Let K be a number field i.e. a finite field extension $\mathbb{Q}$. Set $n = [K : \mathbb{Q}]$, the degree of the field extension, i.e. $\dim_{\mathbb{Q}}(K)$.

For $\alpha \in K$ let $T_\alpha : K \to K$ be the $\mathbb{Q}$-linear transformation given by $T_\alpha(x) = \alpha x$. Then define

1. $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$, the trace of α, to be $\mathrm{tr}(T_\alpha)$;
2. $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, the norm of α, to be $\det(T_\alpha)$.

We will abbreviate $\mathrm{tr}_{K/\mathbb{Q}}$ and $\mathrm{N}_{K/\mathbb{Q}}$ to just tr and N when the extension $K/\mathbb{Q}$ is clear. For any $\alpha, \beta \in K$, we have

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + (\beta) \quad \text{and} \quad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

Let K be a number field i.e. a finite field extension $\mathbb{Q}$. Set $n = [K : \mathbb{Q}]$, the degree of the field extension, i.e. $\dim_{\mathbb{Q}}(K)$.
For $\alpha \in K$ let $T_\alpha : K \to K$ be the $\mathbb{Q}$-linear transformation given by $T_\alpha(x) = \alpha x$. Then define

1. $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$, the trace of α, to be $\mathrm{tr}(T_\alpha)$;
2. $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, the norm of α, to be $\det(T_\alpha)$.

We will abbreviate $\mathrm{tr}_{K/\mathbb{Q}}$ and $\mathrm{N}_{K/\mathbb{Q}}$ to just tr and N when the extension $K/\mathbb{Q}$ is clear. For any $\alpha, \beta \in K$, we have

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + (\beta) \quad \text{and} \quad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

- Let $c_\alpha \in \mathbb{Q}[x]$ be the characteristic polynomial of T_α. Thus $\deg c_\alpha = n$. If $\alpha_1, \ldots, \alpha_n$ are the roots of c_α in a splitting field then $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \ldots \alpha_n$.

Let K be a number field i.e. a finite field extension $\mathbb{Q}$. Set $n = [K : \mathbb{Q}]$, the degree of the field extension, i.e. $\dim_{\mathbb{Q}}(K)$.
For $\alpha \in K$ let $T_\alpha : K \to K$ be the $\mathbb{Q}$-linear transformation given by $T_\alpha(x) = \alpha x$. Then define

1. $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$, the trace of α, to be $\mathrm{tr}(T_\alpha)$;
2. $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, the norm of α, to be $\det(T_\alpha)$.

We will abbreviate $\mathrm{tr}_{K/\mathbb{Q}}$ and $\mathrm{N}_{K/\mathbb{Q}}$ to just tr and N when the extension $K/\mathbb{Q}$ is clear. For any $\alpha, \beta \in K$, we have

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + (\beta) \quad \text{and} \quad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

- Let $c_\alpha \in \mathbb{Q}[x]$ be the characteristic polynomial of T_α. Thus $\deg c_\alpha = n$. If $\alpha_1, \ldots, \alpha_n$ are the roots of c_α in a splitting field then $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \ldots \alpha_n$.
- $c_\alpha(\alpha) = 0$ shows α is an algebraic number.
- If $c_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ then $\mathrm{tr}(\alpha) = -a_{n-1}$ and $\mathrm{N}(\alpha) = (-1)^n a_0$. Note that both belong to $\mathbb{Q}$, which we already knew.

Let K be a number field i.e. a finite field extension $\mathbb{Q}$. Set $n = [K : \mathbb{Q}]$, the degree of the field extension, i.e. $\dim_{\mathbb{Q}}(K)$.
For $\alpha \in K$ let $T_\alpha : K \to K$ be the $\mathbb{Q}$-linear transformation given by $T_\alpha(x) = \alpha x$. Then define

1. $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$, the trace of α, to be $\mathrm{tr}(T_\alpha)$;
2. $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, the norm of α, to be $\det(T_\alpha)$.

We will abbreviate $\mathrm{tr}_{K/\mathbb{Q}}$ and $\mathrm{N}_{K/\mathbb{Q}}$ to just tr and N when the extension $K/\mathbb{Q}$ is clear. For any $\alpha, \beta \in K$, we have

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + (\beta) \quad \text{and} \quad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

- Let $c_\alpha \in \mathbb{Q}[x]$ be the characteristic polynomial of T_α. Thus $\deg c_\alpha = n$. If $\alpha_1, \ldots, \alpha_n$ are the roots of c_α in a splitting field then $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \ldots \alpha_n$.
- $c_\alpha(\alpha) = 0$ shows α is an algebraic number.
- If $c_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ then $\mathrm{tr}(\alpha) = -a_{n-1}$ and $\mathrm{N}(\alpha) = (-1)^n a_0$. Note that both belong to $\mathbb{Q}$, which we already knew.

Let K be a number field i.e. a finite field extension $\mathbb{Q}$. Set $n = [K : \mathbb{Q}]$, the degree of the field extension, i.e. $\dim_{\mathbb{Q}}(K)$.
For $\alpha \in K$ let $T_\alpha : K \to K$ be the $\mathbb{Q}$-linear transformation given by $T_\alpha(x) = \alpha x$. Then define

1. $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$, the trace of α, to be $\mathrm{tr}(T_\alpha)$;
2. $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, the norm of α, to be $\det(T_\alpha)$.

We will abbreviate $\mathrm{tr}_{K/\mathbb{Q}}$ and $\mathrm{N}_{K/\mathbb{Q}}$ to just tr and N when the extension $K/\mathbb{Q}$ is clear. For any $\alpha, \beta \in K$, we have

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + (\beta) \quad \text{and} \quad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

- Let $c_\alpha \in \mathbb{Q}[x]$ be the characteristic polynomial of T_α. Thus $\deg c_\alpha = n$. If $\alpha_1, \ldots, \alpha_n$ are the roots of c_α in a splitting field then $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \ldots \alpha_n$.
- $c_\alpha(\alpha) = 0$ shows α is an algebraic number.
- If $c_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ then $\mathrm{tr}(\alpha) = -a_{n-1}$ and $\mathrm{N}(\alpha) = (-1)^n a_0$. Note that both belong to $\mathbb{Q}$, which we already knew.

