteq \frac{1}{d}\mathbb{Z}^m$. The structure theorem for finitely generated abelian groups shows that there exist $x_1, \dots, x_m \in \Lambda$ with $\Lambda = \bigoplus_{i=1}^m \mathbb{Z} x_i$. □

Definition. If rank $\Lambda = n$, so if $n = m$, we say Λ is a *lattice* in $\mathbb{R}^n$.

Definition. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice with basis $x_1, \dots, x_n$. The *fundamental parallelogram* is $P = \left\{ \sum_{i=1}^n \lambda_i x_i \mid \lambda_i \in [0,1] \right\}$. The *covolume* of Λ is the volume of P, which is $|\det A|$ if $x_i = \sum_{j=1}^n a_{ij} e_j$.

Note that if $x_1', \dots, x_n'$ are another basis of Λ, the change of basis matrix B given by $x_i' = \sum_{j=1}^m b_{ij} x_j$ has integer coefficients, so $B \in GL_n(\mathbb{Z})$, giving $\det B = \pm 1$. Hence, the covolume is well-defined irrespective of the choice of basis. Observe that P is a fundamental domain for the action of Λ on $\mathbb{R}^n$; $\mathbb{R}^n = \bigcup_{\gamma \in \Lambda} (\gamma + P)$ and $(\gamma + P) \cap (\mu + P) \subseteq \partial P$ if $\gamma \neq \mu$. We can think of P as a set of coset representatives for ${}^{\mathbb{R}^n}\!/\!_{\Lambda}$, ignoring the boundary of P; this can be justified by noting that ∂P has no volume.

3.3 Minkowski's lemma

Theorem. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, and P be a fundamental parallelogram for it. Let $S \subseteq \mathbb{R}^n$ be a measurable set.

(i) If $\mathrm{vol}(S) > \mathrm{covol}(\Lambda)$, there exist $x, y \in S$ with $x \neq y$ and $x - y \in \Lambda$.

(ii) Suppose $s \in S$ if and only if $-s \in S$, so S is *symmetric around zero*, and that S is convex. Then, if
  (a) $\mathrm{vol}(S) > 2^n \, \mathrm{covol}(\Lambda)$, or
  (b) $\mathrm{vol}(S) \geq 2^n \, \mathrm{covol}(\Lambda)$ and S is closed,
then there exists $\gamma \in S \cap \Lambda$ with $\gamma \neq 0$.

Note that this implies the result we used when $n = 2$. In the case of the square lattice $\Lambda = \mathbb{Z}^n$ and $S = [-1,1]^n$, we can see that these bounds are sharp.

Proof. Part (i). Observe that $\mathrm{vol}(S) = \sum_{\gamma \in \Lambda} \mathrm{vol}(S \cap (P + \gamma))$ as P is a fundamental domain, volume is additive, and $\mathrm{vol}(\partial(P + \gamma)) = 0$. Note that $\mathrm{vol}(S \cap (P + \gamma)) = \mathrm{vol}((S - \gamma) \cap P)$ as volume is translation invariant. We claim that the sets $(S - \gamma) \cap P$ are not pairwise disjoint. Indeed, if they were, then

$\mathrm{vol}(P) \geq \sum_{\gamma\in\Lambda} \mathrm{vol}((S-\gamma)\cap P) = \mathrm{vol}(S)$ contradicting the assumption. Hence there exists $\gamma\mu \in \Lambda$ with $\gamma \neq \mu$ such that $(S-\gamma)\cap P$ and $(S-\mu)\cap P$ are not disjoint, so there exist $x, y \in S$ with $x-\gamma = y-\mu$, hence $x-y \in \Lambda$.

Part (ii)(a). Let $S' = \frac{1}{2}S = \left\{\frac{1}{2}s \mid s \in S\right\}$. Then $\mathrm{vol}(S') = 2^{-n}\,\mathrm{vol}(S) > \mathrm{covol}(\Lambda)$ by assumption. By part (i), there exist $y, z \in S'$ with $y - z \in \Lambda \setminus \{0\}$. But $y - z = \frac{1}{2}(2y + -2z)$. $2z \in S$ so $-2z \in S$ as S is symmetric around zero. $2y \in S$, and S is convex, so $y - z \in S$ as required.

Part (ii)(b). Apply part (ii)(a) to $S_m = \left(1 + \frac{1}{m}\right)S$ for all $m \in \mathbb{N}, m > 0$. We obtain $\gamma_m \in S_m \cap \Lambda$ with $\gamma_m \neq 0$. By convexity of S, $S_m \subseteq S_1$. So $\gamma_1, \gamma_2, \dots$ are contained in $S_1 \cap \Lambda$, which is a finite set as S_1 is closed and bounded (without loss of generality) and Λ is discrete. So there exists $\gamma \in S_m \cap \Lambda$ such that $\gamma_m = \gamma$ for infinitely many m. Hence, $\gamma \in \bigcap_{m>0} S_m = S$ as S is closed. Therefore $\gamma \in S \cap \Lambda$ with $\gamma \neq 0$. □

Let L be a number field and let $n = [L : \mathbb{Q}]$. Let $\sigma_1, \dots, \sigma_r : L \to \mathbb{R}$ be the real embeddings, and $\sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \dots, \overline{\sigma_{r+s}} : L \to \mathbb{C}$ be the complex embeddings, where $r + 2s = n$. This gives an embedding

$$(\sigma_1, \dots, \sigma_{r+s}) : L \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \xrightarrow{\simeq} \mathbb{R}^r \times \mathbb{R}^{2s} = \mathbb{R}^{r+2s}$$

In other words, we can write

$$\sigma = (\sigma_1, \dots, \sigma_r, \mathrm{Re}\,\sigma_{r+1}, \mathrm{Im}\,\sigma_{r+1}, \dots, \mathrm{Re}\,\sigma_{r+s}, \mathrm{Im}\,\sigma_{r+s})$$

Lemma. $\sigma(\mathcal{O}_L)$ is a lattice in $\mathbb{R}^n$ of covolume $2^{-s}|D_L|^{\frac{1}{2}}$. If $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ is an ideal, then $\sigma(\mathfrak{a})$ is a lattice, and $\mathrm{covol}(\sigma(\mathfrak{a})) = 2^{-s}|D_L|^{\frac{1}{2}}N(\mathfrak{a})$.

Proof. The first part is a special case of the second part. Recall that $\mathfrak{a}$ has an integral basis $\gamma_1, \dots, \gamma_n$, and $(\det(\sigma_i(\gamma_j)))^2 = \Delta(\gamma_1, \dots, \gamma_n) = N(\mathfrak{a})^2 D_L$. Hence, $|\det(\sigma_i(\gamma_j))| = N(\mathfrak{a})|D_L|^{\frac{1}{2}}$. Note that if $\sigma_{r+i}(\gamma)\overline{\sigma_{r+i}(\gamma)} = z\overline{z}$,

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

The determinant of the change of basis matrix is $-\frac{1}{2}$. □

Proposition (Minkowski bound)**.** Let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$. Then there exists $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$ and $|N(\alpha)| \leq C_L N(\mathfrak{a})$ where $C_L = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}|D_L|^{\frac{1}{2}}$.