Let K be a number field i.e. a finite field extension $\mathbb{Q}$. Set $n = [K : \mathbb{Q}]$, the degree of the field extension, i.e. $\dim_{\mathbb{Q}}(K)$.
For $\alpha \in K$ let $T_\alpha : K \to K$ be the $\mathbb{Q}$-linear transformation given by $T_\alpha(x) = \alpha x$. Then define

1. $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$, the trace of α, to be $\mathrm{tr}(T_\alpha)$;
2. $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, the norm of α, to be $\det(T_\alpha)$.

We will abbreviate $\mathrm{tr}_{K/\mathbb{Q}}$ and $\mathrm{N}_{K/\mathbb{Q}}$ to just tr and N when the extension $K/\mathbb{Q}$ is clear. For any $\alpha, \beta \in K$, we have

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + (\beta) \quad \text{and} \quad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

- Let $c_\alpha \in \mathbb{Q}[x]$ be the characteristic polynomial of T_α. Thus $\deg c_\alpha = n$. If $\alpha_1, \ldots, \alpha_n$ are the roots of c_α in a splitting field then $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \ldots \alpha_n$.
- $c_\alpha(\alpha) = 0$ shows α is an algebraic number.
- If $c_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ then $\mathrm{tr}(\alpha) = -a_{n-1}$ and $\mathrm{N}(\alpha) = (-1)^n a_0$. Note that both belong to $\mathbb{Q}$, which we already knew.

- Let f_α be the *minimal polynomial* of α. Thus $f_\alpha \in \mathbb{Q}[x]$ is the unique monic polynomial of minimal positive degree which has α has a root. Now $g \in \mathbb{Q}[x]$, $g(\alpha) = 0 \iff f_\alpha \mid g$. Since $c_\alpha(\alpha) = 0$ we have $f_\alpha | c_\alpha$. But more is true!
- Let $d := \deg(f_\alpha)$. Then the number field $\mathbb{Q}(\alpha)$ has $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ as a basis and the characteristic polynomial of T_α restricted to $\mathbb{Q}(\alpha)$ is f_α. From $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$, one then deduces $c_\alpha = f_\alpha^{n/d}$.

Example

In $K = \mathbb{Q}(i)$, the minimal polynomial of $\alpha = 2 + i$ is $x^2 - 4x + 5$ which has roots $2 + i$ and $2 - i$. This gives

$$\mathrm{tr}_{K/\mathbb{Q}}(2 + i) = (2 + i) + (2 - i) = 4$$

and

$$\mathrm{N}_{K/\mathbb{Q}}(2 + i) = (2 + i)(2 - i) = 5.$$

- Let f_α be the *minimal polynomial* of α. Thus $f_\alpha \in \mathbb{Q}[x]$ is the unique monic polynomial of minimal positive degree which has α has a root. Now $g \in \mathbb{Q}[x]$, $g(\alpha) = 0 \iff f_\alpha \mid g$. Since $c_\alpha(\alpha) = 0$ we have $f_\alpha | c_\alpha$. But more is true!
- Let $d := \deg(f_\alpha)$. Then the number field $\mathbb{Q}(\alpha)$ has $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$ as a basis and the characteristic polynomial of T_α restricted to $\mathbb{Q}(\alpha)$ is f_α. From $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$, one then deduces $c_\alpha = f_\alpha^{n/d}$.

Example

In $K = \mathbb{Q}(i)$, the minimal polynomial of $\alpha = 2 + i$ is $x^2 - 4x + 5$ which has roots $2 + i$ and $2 - i$. This gives

$$\operatorname{tr}_{K/\mathbb{Q}}(2 + i) = (2 + i) + (2 - i) = 4$$

and

$$\mathrm{N}_{K/\mathbb{Q}}(2 + i) = (2 + i)(2 - i) = 5.$$

- Let f_α be the *minimal polynomial* of α. Thus $f_\alpha \in \mathbb{Q}[x]$ is the unique monic polynomial of minimal positive degree which has α has a root. Now $g \in \mathbb{Q}[x]$, $g(\alpha) = 0 \iff f_\alpha \mid g$. Since $c_\alpha(\alpha) = 0$ we have $f_\alpha | c_\alpha$. But more is true!
- Let $d := \deg(f_\alpha)$. Then the number field $\mathbb{Q}(\alpha)$ has $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ as a basis and the characteristic polynomial of T_α restricted to $\mathbb{Q}(\alpha)$ is f_α. From $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$, one then deduces $c_\alpha = f_\alpha^{n/d}$.

Example

In $K = \mathbb{Q}(i)$, the minimal polynomial of $\alpha = 2 + i$ is $x^2 - 4x + 5$ which has roots $2 + i$ and $2 - i$. This gives

$$\mathrm{tr}_{K/\mathbb{Q}}(2 + i) = (2 + i) + (2 - i) = 4$$

and

$$\mathrm{N}_{K/\mathbb{Q}}(2 + i) = (2 + i)(2 - i) = 5.$$

Let's get back to our number field K with $[K : \mathbb{Q}] = n$.

- By the theorem of the primitive element, we can find $\beta \in K$ such that $K = \mathbb{Q}(\beta)$. If f_β is the minimal polynomial of β then $\deg(f_\beta) = n$, $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ is a $\mathbb{Q}$-basis for K and $K = \mathbb{Q}[x]/f_\beta$.
- The polynomial f_β then has n distinct roots in $\mathbb{C}$, say $\beta_1, \ldots, \beta_n$.
- Then we get n embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq n$, determined by $\sigma_i(\beta) = \beta_i$. If r is the number of real roots and s is the number of pairs of complex conjugate roots then $r + 2s = n$.

Let's get back to our number field K with $[K : \mathbb{Q}] = n$.

- By the theorem of the primitive element, we can find $\beta \in K$ such that $K = \mathbb{Q}(\beta)$. If f_β is the minimal polynomial of β then $\deg(f_\beta) = n$, $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ is a $\mathbb{Q}$-basis for K and $K = \mathbb{Q}[x]/f_\beta$.
- The polynomial f_β then has n distinct roots in $\mathbb{C}$, say $\beta_1, \ldots, \beta_n$.
- Then we get n embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq n$, determined by $\sigma_i(\beta) = \beta_i$. If r is the number of real roots and s is the number of pairs of complex conjugate roots then $r + 2s = n$.
- For any $\alpha \in K$ we have

$$\mathrm{tr}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha),$$
$$\mathrm{N}(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha).$$

Let's get back to our number field K with $[K:\mathbb{Q}]=n$.