Proof. Let

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

This set is closed and bounded, hence compact. It is also convex, symmetric around zero, and measurable with volume $2^r\left(\frac{\pi}{2}\right)^2\frac{t^n}{n!}$. Choose t such that the volume of $B_{r,s}(t)$ is $2^n\,\mathrm{covol}(\mathfrak{a})$, so $t^n =$

$\left(\frac{4}{\pi}\right)^s n!|D_L|^{\frac{1}{2}}N(\mathfrak{a})$. Minkowski's lemma implies that there exists $\alpha \in \mathfrak{a}$ and $\alpha \neq 0$ such that $\sigma(\alpha) = (y_1, \dots, y_r, z_1, \dots, z_s) \in B_{r,s}(t)$.

Note that $N(\alpha) = y_1 \dots y_r z_1 \overline{z_1} \dots z_s \overline{z_s} = \prod y_i \prod |z_j|^2$. Since the geometric mean is at most the arithmetic mean, taking nth roots we obtain $|N(\alpha)|^{\frac{1}{n}} \leq \frac{1}{n}\left(\sum |y_i| + 2\sum |z_j|\right) \leq \frac{t}{n}$ as $\sigma(\alpha) \in B_{r,s}(t)$. So $|N(\alpha)| \leq \frac{t^n}{n^n} = C_L N(\mathfrak{a})$ as required. □

To show that the volume of $B_{r,s}(t)$ is $2^r\left(\frac{\pi}{2}\right)^2\frac{t^n}{n!}$, we can use induction with base cases $B_{1,0}(t) = [-t, t]$ and $B_{0,1}(t) = \frac{\pi}{4}t^2$. Given the result for $B_{r,s}(t)$, the volume of $B_{r+1,s}(t)$ is

$$\int_{-t}^{t} \operatorname{vol} B_{r,s}(t - |y|)\,\mathrm{d}y = 2\int_0^t \left(\frac{\pi}{2}\right)^s 2^r \frac{(ty)^n}{n!}\,\mathrm{d}y = 2^{r+1}\left(\frac{\pi}{2}\right)^2 \frac{t^{n+1}}{n!}$$

The other inductive step is on an example sheet.

Corollary. Every element of the class group $[\mathfrak{a}]$ has a representative $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ with norm at most C_L.

Theorem. The class group of L is finite, and generated by prime ideals $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ with $N(\mathfrak{a}) \leq C_L$.

Proof. Follows the argument used for imaginary quadratic fields. □

Theorem (Hermite, Minkowski). Let $n \geq 2$. Then $|D_L| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$. In particular, $|D_L| > 1$, so at least one prime ramifies in L.

Proof. Apply this to $[\mathcal{O}_L]$ and obtain an ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ with $1 \leq N(\mathfrak{a}) \leq C_L$, so $C_L \geq 1$. So

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

as $\frac{\pi}{4} < 1$ and $s \leq \frac{n}{2}$. So $a_2 = \frac{\pi^2}{4}$ and $\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} > \frac{\pi}{4}(1 + 2) = \frac{3\pi}{4}$. So $a_n \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$. □

4 Dirichlet's unit theorem

4.1 Real quadratic fields

Recall that $\alpha \in \mathcal{O}_L$ is a unit if and only if $N(\alpha) = \pm 1$. We aim to show that $\mathcal{O}_L^\star \simeq \boldsymbol{\mu}_L \times \mathbb{Z}^{r+s-1}$ where $\boldsymbol{\mu}_L = \{\alpha \in L \mid \alpha^a = 1 \text{ for some } a > 0\}$ is the set of roots of unity in L, a finite cyclic group.

Example. Let $L = \mathbb{Q}(\sqrt{d})$ where $d > 0$ is square-free. Here, $r = 2, s = 0, n = 2$. $L \subseteq \mathbb{R}$ gives $\boldsymbol{\mu}_L \subseteq \{\pm 1\}$ so $\boldsymbol{\mu}_L = \{\pm 1\}$. Note that $N(x + y\sqrt{d}) = x^2 - dy^2$, so Dirichlet's theorem implies the following statement, which we will now prove directly.

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

Proof. Recall that we have $\sigma : \mathcal{O}_L \to \mathbb{R}^2$ given by $x + y\sqrt{d} \mapsto (x + y\sqrt{d}, x - y\sqrt{d})$. For example, if $d = 2$, the image is a lattice with basis $(1, 1), (-\sqrt{2}, \sqrt{2})$, note also that no point lies in the coordinate axes apart from 0. The covolume of $\sigma(\mathcal{O}_L)$ is $|D_L|^{\frac{1}{2}}$.

Consider

$$S_t = \left\{ (y_1, y_2) \in \mathbb{R}^2 \;\middle|\; |y_1| \leq t, |y_2| \leq \frac{|D_L|^{\frac{1}{2}}}{t} \right\}$$

The volume of S_t is $4|D_L|^{\frac{1}{2}} = 2^n \operatorname{covol}(\sigma(\mathcal{O}_L))$ as $n = 2$. Minkowski's lemma implies that there exists a nonzero $\alpha \in \mathcal{O}_L$ with $\sigma(\alpha) \in S_t$. But $\sigma(\alpha) = (y_1, y_2)$ gives $N(\alpha) = y_1 y_2$.

We have therefore found an element $\alpha \in \mathcal{O}_L$ with $\sigma(\alpha) \in S_t$ that has norm satisfying $1 \leq n(\alpha) \leq |D_L|^{\frac{1}{2}}$. We show that there exist infinitely many such α for $0 < t < 1$, so there are infinitely many $\alpha \in \mathcal{O}_L$ with $|N(\alpha)| = N((\alpha)) < |D_L|^{\frac{1}{2}}$. For fixed t, $S_t \cap \sigma(\mathcal{O}_L)$ is finite as S_t is compact. Given $t_1 > t_2 > \dots > t_n$, choose t_{n+1} less than all y_1 where $\sigma(\alpha) = (y_1, y_2) \in S_{t_n} \cap \sigma(\mathcal{O}_L)$. Note that $\alpha \neq 0$ so $\sigma_1(\alpha) \neq 0$, so $t_{n+1} > 0$.

Hence, there exists $m \in \mathbb{Z}$ with $1 \leq |m| \leq |D_L|^{\frac{1}{2}}$ for which there are infinitely many α with $N(\alpha) = m$, by the pigeonhole principle. But ideals $\mathfrak{a} \trianglelefteq \mathcal{O}_L$ with $m \in \mathfrak{a}$ biject with ideals in ${}^{\mathcal{O}_L}\!/\!_{m} = \left({}^{\mathbb{Z}}\!/\!_{m\mathbb{Z}}\right)^2$, and hence there are finitely many of them. Again by the pigeonhole principle, there exists $\beta \in \mathcal{O}_L$ and infinitely many $\alpha \in \mathcal{O}_L$ with $N(\beta) = N(\alpha) = m$, where $(\beta) = (\alpha)$. But $\frac{\beta}{\alpha}$ is a unit, so there are infinitely many units. □

We can prove Dirichlet's unit theorem for real quadratic fields from this result.

Corollary. $\mathcal{O}_L^\star = \{\pm \varepsilon_0^n \mid n \in \mathbb{Z}\}$ for $\varepsilon_0 \in \mathcal{O}_L^\star$.

Such an ε_0 is called a *fundamental unit.*

Remark. As there are infinitely many units, there exists $\varepsilon \in \mathcal{O}_L^\star$ with $\varepsilon \neq \pm 1$. Hence, $|\sigma_1(\varepsilon)| \neq \pm 1$ as $\sigma_1(\varepsilon) = \pm 1$ if and only if $\varepsilon = \pm 1$. Replacing ε by ε^{-1} if necessary, we can assume $E = |\sigma_1(\varepsilon)| > 1$. Consider $\{\alpha \in \mathcal{O}_L \mid N(\alpha) = \pm 1, 1 \leq |\sigma_1(\alpha)| \leq E\}$, which is a finite set as $\mathcal{O}_L$ is discrete in $\mathbb{R}^2$. Hence, ε_0 can be chosen in this set with minimum $|\sigma_1(\varepsilon_0)|$ and $\varepsilon_0 \neq \pm 1$.

We claim that if $\varepsilon \in \mathcal{O}_L^\star$ has $\sigma_1(\varepsilon) > 0$, then $\varepsilon = \varepsilon_0^N$ for some $N \in \mathbb{Z}$. Indeed, we can write $\frac{\log \sigma_1(\varepsilon)}{\log \sigma_1(\varepsilon_0)} = N + \gamma$ where $N \in \mathbb{Z}, 0 \leq \gamma < 1$. Hence $\varepsilon\varepsilon_0^{-N} = \varepsilon_0^\gamma$, and if $\gamma \neq 0$, $|\varepsilon_0^\gamma| = |\varepsilon|^\gamma < |\varepsilon_0|$ contradicting the choice of ε_0 (taking σ_1 as necessary to simplify notation).

4.2 General case

We can prove Dirichlet's unit theorem in general.

Let L be a number field and let $[L:\mathbb{Q}]=n$ with $\sigma_1,\dots,\sigma_r : L\to\mathbb{R}$ real embeddings and $\sigma_{r+1},\dots,\sigma_{r+s},\overline{\sigma}_{r+1},\dots,\overline{\sigma}_{r+s} : L\to$ $\mathbb{C}$ complex embeddings, choosing some representative between $\sigma_{r+i},\overline{\sigma}_{r+i}$ arbitrarily. Define a map $\ell : \mathcal{O}_L^\star\to\mathbb{R}^{r+s}$ by

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

Lemma. (i) The image of ℓ is a discrete subgroup of $\mathbb{R}^{r+s}$.
(ii) The kernel of ℓ is $\boldsymbol{\mu}_L$, the roots of unity in L, which is a finite cyclic group.

Remark. ℓ is independent of the choice of representative $\sigma_{r+i},\overline{\sigma}_{r+i}$, as they have the same absolute value.

Proof. Part (i). $\log|ab|=\log|a|+\log|b|$, so ℓ is a group homomorphism. The image is therefore an additive subgroup of $\mathbb{R}^{r+s}$. For part (i), it suffices to show that $\operatorname{Im}\ell\cap[-A,A]^{r+s}$ is finite for all $A>0$. ℓ factorises as

$$\mathcal{O}_L^\star \xhookrightarrow{\sigma} (\mathbb{R}_{\neq 0})^r\times\mathbb{C}^s \xrightarrow{j} \mathbb{R}^{r+s}$$

where

$$j(y_1,\dots,y_r,z_1,\dots,z_s)=(\log|y_1|,\dots,\log|y_r|,2\log|z_1|,\dots,2\log|z_s|)$$

and

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

which is compact. As $\sigma(\mathcal{O}_L)$ is a lattice, $\sigma(\mathcal{O}_L^\star)\cap j^{-1}([-A,A]^{r+s})$ is finite. This gives (i), and also shows that $\ker j=\ker\ell$ is finite.

Part (ii). $\ker\ell$ is a group and finite, so every element has finite order. In particular, $\ker\ell\le\boldsymbol{\mu}_L$. But each root of unity lies in $\ker\ell$, so $\ker\ell=\boldsymbol{\mu}_L$. But $L\hookrightarrow\mathbb{C}$ by any embedding, so $\boldsymbol{\mu}_L$ is contained in the set of roots of unity in $\mathbb{C}$ of a fixed order, which is a cyclic group. Subgroups of cyclic groups are cyclic. □

Note that if $r>0$, $L\hookrightarrow\mathbb{R}$, so $\boldsymbol{\mu}_L=\{\pm1\}$.

Observe that $\operatorname{Im}\ell$ is contained in the set $\{(y_1,\dots,y_{r+s})\mid y_1+\dots+y_{r+s}=0\}$. Indeed, $\alpha\in\mathcal{O}_L^\star$ gives $N(\alpha)=\prod_{i=1}^r\sigma_i(\alpha)\prod_{i=1}^s\sigma_{r+i}(\alpha)\overline{\sigma}_{r+i}(\alpha)=\pm1$, so taking logarithms,

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

So $\operatorname{Im}\ell\subseteq\mathbb{R}^{r+s-1}$ is a discrete subgroup, hence isomorphic to $\mathbb{Z}^a$ for $a\le r+s-1$.

Theorem (Dirichlet's unit theorem). $\operatorname{Im}\ell\subseteq\mathbb{R}^{r+s-1}$ is a lattice; it is isomorphic to $\mathbb{Z}^{r+s-1}$.

We now prove this theorem.

Lemma. Let $1 \leq k \leq s$, and $\alpha \in \mathcal{O}_L$, $\alpha \neq 0$. Then there exists $\beta \in \mathcal{O}_L$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^s |D_L|^{\frac{1}{2}}$ and with $b_i < a_i$ for all $i \neq k$, where $\ell(\alpha) = (a_1, \dots, a_{r+s})$ and $\ell(\beta) = (b_1, \dots, b_{r+s})$.