- By the theorem of the primitive element, we can find $\beta \in K$ such that $K=\mathbb{Q}(\beta)$. If f_β is the minimal polynomial of β then $\deg(f_\beta)=n$, $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$ is a $\mathbb{Q}$-basis for K and $K=\mathbb{Q}[x]/f_\beta$.
- The polynomial f_β then has n distinct roots in $\mathbb{C}$, say $\beta_1,\ldots,\beta_n$.
- Then we get n embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$, $1 \le i \le n$, determined by $\sigma_i(\beta)=\beta_i$. If r is the number of real roots and s is the number of pairs of complex conjugate roots then $r+2s=n$.
- For any $\alpha \in K$ we have

$$\begin{aligned}\mathrm{tr}(\alpha) &= \sigma_1(\alpha)+\ldots+\sigma_n(\alpha),\\ \mathrm{N}(\alpha) &= \sigma_1(\alpha)\ldots\sigma_n(\alpha).\end{aligned}$$

Let's get back to our number field K with $[K : \mathbb{Q}] = n$.

- By the theorem of the primitive element, we can find $\beta \in K$ such that $K = \mathbb{Q}(\beta)$. If f_β is the minimal polynomial of β then $\deg(f_\beta) = n$, $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ is a $\mathbb{Q}$-basis for K and $K = \mathbb{Q}[x]/f_\beta$.
- The polynomial f_β then has n distinct roots in $\mathbb{C}$, say $\beta_1, \ldots, \beta_n$.
- Then we get n embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq n$, determined by $\sigma_i(\beta) = \beta_i$. If r is the number of real roots and s is the number of pairs of complex conjugate roots then $r + 2s = n$.
- For any $\alpha \in K$ we have

$$\mathrm{tr}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha),$$
$$\mathrm{N}(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha).$$

Let's get back to our number field K with $[K:\mathbb{Q}]=n$.

- By the theorem of the primitive element, we can find $\beta \in K$ such that $K=\mathbb{Q}(\beta)$. If f_β is the minimal polynomial of β then $\deg(f_\beta)=n$, $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$ is a $\mathbb{Q}$-basis for K and $K=\mathbb{Q}[x]/f_\beta$.
- The polynomial f_β then has n distinct roots in $\mathbb{C}$, say $\beta_1,\ldots,\beta_n$.
- Then we get n embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$, $1 \le i \le n$, determined by $\sigma_i(\beta)=\beta_i$. If r is the number of real roots and s is the number of pairs of complex conjugate roots then $r+2s=n$.
- For any $\alpha \in K$ we have

$$\begin{aligned}\mathrm{tr}(\alpha) &= \sigma_1(\alpha)+\ldots+\sigma_n(\alpha),\\ \mathrm{N}(\alpha) &= \sigma_1(\alpha)\ldots\sigma_n(\alpha).\end{aligned}$$

Definition

Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be an n-tuple of elements of K, where $n = [K : \mathbb{Q}]$.

1. The **determinant** $\Delta(\omega) = \det(\sigma_i \omega_j)$.
2. The **discriminant** is $\Delta^2(\omega)$.

Lemma (1.1)

$\Delta^2(\omega) = \det(tr_{K/\mathbb{Q}}(\omega_i\omega_j))$, so $\Delta^2(\omega) \in \mathbb{Q}$.

Proof.

Let $A = (\sigma_i \omega_j)$. Then $\Delta^2(\omega) = \det(A^t A)$

$$= \det\left(\sum_k \sigma_k(\omega_i)\sigma_k(\omega_j)\right) = \det\left(\sum_k \sigma_k(\omega_i\omega_j)\right) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)).$$

□

Definition

Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be an n-tuple of elements of K, where $n = [K : \mathbb{Q}]$.

1. The **determinant** $\Delta(\omega) = \det(\sigma_i \omega_j)$.
2. The **discriminant** is $\Delta^2(\omega)$.

Lemma (1.1)

$\Delta^2(\omega) = \det(tr_{K/\mathbb{Q}}(\omega_i \omega_j))$, so $\Delta^2(\omega) \in \mathbb{Q}$.

Proof.

Let $A = (\sigma_i \omega_j)$. Then $\Delta^2(\omega) = \det(A^t A)$

$$= \det\left(\sum_k \sigma_k(\omega_i)\sigma_k(\omega_j)\right) = \det\left(\sum_k \sigma_k(\omega_i \omega_j)\right) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i \omega_j)).$$

□

Definition

Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be an n-tuple of elements of K, where $n = [K : \mathbb{Q}]$.

1. The **determinant** $\Delta(\omega) = \det(\sigma_i \omega_j)$.
2. The **discriminant** is $\Delta^2(\omega)$.

Lemma (1.1)

$\Delta^2(\omega) = \det(tr_{K/\mathbb{Q}}(\omega_i \omega_j))$, so $\Delta^2(\omega) \in \mathbb{Q}$.

Proof.

Let $A = (\sigma_i \omega_j)$. Then $\Delta^2(\omega) = \det(A^t A)$

$$= \det\left(\sum_k \sigma_k(\omega_i)\sigma_k(\omega_j)\right) = \det\left(\sum_k \sigma_k(\omega_i\omega_j)\right) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)).$$

$\square$

Lemma (1.2)

Let $\omega = \{\omega_1, \ldots, \omega_n\}$ *and* $\theta = \{\theta_1, \ldots, \theta_n\}$ *be two* $\mathbb{Q}$*-bases for* K*, and let* $C = (c_{ij})$ *be the matrix transforming* θ *to* ω *i.e.* $\omega_i = \sum c_{ij}\theta_j$*,* $c_{ij} \in \mathbb{Q}$*. Then* $\Delta(\omega) = \det(C)\Delta(\theta)$*, so* $\Delta^2(\omega) = (\det C)^2 \Delta^2(\theta)$*.*

(Proof trivial.)

Lemma (1.3)

If $K = \mathbb{Q}(\alpha)$ *and we take* $\omega = \{1, \alpha, \ldots, \alpha^{n-1}\}$ *then* $\Delta^2(\omega) = \prod_{i<j}(\alpha_i - \alpha_j)^2$*, where* $\alpha_1, \ldots, \alpha_n$ *are the conjugates of* α*.*

Proof.

$$\Delta(\omega) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}.$$

This has total degree $n(n-1)/2$ in the α_i, but is divisible by each of the $n(n-1)/2$ factors $(\alpha_i - \alpha_j)$. Comparing coefficients, it must be $\pm\prod_{i<j}(\alpha_i - \alpha_j)$. □

Lemma (1.2)

Let $\omega = \{\omega_1, \ldots, \omega_n\}$ and $\theta = \{\theta_1, \ldots, \theta_n\}$ be two $\mathbb{Q}$-bases for K, and let $C = (c_{ij})$ be the matrix transforming θ to ω i.e. $\omega_i = \sum c_{ij}\theta_j$, $c_{ij} \in \mathbb{Q}$. Then $\Delta(\omega) = \det(C)\Delta(\theta)$, so $\Delta^2(\omega) = (\det C)^2\Delta^2(\theta)$.

(Proof trivial.)

Lemma (1.3)

If $K = \mathbb{Q}(\alpha)$ and we take $\omega = \{1, \alpha, \ldots, \alpha^{n-1}\}$ then $\Delta^2(\omega) = \prod_{i<j}(\alpha_i - \alpha_j)^2$, where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α.

Proof.

$$\Delta(\omega) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}.$$

This has total degree $n(n-1)/2$ in the α_i, but is divisible by each of the $n(n-1)/2$ factors $(\alpha_i - \alpha_j)$. Comparing coefficients, it must be $\pm\prod_{i<j}(\alpha_i - \alpha_j)$. $\square$

Lemma (1.2)

Let $\omega = \{\omega_1, \dots, \omega_n\}$ and $\theta = \{\theta_1, \dots, \theta_n\}$ be two $\mathbb{Q}$-bases for K, and let $C = (c_{ij})$ be the matrix transforming θ to ω i.e. $\omega_i = \sum c_{ij}\theta_j$, $c_{ij} \in \mathbb{Q}$. Then $\Delta(\omega) = \det(C)\Delta(\theta)$, so $\Delta^2(\omega) = (\det C)^2\Delta^2(\theta)$.

(Proof trivial.)

Lemma (1.3)

If $K = \mathbb{Q}(\alpha)$ and we take $\omega = \{1, \alpha, \dots, \alpha^{n-1}\}$ then $\Delta^2(\omega) = \prod_{i<j}(\alpha_i - \alpha_j)^2$, where $\alpha_1, \dots, \alpha_n$ are the conjugates of α.

Proof.

$$\Delta(\omega) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix}.$$

This has total degree $n(n-1)/2$ in the α_i, but is divisible by each of the $n(n-1)/2$ factors $(\alpha_i - \alpha_j)$. Comparing coefficients, it must be $\pm\prod_{i<j}(\alpha_i - \alpha_j)$. $\square$

Lemma (1.2)

Let $\omega = \{\omega_1, \ldots, \omega_n\}$ *and* $\theta = \{\theta_1, \ldots, \theta_n\}$ *be two* $\mathbb{Q}$*-bases for* K*, and let* $C = (c_{ij})$ *be the matrix transforming* θ *to* ω *i.e.* $\omega_i = \sum c_{ij}\theta_j$*,* $c_{ij} \in \mathbb{Q}$*. Then* $\Delta(\omega) = \det(C)\Delta(\theta)$*, so* $\Delta^2(\omega) = (\det C)^2\Delta^2(\theta)$*.*

(Proof trivial.)

Lemma (1.3)

If $K = \mathbb{Q}(\alpha)$ *and we take* $\omega = \{1, \alpha, \ldots, \alpha^{n-1}\}$ *then* $\Delta^2(\omega) = \prod_{i<j}(\alpha_i - \alpha_j)^2$*, where* $\alpha_1, \ldots, \alpha_n$ *are the conjugates of* α*.*

Proof.

$$\Delta(\omega) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}.$$

This has total degree $n(n-1)/2$ in the α_i, but is divisible by each of the $n(n-1)/2$ factors $(\alpha_i - \alpha_j)$. Comparing coefficients, it must be $\pm\prod_{i<j}(\alpha_i - \alpha_j)$. $\square$

Corollary (1.5)

If $K = \mathbb{Q}(\alpha)$ *and* $\omega = \{1, \alpha, \ldots, \alpha^{n-1}\}$ *then* $\Delta(\omega) \neq 0$*.*

Corollary (1.4)

Let $\theta = \{\theta_1, \ldots, \theta_n\}$ *be an* n*-tuple of numbers in* K*.* $\Delta(\theta) \neq 0$ *if and only if* θ *is a* $\mathbb{Q}$*-basis for* K*.*

This follows from Lemma 2 and the preceding corollary when θ is a basis of K. If θ is not a basis then $\Delta(\theta) = 0$ (since the matrix has linearly dependent columns).

Corollary (1.5)

If $K = \mathbb{Q}(\alpha)$ *and* $\omega = \{1, \alpha, \ldots, \alpha^{n-1}\}$ *then* $\Delta(\omega) \neq 0$.

Corollary (1.4)

Let $\theta = \{\theta_1, \ldots, \theta_n\}$ *be an* n*-tuple of numbers in* K. $\Delta(\theta) \neq 0$ *if and only if* θ *is a* $\mathbb{Q}$*-basis for* K.

This follows from Lemma 2 and the preceding corollary when θ is a basis of K. If θ is not a basis then $\Delta(\theta) = 0$ (since the matrix has linearly dependent columns).

Corollary (1.5)

If $K = \mathbb{Q}(\alpha)$ and $\omega = \{1, \alpha, \dots, \alpha^{n-1}\}$ then $\Delta(\omega) \neq 0$.

Corollary (1.4)

Let $\theta = \{\theta_1, \dots, \theta_n\}$ be an n-tuple of numbers in K. $\Delta(\theta) \neq 0$ if and only if θ is a $\mathbb{Q}$-basis for K.

This follows from Lemma 2 and the preceding corollary when θ is a basis of K. If θ is not a basis then $\Delta(\theta) = 0$ (since the matrix has linearly dependent columns).

Definition

An algebraic number α is an *algebraic integer* if there exists a monic polynomial $g \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$.
If K is a number field then the set of all algebraic integers in K will be denoted by $\mathcal{O}_K$.