Proof. Apply Minkowski's lemma. Let

$$S = \left\{ (y_1, \dots, y_r, z_r, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n \,\middle|\, |y_i| \leq c_i, \left|z_j\right|^2 \leq c_{r+j} \right\}$$

We have $\operatorname{vol}(S) = 2^r \pi^s c_1 \dots c_{r+s}$. This is convex and symmetric around zero. By choosing c_i such that $0 < c_i < e^{a_i}$ for $i \neq k$, and setting $c_k = \left(\frac{2}{\pi}\right)^s |D_L|^{\frac{1}{2}} c_1^{-1} \dots c_{k-1}^{-1} c_{k+1}^{-1} \dots c_{r+s}^{-1}$, Minkowski gives $\beta \in \sigma(\mathcal{O}_L) \cap S$. □

Fix some $1 \leq k \leq s$. Repeatedly applying this lemma, we can obtain a sequence $\alpha_1, \alpha_2, \dots \in \mathcal{O}_L$ such that $N(\alpha_j)$ is bounded, and for all $i \neq k$, the ith coordinate of $\ell(\alpha_1), \ell(\alpha_2), \dots$ is strictly decreasing. Hence, there exists $t < t'$ with $N(\alpha_t) = N(\alpha_{t'}) = m$ as there are only finitely many possible norms of the α_t, and $\alpha_t = \alpha_{t'}$ modulo ${}^{\mathcal{O}_L}\!/_{m}$ by the pigeonhole principle. Therefore $(\alpha_t) = (\alpha_{t'})$ as in the proof for real quadratic fields.

Let $u_k = \alpha_t \alpha_{t'}^{-1}$; this is a unit in $\mathcal{O}_L$ such that $\ell(u_k) = \ell(a_t) - \ell(a_{t'}) = (y_1, \dots, y_{r+s})$ has $y_i < 0$ if $i \neq k$. Note that as $\sum y_i = 0$, we have $y_k > 0$.

We now have units $u_1, \dots, u_{r+s}$ by performing this for each coordinate. We now show that $\ell(u_1), \dots, \ell(u_{r+s-1})$ are linearly independent, hence the rank of $\ell(\mathcal{O}_L^\star)$ is $r + s - 1$. Indeed, let A be the $(r+s) \times (r+s)$ matrix with jth row given by $\ell(u_j)$, and apply the following lemma.

Lemma. Let $A \in M_{m \times m}(\mathbb{R})$ be a matrix with $a_{ii} > 0$, $a_{ij} < 0$ for $i \neq j$, and $\sum_j a_{ij} \geq 0$ for all i. Then $\operatorname{rank} A \geq m - 1$.

Note that the assumptions of this lemma are satisfied for our choice of matrix A.

Proof. Let v_i be the ith column of A. We show that $v_1, \dots, v_{m-1}$ are linearly independent. Suppose that there exist $t_i \in \mathbb{R}$ with $\sum_{i=1}^{m-1} t_i v_i = 0$, and not all t_i are zero. Choose k such that t_k has maximum absolute value. Dividing the linear dependence relation by t_k, we can assume $t_k = 1$ and all other t_i have absolute value at most 1. Now consider the kth entry of the linear dependence relation.

$$0 = \sum_{i=1}^{m-1} t_i a_{ki} = t_k a_{kk} + \sum_{i \neq k, 1 \leq i \leq m-1} t_i a_{ki}$$

Since $t_i \leq 1, a_{ki} < 0$, we have

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

as $a_{km} < 0$, giving a contradiction as required. □

This proves Dirichlet's unit theorem.

Definition. Let $R_L = \mathrm{covol}(\ell(\mathcal{O}_L^\star) \subseteq \mathbb{R}^{r+s-1})$. This is an invariant of a number field, called the *regulator* of L.

Concretely, choose $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ in $\mathcal{O}_L^\star$ such that $\mathcal{O}_L^\star \simeq \boldsymbol{\mu}_L \times \{\varepsilon_1^{n_1} \dots \varepsilon_{r+s-1}^{n_{r+s-1}} \mid n_i \in \mathbb{Z}\}$. Take any $(r+s-1) \times (r+s-1)$ minor of the $(r+s-1) \times (r+s)$ matrix $(\ell(\varepsilon_1), \dots, \ell(\varepsilon_{r+s}))$. The determinant of the absolute value of this submatrix is R_L.

Example. Let L be a real quadratic field, and let ε be a fundamental unit. Then $\log|\sigma_1(\varepsilon)| = R_L$.

4.3 Finding fundamental units

We now need to find such fundamental units. One way is to guess a unit and then find all smaller ones.

Example. Let $L = \mathbb{Q}(\sqrt{d})$ and $d > 0$, and embed this into $\mathbb{R}$ by choosing $\sqrt{d} > 0$. Consider $d = 2$. One might guess $\varepsilon = 1 + \sqrt{2}$, as $N(\varepsilon) = 1$ so ε is a unit. We claim that this is fundamental. If not, there exists $u = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$, $u \in \mathcal{O}_L^\star$, and $1 < u < \varepsilon$ as elements of $\mathbb{R}$, identifying L with $\sigma_1(L) \subseteq \mathbb{R}$. The other embedding $\overline{u} = a - b\sqrt{2}$ has $u\overline{u} = \pm 1$. As $u > 1$, $|\overline{u}| < 1$, so $u + \overline{u}, u - \overline{u} > 0$. Hence $a, b > 0$, so there are no possibilities for $1 < a + b\sqrt{2} < 1 + 1\sqrt{2}$ with $a, b > 0$ integers. Hence ε is a fundamental unit.

Example. Consider $d = 11$. Let $\varepsilon = 10 - 3\sqrt{11}$ as $N(\varepsilon) = 1$. Notice that $\varepsilon \approx 0.5$. $\varepsilon^{-1} > 1$ and $\varepsilon^{-1} < 20$. If this were not fundamental, there exists $u = a + b\sqrt{11}$ with $1 < u < \varepsilon^{-1} = 10 + 3\sqrt{11} < 20$. We could check all cases like in the above example, but we can do better in this case. If $N(u) = -1$, we have $a^2 - 11b^2 = -1$, which has no solutions modulo 11 as -1 is not a square in $\mathbb{F}_{11}$. Hence $N(u) = 1$ so $\overline{u} = u^{-1}$, giving $\varepsilon^{-1} > u > 1$ implies $0 < \varepsilon < u^{-1} = \overline{u} < 1$, so $0 < a - b\sqrt{11} < 1$, so $-1 < -a + b\sqrt{11} < 0$. Combining with the previous inequality, $0 < 2b\sqrt{11} < 10 + 3\sqrt{11} < 7\sqrt{11}$ so $b = 1, 2, 3$. Now we can check that $1 + b^2 \cdot 11$ is not a square in $\mathbb{F}_{11}$ for $b = 1, 2, 3$ so there is no possible a. Hence ε is a fundamental unit.

Remark. There is an algorithm for $\mathbb{Q}(\sqrt{d})$ to compute fundamental units. Recall that any real number t can be written as

$$t = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} = [a_0, a_1, a_2, a_3, \dots]$$

where $a_0 = \lfloor t \rfloor$. t is a quadratic algebraic number, so $[\mathbb{Q}(t) : \mathbb{Q}] = 2$, if and only if the expansion of t as a continued fraction is periodic $t = [a_0, \overline{a_1, \dots, a_m}]$.

The following proposition is non-examinable (and should not be used in exams).

Proposition. Let $\sqrt{d} = [a_0, \overline{a_1, \dots, a_m}]$ and let $\frac{p}{q} = [a_0, \dots, a_{m-1}]$. Then $p + q\sqrt{d}$ is a unit in $L = \mathbb{Q}(\sqrt{d})$, and if $d \equiv 2, 3 \bmod 4$, it is fundamental.

The proof is omitted.

Example. $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$ so $\frac{p}{q} = [2, 1, 1, 1] = \frac{8}{3}$ and $(8 + 3\sqrt{7})(8 - 3\sqrt{7}) = 1$.

This algorithm is polynomial-time in the regulator, but not polynomial-time in the discriminant.

If $q(x,y) = ax^2 + bxy + cy^2$ is a quadratic form for $a,b,c \in \mathbb{Z}$ and $D = b^2 - 4ac$, define $L = \mathbb{Q}(\sqrt{D})$, and define the ideal associated to q to be $\left(a, \frac{-b+\sqrt{D}}{2}\right)$. One can show that if $a > 0, D < 0$, the ideal attached to q is equal to the ideal attached to q' in the class group if and only q and q' are equal under the action of $SL_2(\mathbb{Z})$, i.e. if $q'(x,y) = q(x',y')$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \underbrace{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}}_{\in SL_2(\mathbb{Z})} \begin{pmatrix} x \\ y \end{pmatrix}$$

In particular, the size of the class group is exactly the number of orbits of positive definite quadratic forms with discriminant D under the action of $SL_2(\mathbb{Z})$.

5 Dirichlet series and L-functions

5.1 Dirichlet series

Theorem (Euclid). There exist infinitely many primes.

The following proof is due to Euler in 1748.

Proof. Consider

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \text{ prime}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) = \sum_{n=1}^{\infty} \frac{1}{n}$$

as every $n > 0$ factors uniquely as a product of primes so occurs exactly once when we expand the product. If there are finitely many primes, the product is finite. As $\sum_{i=1}^{\infty} p^{-i}$ converges to $\left(1 - \frac{1}{p}\right)^{-1}$, $\sum_{i=1}^{\infty} \frac{1}{n}$ must converge. □

We aim to prove that for all $a, q \in \mathbb{Z}$ coprime, there are infinitely many primes of the form $a + kq$, $k \in \mathbb{N}$. Note that there is no nice series expansion for $\prod_{p \equiv a \bmod q, p \text{ prime}} \left(1 - \frac{1}{p}\right)^{-1}$, so Euler's proof does not generalise.

Definition. The *Riemann zeta function* is $\zeta(s) = \sum_{n \geq 1} n^{-s}$ for $s \in \mathbb{C}$.

Proposition. (i) $\zeta(s)$ converges for $\operatorname{Re}(s) > 1$.

(ii) $\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$ in this region; this result is known as the *Euler product*. This product converges absolutely.

(iii) $\zeta(s) - \frac{1}{s-1}$ extends to a holomorphic function for $\operatorname{Re}(s) > 0$, so the zeta function has a simple pole with residue 1 at $s = 1$.

If the series $\sum \log(1 - a_n)$ converges, $\prod(1 - a_n)$ converges. $\prod(1 - a_n)$ absolutely converges if $\sum |\log(1 - a_n)|$ converges.

If a_n is a sequence of complex numbers, call the function $\sum_{n\geq 1} a_n n^{-s}$ a *Dirichlet series*. Instead of part (i), we will prove the following more general lemma.

> **Lemma.** If there exists $r \in \mathbb{R}$ with $a_1 + \dots + a_N = O(N^r)$, then $\sum_{n\geq 1} a_n n^{-s}$ converges for $\operatorname{Re}(s) > r$, and it is holomorphic in this region.

Proof of lemma.

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

where $R_n = \frac{T(N)}{N^s}$ with $T(N) = a_1 + \dots + a_N = O(N^r)$. By assumption, if $\operatorname{Re}(s) > r$,

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

as $x^s = e^{s\log x}$ so $|x^s| = |x^{\operatorname{Re} s}|$. So if $\operatorname{Re}(s) > r$, $\sum a_n n^{-s} = \sum T(N)(N^{-s} - (N+1)^{-s})$. But $|T(N)| \leq BN^r$ for some constant B by assumption, so it suffices to show $\sum N^r(N^{-s} - (N+1)^{-s})$ converges. Note that

$$N^{-s} - (N+1)^{-s} = \int_N^{N+1} s\frac{\mathrm{d}x}{x^{s+1}}$$

and $N^r \leq x^r$ if $x \in [N, N+1]$. Hence

$$N^r(N^{-s} - (N+1)^{-s}) \leq \int_N^{N+1} x^r s\frac{\mathrm{d}x}{x^{s+1}} \leq s\int_N^{N+1} \frac{\mathrm{d}x}{x^{s+1-r}}$$

It is enough to show that $s\int_1^N \frac{\mathrm{d}x}{x^{s+1-r}}$ converges, which it does to $\frac{s}{s-r}$. □

Proof of proposition. Part (ii). Let $p_1, \dots, p_r$ be the first r primes. Then, $\prod_{i=1}^{r}(1 - p_r^{-s})^{-1} = \sum_{n\in X} n^{-s}$ where X is the set of positive integers whose prime divisors are only in $p_1, \dots, p_r$. So

$$\left|\zeta(s) - \prod_{i=1}^{r}(1 - p_r^{-s})^{-1}\right| = \left|\sum_{n\notin X} n^{-s}\right| \leq \sum_{n\notin X} |n^{-s}| = \sum_{n\notin X} n^{-\operatorname{Re}(s)} \leq \sum_{n>r} n^{-\operatorname{Re}(s)}$$

as $1, \dots, r \in X$. Hence the infinite product converges to $\zeta(s)$. The proof of absolute convergence is omitted.

Part (iii). Left as an exercise, noting that

$$\frac{1}{s-1} = \sum_{i=1}^{\infty} \int_n^{n+1} \frac{\mathrm{d}t}{t^s}$$

□

5.2 Zeta functions in number fields

The remaining new content in this course is nonexaminable.

Definition. Let L be a number field. The *zeta function of L* is

$$\zeta_L(s) = \sum_{\mathfrak{a} \trianglelefteq \mathcal{O}_L} N(\mathfrak{a})^{-s} = \sum_{n \geq 1} \#\{\mathfrak{a} \trianglelefteq \mathcal{O}_L \mid N(\mathfrak{a}) = n\} n^{-s}$$

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

(ii) $\zeta_L(s) = \prod_{\mathfrak{p} \text{ prime ideal}} (1 - N(\mathfrak{p})^{-s})^{-1}$ in this region.

(iii) $\zeta_L(s)$ is a meromorphic function for $\mathrm{Re}(s) > 1 - \frac{1}{[L:\mathbb{Q}]}$, with a simple pole at $s = 1$ with residue

$$\frac{|\mathrm{Cl}_L| 2^{r+s} \pi^s R_L}{|D_L|^{\frac{1}{2}} |\boldsymbol{\mu}_L|}$$

This is called the *analytic class number formula*.