- α is an algebraic integer if and only if f_α, the minimal polynomial of α, is in $\mathbb{Z}[x]$. The verification is left as an exercise.
  Note that if $K = \mathbb{Q}$ then $\mathcal{O}_K = \mathbb{Z}$, since the min poly of $r \in \mathbb{Q}$ is $x - r$, which is in $\mathbb{Z}[x]$ iff $r \in \mathbb{Z}$. Of course $\mathbb{Z} \subseteq \mathcal{O}_K$.
- Suppose $\alpha \in K$ and $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Q}$. If $n \in \mathbb{Z}$ then

$$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + \ldots + n^d a_0 = 0.$$

  Choosing n large enough to clear the denominators of all the a_i, we get $n\alpha \in \mathcal{O}_K$.

Definition

An algebraic number α is an *algebraic integer* if there exists a monic polynomial $g \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$.
If K is a number field then the set of all algebraic integers in K will be denoted by $\mathcal{O}_K$.

- α is an algebraic integer if and only if f_α, the minimal polynomial of α, is in $\mathbb{Z}[x]$. The verification is left as an exercise.
  Note that if $K = \mathbb{Q}$ then $\mathcal{O}_K = \mathbb{Z}$, since the min poly of $r \in \mathbb{Q}$ is $x - r$, which is in $\mathbb{Z}[x]$ iff $r \in \mathbb{Z}$. Of course $\mathbb{Z} \subseteq \mathcal{O}_K$.
- Suppose $\alpha \in K$ and $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Q}$. If $n \in \mathbb{Z}$ then
  $$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + \ldots + n^d a_0 = 0.$$
  Choosing n large enough to clear the denominators of all the a_i, we get $n\alpha \in \mathcal{O}_K$.

Definition

An algebraic number α is an *algebraic integer* if there exists a monic polynomial $g \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$.
If K is a number field then the set of all algebraic integers in K will be denoted by $\mathcal{O}_K$.

- α is an algebraic integer if and only if f_α, the minimal polynomial of α, is in $\mathbb{Z}[x]$. The verification is left as an exercise.
  Note that if $K = \mathbb{Q}$ then $\mathcal{O}_K = \mathbb{Z}$, since the min poly of $r \in \mathbb{Q}$ is $x - r$, which is in $\mathbb{Z}[x]$ iff $r \in \mathbb{Z}$. Of course $\mathbb{Z} \subseteq \mathcal{O}_K$.
- Suppose $\alpha \in K$ and $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Q}$. If $n \in \mathbb{Z}$ then
  $$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + \ldots + n^d a_0 = 0.$$
  Choosing n large enough to clear the denominators of all the a_i, we get $n\alpha \in \mathcal{O}_K$.

Definition

An algebraic number α is an *algebraic integer* if there exists a monic polynomial $g \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$.
If K is a number field then the set of all algebraic integers in K will be denoted by $\mathcal{O}_K$.

- α is an algebraic integer if and only if f_α, the minimal polynomial of α, is in $\mathbb{Z}[x]$. The verification is left as an exercise.
  Note that if $K = \mathbb{Q}$ then $\mathcal{O}_K = \mathbb{Z}$, since the min poly of $r \in \mathbb{Q}$ is $x - r$, which is in $\mathbb{Z}[x]$ iff $r \in \mathbb{Z}$. Of course $\mathbb{Z} \subseteq \mathcal{O}_K$.
- Suppose $\alpha \in K$ and $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Q}$. If $n \in \mathbb{Z}$ then

  $$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + \ldots + n^d a_0 = 0.$$

  Choosing n large enough to clear the denominators of all the a_i, we get $n\alpha \in \mathcal{O}_K$.

Example. Quadratic fields K i.e. $[K : \mathbb{Q}] = 2$. Such a K is necessarily of the form $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$, $d \neq 1$, and $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for K.

Consider $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$ with $b \neq 0$. This has minimal polynomial $f_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$. So $\alpha \in O_K$ iff $2a, a^2 - db^2 \in \mathbb{Z}$. An elementary congruence analysis then shows that

- *Case 1.* If $d \equiv 2, 3 \pmod 4$ then $a, b \in \mathbb{Z}$. So $O_K = \mathbb{Z} + \sqrt{d}\mathbb{Z}$.

Example. Quadratic fields K i.e. $[K : \mathbb{Q}] = 2$. Such a K is necessarily of the form $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$, $d \neq 1$, and $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for K.

Consider $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$ with $b \neq 0$. This has minimal polynomial $f_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$. So $\alpha \in O_K$ iff $2a, a^2 - db^2 \in \mathbb{Z}$. An elementary congruence analysis then shows that

- *Case 1.* If $d \equiv 2, 3 \pmod 4$ then $a, b \in \mathbb{Z}$. So $\mathcal{O}_K = \mathbb{Z} + \sqrt{d}\mathbb{Z}$.
- *Case 2.* If $d \equiv 1 \pmod 4$, then a, b are both in $\mathbb{Z}$ or both in $\mathbb{Z} + \frac{1}{2}$. Thus $\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$.

Example. Quadratic fields K i.e. $[K : \mathbb{Q}] = 2$. Such a K is necessarily of the form $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$, $d \neq 1$, and $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for K.

Consider $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$ with $b \neq 0$. This has minimal polynomial $f_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$. So $\alpha \in O_K$ iff $2a, a^2 - db^2 \in \mathbb{Z}$. An elementary congruence analysis then shows that

- *Case 1.* If $d \equiv 2, 3 \pmod 4$ then $a, b \in \mathbb{Z}$. So $\mathcal{O}_K = \mathbb{Z} + \sqrt{d}\mathbb{Z}$.
- *Case 2.* If $d \equiv 1 \pmod 4$, then a, b are both in $\mathbb{Z}$ or both in $\mathbb{Z} + \frac{1}{2}$. Thus $\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$.

For example: If $K = \mathbb{Q}(i)$ then $O_K = \mathbb{Z}[i]$. If $K = \mathbb{Q}(\sqrt{-3})$ then $-\frac{1}{2} + \frac{\sqrt{-3}}{2} \in O_K$ (with min poly $x^2 + x + 1$).

Example. Quadratic fields K i.e. $[K:\mathbb{Q}]=2$. Such a K is necessarily of the form $K=\mathbb{Q}(\sqrt{d})$ for some square-free $d\in\mathbb{Z}$, $d\neq 1$, and $\{1,\sqrt{d}\}$ is a $\mathbb{Q}$-basis for K.