Proof. Part (ii) is clear. Parts (i) and (iii) follow from the following estimate. Writing $\zeta_L(s) = \sum \frac{a_n}{n^s}$ where a_n is the number of ideals of norm n, one can show

$$a_1 + \cdots + a_N = \frac{|\mathrm{Cl}_L| 2^{r+s} \pi^s R_L}{|D_L|^{\frac{1}{2}} |\boldsymbol{\mu}_L|} \cdot N + O\left(N^{1 - \frac{1}{[L:\mathbb{Q}]}}\right)$$

□

If $L \neq \mathbb{Q}$, it turns out that $\zeta_L(s)$ factors into $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ and some other factors. Suppose $L = \mathbb{Q}(\sqrt{d})$ and $d \neq 0, 1$ is square-free.

$$\zeta_L - \prod_{\mathfrak{p} \text{ prime ideal}} (1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{p \text{ prime}} \prod_{\mathfrak{p} | (p)} (1 - N(\mathfrak{p})^{-s})^{-1}$$

If $p \mid D_L$, then $(p) = \mathfrak{p}^2$ ramifies. In this case, $N(\mathfrak{p}) = p$ and we have a term $(1 - p^{-s})$ in the product. If (p) remains prime in L, then $N(\mathfrak{p}) = p^2$ giving the term $(1 - p^{-2s}) = (1 - p^{-s})(1 - p^s)$. If $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ splits, then $N(\mathfrak{p}_i) = p$ and we have a term $(1 - p^{-s})^2$. Let

$$\chi_{D_L}(p) = \chi(p) = \begin{cases} 0 & p \text{ ramifies} \\ -1 & p \text{ inert} \\ 1 & p \text{ splits} \end{cases} = \underbrace{\left(\frac{D_L}{p}\right)}_{\text{if } p \text{ odd}}$$

Then, defining $L(\chi, s) = \prod_{p \text{ prime}} 1 - \chi(p) p^{-s^{-1}}$, we have $\zeta_L(s) = \zeta_{\mathbb{Q}}(s) L(\chi, s)$. The function L is called a *Dirichlet L-function*. When expanding the infinite product defining $L(\chi_D, s)$ the coefficient of n^{-s}, if $n = p_1^{e_1} \dots p_r^{e_r}$ is $\chi_D(p_1)^{e_1} \dots \chi_D(p_r)^{e_r}$. We can extend the definition of χ to make it multiplicative: $\chi_D(p_1^{e_1} \dots p_r^{e_r}) = \chi_D(p_1)^{e_1} \dots \chi_D(p_r)^{e_r}$.

Example. Let $L = \mathbb{Q}(\sqrt{-1})$, so $D_L = 4$. We have $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ for $p \neq 2$. 2 ramifies, so $\chi_D(2) = 0$. We claim that

$$\chi_{-4}(m) = \begin{cases} (-1)^{\frac{m-1}{2}} & m \text{ odd} \\ 0 & m \text{ even} \end{cases}$$

Indeed, if n is even, this is clear; otherwise, this claim is that $(-1)^{\frac{mn-1}{2}} = (-1)^{\frac{m-1}{2}}(-1)^{\frac{n-1}{2}}$, which is easy to verify. Hence,

$$L(\chi_{-4}, s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots$$

In this example, the coefficients are periodic mod 4; this is true for general $L(\chi_D, s)$. Since $\zeta_L(s) = \zeta_{\mathbb{Q}}(s)L(\chi_{-4}, s)$, the fact that $\zeta_{\mathbb{Q}}(s)$ has a simple pole at $s = 1$ with residue 1, together with the analytic class number formula, gives $L(\chi_{-4}, 1) = \frac{\pi}{4}$.

Definition. $\chi : \mathbb{Z} \to \mathbb{C}$ is a *Dirichlet character* of modulus D if there exists a group homomorphism $\omega : \left({}^{\mathbb{Z}}\!/\!_{D\mathbb{Z}}\right)^\star \to \mathbb{C}$ such that

$$\chi(n) = \begin{cases} \omega(n \bmod D) & n \text{ invertible mod } D \\ 0 & \text{otherwise} \end{cases}$$

For such a χ, we have $\chi(n)\chi(m) = \chi(nm)$, and we can define

$$L(\chi, s) = \prod_{p \text{ prime}} (1 - \chi(p)p^{-s})^{-1} = \sum_{n \geq 1} \chi(n)n^{-s}$$

The previous example shows that χ_{-4} is a Dirichlet character of modulus 4.

Theorem. For any $d \neq 0, 1$ square-free, defining $L = \mathbb{Q}(\sqrt{d}), D = D_L$, we have that χ_D is a Dirichlet character of modulus D.

Proof. We must show $\chi_D(n + D) = \chi_D(n)$ for $n \in \mathbb{N}$. Suppose first that $d \equiv 3 \bmod 4$. Here, $D = 4d$, so $\chi_D(2) = 0$ as 2 ramifies, so $\chi_D(n) = 0$ if n is even as required. For $p > 2$, $\chi_D(p) = \left(\frac{D}{p}\right) = \left(\frac{d}{p}\right)$ by definition, but this is equal to $\left(\frac{p}{d}\right)(-1)^{\frac{p-1}{2}}$ by quadratic reciprocity as p, d are odd, and as $d \equiv 3$ mod 4, $\frac{d-1}{2} \equiv 1 \bmod 4$. $n \mapsto (-1)^{\frac{n-1}{2}}$ is multiplicative, so $\chi_D(n + D) = \left(\frac{n+D}{d}\right)(-1)^{\frac{n-1}{2}}(-1)^{4d}2 = \chi_D(n)$. The other cases are omitted. □

This theorem can be seen as equivalent to the law of quadratic reciprocity. Note that χ is nontrivial if $\omega \not\equiv 1$

Lemma. If χ is a nontrivial Dirichlet character, $L(\chi, s)$ is holomorphic for $\operatorname{Re} s > 0$.

Proof. Recall that if G is a finite group and χ_1, χ_2 are characters of irreducible complex representations, then

$$\frac{1}{G} \sum_{g \in G} \overline{\chi_1(g)}\chi_2(g) = \begin{cases} 1 & \chi_1 = \chi_2 \\ 0 & \text{otherwise} \end{cases}$$

Applying this to $G = \left({}^{\mathbb{Z}}\!/\!_{d\mathbb{Z}}\right)^\star$ where χ_1 is the trivial character and $\chi_2 = \omega$, this gives

$$\sum_{ad < i < (a+1)d} \chi(i) = \sum_{i \in {}^{\mathbb{Z}}\!/\!_{d\mathbb{Z}}} \chi(i) = \sum_{i \in \left({}^{\mathbb{Z}}\!/\!_{d\mathbb{Z}}\right)^\star} \omega(i) = 0$$

In particular, $\sum_{i=1}^{n}\chi(i) = O(1)$ is bounded. So $\sum_{i=1}^{n}\frac{\chi(i)}{n^s}$ converges for $\mathrm{Re}(s) > 0$. □

Corollary. If $D < 0$,

$$L(\chi_D, 1) = \frac{2\pi\left|\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}\right|}{|D|^{\frac{1}{2}}\left|\boldsymbol{\mu}_{\mathbb{Q}(\sqrt{D})}\right|}$$

In particular, $L(\chi_D, 1) \neq 0$.

Proof. $\zeta_{\mathbb{Q}(\sqrt{(D)})}(s) = \zeta_{\mathbb{Q}}(s)L(\chi_D, s)$, so both sides have a simple pole at $s = 1$. The analytic class number formula gives the residue of the left hand side, and $\mathrm{Res}_{\zeta}(1) = 1$. □

5.3 L-functions in cyclotomic fields

We will show that $L(\chi, 1) \neq 0$ for any Dirichlet character χ, and hence show that there are infinitely many primes in arithmetic progression. To do this, we will factor $\zeta_{\mathbb{Q}(e^{\frac{2\pi i}{q}})}$ for any q. Consider $L = \mathbb{Q}(\omega_q)$ where ω_q is a primitive qth root of unity,

Proposition. (i) $[L : \mathbb{Q}] = \varphi(q)$ where $\varphi(q) = \left|\left(\mathbb{Z}/q\mathbb{Z}\right)^\star\right|$;

(ii) $L/\mathbb{Q}$ is a Galois extension with Galois group $G = \left(\mathbb{Z}/q\mathbb{Z}\right)^\star$, and if $r \in \left(\mathbb{Z}/q\mathbb{Z}\right)^\star$, then r acts on L by mapping ω_q to ω_q^r;

(iii) $\mathcal{O}_L = \mathbb{Z}[\omega_q] = \mathbb{Z}[x]/\Phi_q(x)$ where Φ_q is the qth cyclotomic polynomial;

(iv) if p is prime, $p \mid D_L$ if and only if $p \mid q$;

(v) if p is prime, p ramifies in $\mathcal{O}_L$ if and only if $p \mid q$;

(vi) if p is prime with $p \nmid q$, then (p) factors as a product of $\frac{\varphi(q)}{f}$ distinct prime ideals, each of norm p^f, where f is the order of p in $\left(\mathbb{Z}/q\mathbb{Z}\right)^\star$.

Proof. Parts (i) and (ii) follow from Galois theory. Part (iii) for q prime is on an example sheet, and the general case is omitted. Part (iv) is omitted. Part (iv) implies (v) is a general fact; we will only show part (vi).

As $\mathcal{O}_L = \mathbb{Z}[x]/\Phi_q(x)$, Dedekind's theorem applies. We study $\mathcal{O}_L/(p) = \mathbb{F}_p[x]/\Phi_q(x)$ by factoring $\Phi_q(x)$ modulo p. Recall that

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

so for instance $\Phi_8(x) = \frac{x^8-1}{x^4-1} = x^4 + 1$.

$$\left(\mathbb{Z}/8\mathbb{Z}\right)^\star = \{1, 3, -3, -1\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

In this example, if $p = 17$, $x^4 + 1$ factors into four linear factors, but if $p = 3$, $x^4 + 1$ factors into two factors as the order of 3 is 2 in $\left(\mathbb{Z}/8\mathbb{Z}\right)^\star$.

Write $\Phi_q(x) = \gamma_1^{e_1} \dots \gamma_g^{e_g}$ for γ_i irreducible and distinct, so

$$\mathcal{O}_L/_{(p)} = \mathbb{F}_p[x]/_{(\gamma_1^{e_1})} \times \dots \mathbb{F}_p[x]/_{(\gamma_g^{e_g})}$$

For any number field L, $\operatorname{Gal}(L/\mathbb{Q})$ preserves $\mathcal{O}_L$. Indeed, if $\alpha \in \mathcal{O}_L$, $f(\alpha) = 0$ for some monic polynomial $f \in \mathbb{Z}[x]$, but then $g \in \operatorname{Gal}(L/\mathbb{Q})$ givesn $0 = gf(\alpha) = f(g(\alpha)) = 0$, so $g(\alpha)$ is also a root of f and hence in $\mathcal{O}_L$.

G permutes the roots of Φ_q, so G acts on $\{\gamma_1, \dots, \gamma_g\}$. This action is transitive on the roots, so is transitive on $\{\gamma_1, \dots, \gamma_g\}$. Hence $\deg \gamma_1 = \dots = \deg \gamma_g$, so $e_1 = \dots = e_g = e$. Further, ge is the order of $G/_{\operatorname{Stab}_G(\gamma_1)}$.

If $p \nmid D_L$, or equivalently $p \nmid q$, then $e = 1$ as p is unramified. Hence $\mathbb{F}_p[x]/_{(\gamma_1)} = \mathbb{F}_{p^{f'}}$ for some f', and $\frac{\varphi(q)}{f'}$ factors. We must show that $f' = f$.

$p \in \left(\mathbb{Z}/_{q\mathbb{Z}}\right)^\star = \operatorname{Gal}(L/\mathbb{Q})$ acts as $\alpha \mapsto \alpha^p$ on $\mathbb{F}_{p^{f'}}$, so it acts as the Frobenius automorphism, which is the generator of the Galois group of $\mathbb{F}_{p^{f'}}/_{\mathbb{F}_p}$ by (ii). Conversely, the image of x in $\mathbb{F}_p[x]/_{(\gamma_1)}$, is the image of ω_q which is a primitive qth root of unity. So $q \mid \left|\mathbb{F}_{p^{f'}}^\star\right|$, so $q \mid p^{f'} - 1$. In particular, $p^{f'} \equiv 1 \mod q$, so $f = \operatorname{ord}(p) \mid f'$. Hence $f = f'$ as required. □

Recall that $\zeta_{\mathbb{Q}(\omega_q)}(s) = \prod_{\mathfrak{p} \text{ prime}}(1 - N(\mathfrak{p})^{-s})^{-1}$. Consider prime ideals $\mathfrak{p}$ dividing (p) for a fixed integer prime p. If $p \nmid q$, part (vi) shows that these contribute $(1 - p^{-fs})^{-\frac{\varphi(q)}{f}}$ to the zeta function, where f is the order of p in $\left(\mathbb{Z}/_{q\mathbb{Z}}\right)^\star$. But this factors as $(1 - t^f) = \prod_{\gamma \in \mu_f}(1 - \gamma t)$ where $\mu_f = \{\gamma \in \mathbb{C} \mid \gamma^f = 1\}$.