Consider $\alpha=a+b\sqrt{d}$ where $a,b\in\mathbb{Q}$ with $b\neq 0$. This has minimal polynomial $f_\alpha(x)=x^2-2ax+(a^2-db^2)$. So $\alpha\in O_K$ iff $2a, a^2-db^2\in\mathbb{Z}$. An elementary congruence analysis then shows that

- *Case 1.* If $d\equiv 2,3 \pmod 4$ then $a,b\in\mathbb{Z}$. So $\mathcal{O}_K=\mathbb{Z}+\sqrt{d}\mathbb{Z}$.
- *Case 2.* If $d\equiv 1 \pmod 4$, then a,b are both in $\mathbb{Z}$ or both in $\mathbb{Z}+\frac{1}{2}$. Thus $\mathcal{O}_K=\mathbb{Z}+\frac{1+\sqrt{d}}{2}\mathbb{Z}$.

For example: If $K=\mathbb{Q}(i)$ then $O_K=\mathbb{Z}[i]$. If $K=\mathbb{Q}(\sqrt{-3})$ then $-\frac{1}{2}+\frac{\sqrt{-3}}{2}\in O_K$ (with min poly x^2+x+1).

Example. Quadratic fields K i.e. $[K : \mathbb{Q}] = 2$. Such a K is necessarily of the form $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$, $d \neq 1$, and $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for K.

Consider $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$ with $b \neq 0$. This has minimal polynomial $f_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$. So $\alpha \in O_K$ iff $2a, a^2 - db^2 \in \mathbb{Z}$. An elementary congruence analysis then shows that

- *Case 1.* If $d \equiv 2, 3 \pmod 4$ then $a, b \in \mathbb{Z}$. So $\mathcal{O}_K = \mathbb{Z} + \sqrt{d}\mathbb{Z}$.
- *Case 2.* If $d \equiv 1 \pmod 4$, then a, b are both in $\mathbb{Z}$ or both in $\mathbb{Z} + \frac{1}{2}$. Thus $\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$.

For example: If $K = \mathbb{Q}(i)$ then $O_K = \mathbb{Z}[i]$. If $K = \mathbb{Q}(\sqrt{-3})$ then $-\frac{1}{2} + \frac{\sqrt{-3}}{2} \in O_K$ (with min poly $x^2 + x + 1$).

Example. Quadratic fields K i.e. $[K:\mathbb{Q}]=2$. Such a K is necessarily of the form $K=\mathbb{Q}(\sqrt{d})$ for some square-free $d\in\mathbb{Z}$, $d\neq 1$, and $\{1,\sqrt{d}\}$ is a $\mathbb{Q}$-basis for K.

Consider $\alpha=a+b\sqrt{d}$ where $a,b\in\mathbb{Q}$ with $b\neq 0$. This has minimal polynomial $f_\alpha(x)=x^2-2ax+(a^2-db^2)$. So $\alpha\in O_K$ iff $2a, a^2-db^2\in\mathbb{Z}$. An elementary congruence analysis then shows that

- *Case 1.* If $d\equiv 2,3 \pmod 4$ then $a,b\in\mathbb{Z}$. So $\mathcal{O}_K=\mathbb{Z}+\sqrt{d}\mathbb{Z}$.
- *Case 2.* If $d\equiv 1 \pmod 4$, then a,b are both in $\mathbb{Z}$ or both in $\mathbb{Z}+\frac{1}{2}$. Thus $\mathcal{O}_K=\mathbb{Z}+\frac{1+\sqrt{d}}{2}\mathbb{Z}$.

For example: If $K=\mathbb{Q}(i)$ then $O_K=\mathbb{Z}[i]$. If $K=\mathbb{Q}(\sqrt{-3})$ then $-\frac{1}{2}+\frac{\sqrt{-3}}{2}\in O_K$ (with min poly x^2+x+1).

Lemma (2.1)

Let K be any number field. An algebraic number $\alpha \in K$ is an algebraic integer iff there exists a non-zero, finitely generated $\mathbb{Z}$-submodule $M \subseteq K$ s.t. $\alpha M \subseteq M$.

Proof.

- First suppose $\alpha \in \mathcal{O}_K$, say $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Z}$. Then
$$M := \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{d-1}$$
is a finitely generated $\mathbb{Z}$-submodule of K and satisfies $\alpha M \subseteq M$.
- Conversely, suppose M is a submodule of K, finitely generated by $\{\omega_1, \ldots, \omega_m\}$, and that $\alpha M \subseteq M$. We can then write $\alpha\omega_i = \sum c_{ij}\omega_j$ with $c_{ij} \in \mathbb{Z}$.

Lemma (2.1)

Let K be any number field. An algebraic number $\alpha \in K$ is an algebraic integer iff there exists a non-zero, finitely generated $\mathbb{Z}$-submodule $M \subseteq K$ s.t. $\alpha M \subseteq M$.

Proof.

- First suppose $\alpha \in \mathcal{O}_K$, say $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Z}$. Then
$$M := \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{d-1}$$
is a finitely generated $\mathbb{Z}$-submodule of K and satisfies $\alpha M \subseteq M$.
- Conversely, suppose M is a submodule of K, finitely generated by $\{\omega_1, \ldots, \omega_m\}$, and that $\alpha M \subseteq M$. We can then write $\alpha\omega_i = \sum c_{ij}\omega_j$ with $c_{ij} \in \mathbb{Z}$.

  The square matrix $\alpha I_m - (c_{ij})$ kills the non-zero column vector (ω_i). Multiplying on the left by the adjoint of $\alpha I_m - (c_{ij})$, we get $\det(\alpha I_m - (c_{ij}))(\omega_i) = (0)$.

Lemma (2.1)

Let K be any number field. An algebraic number $\alpha \in K$ is an algebraic integer iff there exists a non-zero, finitely generated $\mathbb{Z}$-submodule $M \subseteq K$ s.t. $\alpha M \subseteq M$.

Proof.

- First suppose $\alpha \in \mathcal{O}_K$, say $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Z}$. Then
$$M := \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{d-1}$$
is a finitely generated $\mathbb{Z}$-submodule of K and satisfies $\alpha M \subseteq M$.
- Conversely, suppose M is a submodule of K, finitely generated by $\{\omega_1, \ldots, \omega_m\}$, and that $\alpha M \subseteq M$. We can then write $\alpha\omega_i = \sum c_{ij}\omega_j$ with $c_{ij} \in \mathbb{Z}$.