Set $t = p^{-s}$, and let $\omega_1, \dots, \omega_{\varphi(q)} : \left(\mathbb{Z}/_{q\mathbb{Z}}\right)^\star \to \mathbb{C}$ be the distinct irreducible complex representations of $\left(\mathbb{Z}/_{q\mathbb{Z}}\right)^\star$, such that $\omega_1 = \mathbb{1}$ so $\omega_1(\alpha) = 1$ for all $\alpha \in \left(\mathbb{Z}/_{q\mathbb{Z}}\right)^\star$. We claim that $\omega_1(p), \dots, \omega_{\varphi(q)}(p)$ are the distinct fth roots of unity, each repeated $\frac{\varphi(q)}{f}$ times. Certainly p generates a cyclic subgroup (p) of $\left(\mathbb{Z}/_{q\mathbb{Z}}\right)^\star$ of order f by definition of f. The claim is that the restriction of of $\omega_1, \dots, \omega_{\varphi(q)}$ to (p) are the f distinct irreducible representations of (p), each repeated $\frac{\varphi(q)}{f}$ times, which can be easily proven using representation theory. We have therefore shown that

$$(1 - p^{-fs})^{-\frac{\varphi(q)}{f}} = \prod_{i=1}^{\varphi(q)} (1 - \omega_i(p) p^{-s})^{-1}$$

Let

$$\chi_i(n) = \begin{cases} \omega_i(n \bmod q) & \text{if } \gcd(n, q) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then we have shown that

$$\zeta_{\mathbb{Q}(\omega_q)}(s) = \prod_{i=1}^{\varphi(q)} L(\chi_i, s) \text{ multiplied by a correction term}$$

which is a finite product of the form $\prod_{p|q}(1-p^{-f_p s})^{-1}$. Note that $\zeta_{\mathbb{Q}}(s) = L(\chi_1, s)\prod_{p|q}(1-p^{-s})^{-1}$, so we can rewrite this as

$$\zeta_{\mathbb{Q}(\omega_p)}(s) = \zeta_{\mathbb{Q}}(s)\prod_{i=2}^{\varphi(q)} L(\chi_i, s) \text{ multiplied by a correction term}$$

Theorem. If χ_i is a nontrivial Dirichlet character, then $L(\chi_i, 1) \neq 0$.

In fact, if χ is any nontrivial Dirichlet character modulo q, $\chi = \chi_i$ for some i.

Proof. We have shown that if χ is a nontrivial Dirichlet character, $L(\chi, s)$ is holomorphic at $s = 1$. In the above expansion, the left hand side and right hand side are meromorphic functions at $s = 1$ with a simple pole. The residue of the right hand side and left hand side therefore agree, and its value is

$$\operatorname{Res}_{s=1}\zeta_{\mathbb{Q}}(s)\prod_{i=2}^{\varphi(q)} L(\chi_i, 1) \text{ multiplied by a correction term}$$

The analytic class number formula implies that this is nonzero, so $L(\chi_i, 1) \neq 0$. □

Note that Dirichlet characters of quadratic fields have values in ±1.

5.4 Primes in arithmetic progression

Theorem (Dirichlet). Let $a, q \in \mathbb{N}$ with $\gcd(a, q) = 1$. There are infinitely many primes in $a, a+q, a+2q, \dots$.

Proof. Consider $\left(\mathbb{Z}/q\mathbb{Z}\right)^\star$, an abelian group of order $\varphi(q)$. Let $\omega_1, \dots, \omega_{\varphi(q)} : \left(\mathbb{Z}/q\mathbb{Z}\right)^\star \to \mathbb{C}^\star$ where $\omega_1 = \mathbb{1}$, and $\chi_1, \dots, \chi_{\varphi(q)} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be the corresponding Dirichlet characters. Recall the orthogonality of the columns of the character table of a finite group:

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

if $\gcd(p, q) = 1$, so p defines an element of $\left(\mathbb{Z}/q\mathbb{Z}\right)^\star$. Hence,

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

even if $\gcd(p, q) \neq 1$, since in this case $\chi_i(p) = 0$ by definition. Hence,

$$\sum_{p \equiv a \bmod q, p \text{ prime}} p^{-s} = \frac{1}{\varphi(q)}\sum_{i,p}\overline{\chi_i(a)}\chi_i(p)p^{-s}$$

We want to show that this has a pole at $s = 1$. If χ is a Dirichlet character, by the series expansion of logarithm which is valid by absolute convergence, we can write

$$\begin{aligned}\log L(\chi, s) &= -\sum_p \log(1 - \chi(p)p^{-s}) \\ &= \sum_{n,p} \frac{\chi(p)^n}{p^{ns}n} \\ &= \sum_{n,p} \frac{\chi(p^n)}{p^{ns}n} \\ &= \sum_p \frac{\chi(p)}{p^s} + \sum_{n\geq 2,p} \frac{\chi(p^n)}{p^{ns}n}\end{aligned}$$

We claim that $\sum_{n\geq 2,p \text{ prime}} \frac{\chi(p^n)}{p^{ns}n}$ converges at $s = 1$. This holds as its absolute value is at most

$$\sum_{n\geq 2,p \text{ prime}} p^{-ns} = \sum_{p \text{ prime}} \frac{1}{p^s(p^s - 1)} \leq \sum_n \frac{1}{n^s(n^s - 1)} \leq 2\frac{1}{n^{2s}}$$

which is finite at $s = 1$. Hence, the series above has a pole at $s = 1$ if and only if

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

has a pole at $s = 1$.

If χ_1 is the trivial character, $L(\chi_1, s) = \zeta_{\mathbb{Q}}(s) \prod_{p|s}(1 - p^{-s})$, so as $\zeta_{\mathbb{Q}}(s)$ has only a simple pole at $s = 1$, $\log \zeta_{\mathbb{Q}}(s) = \log \frac{1}{s-1} +$ bounded function near $s = 1$, so $\log L(\chi_1, s) \sim \log \frac{1}{s-1}$ has a pole at $s = 1$. For $i \neq 1$, $L(\chi_i, s)$ is nonzero at $s = 1$ by the above theorem, so $\log L(\chi_i, s)$ is bounded at $s = 1$. Hence, $\frac{1}{\varphi(q)} \sum_{i,p} \overline{\chi_i(a)}\chi_i(p)p^{-s} \sim \frac{1}{\varphi(q)} \log \frac{1}{s-1}$, and in particular has a pole at $s = 1$.

Hence, there are infinitely many primes in arithmetic progression. □

This proof shows that approximately $\frac{1}{\varphi(q)}$ of all primes lie in this arithmetic progression.

One can in fact show that for any number field L, $\zeta_L(s)$ always factors and the factors have meaning. Suppose $L/\mathbb{Q}$ is Galois, and $G = \mathrm{Gal}(L/\mathbb{Q})$. Then,

(i) We can factor $\zeta_L(s) = \prod_{\rho \text{ irreducible representation of } G} L(\rho, s)^{\dim \rho}$, where the $L(\rho, s)$ are *Artin L-functions*. Moreover, $L/\mathbb{Q}$ is the regular representation of G.

(ii) $L(\mathbb{1}, s) = \zeta_{\mathbb{Q}}(s)$.

(iii) $L(\rho, s)$ is a meromorphic function of s. It is conjectured, but still not known, that $L(\rho, s)$ is holomorphic if $\rho \neq \mathbb{1}$.

(iv) If ρ is one-dimensional, then $L(\rho, s) = L(\chi, s)$ multiplied by a correction factor, where $L(\chi, s)$ is a Dirichlet L-function. Finding χ given ρ is a generalisation of quadratic reciprocity, called class field theory.

(v) The properties of mutidimensional ρ are studied in the Langlands programme.