  The square matrix $\alpha I_m - (c_{ij})$ kills the non-zero column vector (ω_i). Multiplying on the left by the adjoint of $\alpha I_m - (c_{ij})$, we get $\det(\alpha I_m - (c_{ij}))(\omega_i) = (0)$. Since $(\omega_i) \neq (0)$, this forces $\det(\alpha I_m - (c_{ij})) = 0$ giving a monic poly in $\mathbb{Z}[x]$ satisfied by α.

□

Lemma (2.1)

Let K be any number field. An algebraic number $\alpha \in K$ is an algebraic integer iff there exists a non-zero, finitely generated $\mathbb{Z}$-submodule $M \subseteq K$ s.t. $\alpha M \subseteq M$.

Proof.

- First suppose $\alpha \in \mathcal{O}_K$, say $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Z}$. Then

$$M := \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{d-1}$$

  is a finitely generated $\mathbb{Z}$-submodule of K and satisfies $\alpha M \subseteq M$.
- Conversely, suppose M is a submodule of K, finitely generated by $\{\omega_1, \ldots, \omega_m\}$, and that $\alpha M \subseteq M$. We can then write $\alpha\omega_i = \sum c_{ij}\omega_j$ with $c_{ij} \in \mathbb{Z}$.

  The square matrix $\alpha I_m - (c_{ij})$ kills the non-zero column vector (ω_i). Multiplying on the left by the adjoint of $\alpha I_m - (c_{ij})$, we get $\det(\alpha I_m - (c_{ij}))(\omega_i) = (0)$. Since $(\omega_i) \neq (0)$, this forces $\det(\alpha I_m - (c_{ij})) = 0$ giving a monic poly in $\mathbb{Z}[x]$ satisfied by α.

□

Lemma (2.1)

Let K be any number field. An algebraic number $\alpha \in K$ is an algebraic integer iff there exists a non-zero, finitely generated $\mathbb{Z}$-submodule $M \subseteq K$ s.t. $\alpha M \subseteq M$.

Proof.

- First suppose $\alpha \in \mathcal{O}_K$, say $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Z}$. Then
$$M := \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{d-1}$$
is a finitely generated $\mathbb{Z}$-submodule of K and satisfies $\alpha M \subseteq M$.
- Conversely, suppose M is a submodule of K, finitely generated by $\{\omega_1, \ldots, \omega_m\}$, and that $\alpha M \subseteq M$. We can then write $\alpha\omega_i = \sum c_{ij}\omega_j$ with $c_{ij} \in \mathbb{Z}$.

  The square matrix $\alpha I_m - (c_{ij})$ kills the non-zero column vector (ω_i). Multiplying on the left by the adjoint of $\alpha I_m - (c_{ij})$, we get $\det(\alpha I_m - (c_{ij}))(\omega_i) = (0)$. Since $(\omega_i) \neq (0)$, this forces $\det(\alpha I_m - (c_{ij})) = 0$ giving a monic poly in $\mathbb{Z}[x]$ satisfied by α.

□

Lemma (2.1)

Let K be any number field. An algebraic number $\alpha \in K$ is an algebraic integer iff there exists a non-zero, finitely generated $\mathbb{Z}$-submodule $M \subseteq K$ s.t. $\alpha M \subseteq M$.

Proof.

- First suppose $\alpha \in \mathcal{O}_K$, say $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$, with $a_i \in \mathbb{Z}$. Then
$$M := \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{d-1}$$
is a finitely generated $\mathbb{Z}$-submodule of K and satisfies $\alpha M \subseteq M$.
- Conversely, suppose M is a submodule of K, finitely generated by $\{\omega_1, \ldots, \omega_m\}$, and that $\alpha M \subseteq M$. We can then write $\alpha\omega_i = \sum c_{ij}\omega_j$ with $c_{ij} \in \mathbb{Z}$.

  The square matrix $\alpha I_m - (c_{ij})$ kills the non-zero column vector (ω_i). Multiplying on the left by the adjoint of $\alpha I_m - (c_{ij})$, we get $\det(\alpha I_m - (c_{ij}))(\omega_i) = (0)$. Since $(\omega_i) \neq (0)$, this forces $\det(\alpha I_m - (c_{ij})) = 0$ giving a monic poly in $\mathbb{Z}[x]$ satisfied by α.

$\square$

Theorem (2.2)

Let K be a number field. If $\alpha, \beta \in \mathcal{O}_K$ then $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. It follows that $\mathcal{O}_K$ is a ring: the ring of integers of K.

Proof.

- Take non-zero submodules $M, N \subseteq K$, finitely generated by $\{\omega_1, \dots, \omega_d\}$ and $\{\theta_1, \dots, \theta_e\}$ respectively, such that $\alpha M \subseteq M$ and $\beta N \subseteq N$.
- Let $MN = \left\{\sum_{i=1}^{k} m_i n_i \;\middle|\; m_i \in M, n_i \in N\right\}$. This MN is a non-zero, finitely generated (by all the $\omega_i \theta_j$) $\mathbb{Z}$-submodule of K. Then:

$$(\alpha + \beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

and

$$(\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN.$$

So by the lemma, $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$.

□

Theorem (2.2)

Let K be a number field. If $\alpha, \beta \in \mathcal{O}_K$ then $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. It follows that $\mathcal{O}_K$ is a ring: the ring of integers of K.

Proof.

- Take non-zero submodules $M, N \subseteq K$, finitely generated by $\{\omega_1, \ldots, \omega_d\}$ and $\{\theta_1, \ldots, \theta_e\}$ respectively, such that $\alpha M \subseteq M$ and $\beta N \subseteq N$.
- Let $MN = \left\{\sum_{i=1}^{k} m_i n_i \ \middle|\ m_i \in M, n_i \in N\right\}$. This MN is a non-zero, finitely generated (by all the $\omega_i \theta_j$) $\mathbb{Z}$-submodule of K. Then:

$$(\alpha + \beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

and

$$(\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN.$$

So by the lemma, $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. □

Theorem (2.2)

Let K be a number field. If $\alpha, \beta \in \mathcal{O}_K$ then $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. It follows that $\mathcal{O}_K$ is a ring: the ring of integers of K.

Proof.

- Take non-zero submodules $M, N \subseteq K$, finitely generated by $\{\omega_1, \ldots, \omega_d\}$ and $\{\theta_1, \ldots, \theta_e\}$ respectively, such that $\alpha M \subseteq M$ and $\beta N \subseteq N$.
- Let $MN = \left\{\sum_{i=1}^{k} m_i n_i \;\middle|\; m_i \in M, n_i \in N\right\}$. This MN is a non-zero, finitely generated (by all the $\omega_i \theta_j$) $\mathbb{Z}$-submodule of K. Then:

$$(\alpha + \beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

and

$$(\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN.$$

So by the lemma, $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$.

□

Theorem (2.2)

Let K be a number field. If $\alpha, \beta \in \mathcal{O}_K$ then $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. It follows that $\mathcal{O}_K$ is a ring: the ring of integers of K.

Proof.

- Take non-zero submodules $M, N \subseteq K$, finitely generated by $\{\omega_1, \ldots, \omega_d\}$ and $\{\theta_1, \ldots, \theta_e\}$ respectively, such that $\alpha M \subseteq M$ and $\beta N \subseteq N$.
- Let $MN = \left\{ \sum_{i=1}^{k} m_i n_i \ \middle| \ m_i \in M, n_i \in N \right\}$. This MN is a non-zero, finitely generated (by all the $\omega_i \theta_j$) $\mathbb{Z}$-submodule of K. Then:

$$(\alpha + \beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

and

$$(\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN.$$

So by the lemma, $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$.

$\square$

Some useful consequences of the theorem above:

Proposition (2.3)

Let K be a number field, and let $\alpha \in \mathcal{O}_K$.

1. *$tr_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.*
2. *α is a unit in $\mathcal{O}_K$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof.

Suppose $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots \alpha_n$ are the $K/\mathbb{Q}$-conjugates of α. These are all algebraic integers.

Some useful consequences of the theorem above:

Proposition (2.3)

Let K be a number field, and let $\alpha \in \mathcal{O}_K$.

1. *$tr_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.*
2. *α is a unit in $\mathcal{O}_K$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof.

Suppose $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots \alpha_n$ are the $K/\mathbb{Q}$-conjugates of α. These are all algebraic integers.

1. $\mathrm{tr}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}(\alpha) = \alpha_1 \ldots \alpha_n$ are algebraic integers and also in $\mathbb{Q}$. Hence they must in fact be in $\mathbb{Z}$.

Some useful consequences of the theorem above:

Proposition (2.3)

Let K be a number field, and let $\alpha \in \mathcal{O}_K$.

1. *$tr_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.*
2. *α is a unit in $\mathcal{O}_K$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof.

Suppose $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots \alpha_n$ are the $K/\mathbb{Q}$-conjugates of α. These are all algebraic integers.

1. $\mathrm{tr}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}(\alpha) = \alpha_1 \ldots \alpha_n$ are algebraic integers and also in $\mathbb{Q}$. Hence they must in fact be in $\mathbb{Z}$.
2. First suppose α is a unit i.e. $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Then $\mathrm{N}(\alpha)\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = \mathrm{N}(1) = 1$. So $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are units of $\mathbb{Z}$, necessarily ± 1.

Some useful consequences of the theorem above:

Proposition (2.3)

Let K be a number field, and let $\alpha \in \mathcal{O}_K$.

1. *$tr_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.*
2. *α is a unit in $\mathcal{O}_K$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof.

Suppose $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots \alpha_n$ are the $K/\mathbb{Q}$-conjugates of α. These are all algebraic integers.

1. $\mathrm{tr}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}(\alpha) = \alpha_1 \ldots \alpha_n$ are algebraic integers and also in $\mathbb{Q}$. Hence they must in fact be in $\mathbb{Z}$.
2. First suppose α is a unit i.e. $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Then $\mathrm{N}(\alpha)\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = \mathrm{N}(1) = 1$. So $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are units of $\mathbb{Z}$, necessarily ± 1.

   Conversely, if $\mathrm{N}(\alpha) = 1$ then $\alpha^{-1} = \pm\alpha_2 \ldots \alpha_n$. So α^{-1} is an algebraic integer and also in K i.e. $\alpha^{-1} \in \mathcal{O}_K$.

□

Some useful consequences of the theorem above:

Proposition (2.3)

Let K be a number field, and let $\alpha \in \mathcal{O}_K$.

1. *$tr_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.*
2. *α is a unit in $\mathcal{O}_K$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof.

Suppose $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots \alpha_n$ are the $K/\mathbb{Q}$-conjugates of α. These are all algebraic integers.

1. $\mathrm{tr}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}(\alpha) = \alpha_1 \ldots \alpha_n$ are algebraic integers and also in $\mathbb{Q}$. Hence they must in fact be in $\mathbb{Z}$.
2. First suppose α is a unit i.e. $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Then $\mathrm{N}(\alpha)\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = \mathrm{N}(1) = 1$. So $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are units of $\mathbb{Z}$, necessarily ± 1.

   Conversely, if $\mathrm{N}(\alpha) = 1$ then $\alpha^{-1} = \pm \alpha_2 \ldots \alpha_n$. So α^{-1} is an algebraic integer and also in K i.e. $\alpha^{-1} \in \mathcal{O}_K$.

□

Some useful consequences of the theorem above:

Proposition (2.3)

Let K be a number field, and let $\alpha \in \mathcal{O}_K$.

1. *$tr_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.*
2. *α is a unit in $\mathcal{O}_K$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof.

Suppose $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots \alpha_n$ are the $K/\mathbb{Q}$-conjugates of α. These are all algebraic integers.

1. $\mathrm{tr}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}(\alpha) = \alpha_1 \ldots \alpha_n$ are algebraic integers and also in $\mathbb{Q}$. Hence they must in fact be in $\mathbb{Z}$.
2. First suppose α is a unit i.e. $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Then $\mathrm{N}(\alpha)\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = \mathrm{N}(1) = 1$. So $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are units of $\mathbb{Z}$, necessarily ± 1.

   Conversely, if $\mathrm{N}(\alpha) = 1$ then $\alpha^{-1} = \pm \alpha_2 \ldots \alpha_n$. So α^{-1} is an algebraic integer and also in K i.e. $\alpha^{-1} \in \mathcal{O}_K$.

$\square$

Some useful consequences of the theorem above:

Proposition (2.3)

Let K be a number field, and let $\alpha \in \mathcal{O}_K$.

1. $tr_{K/\mathbb{Q}}(\alpha)$ *and* $N_{K/\mathbb{Q}}(\alpha)$ *are in* $\mathbb{Z}$*.*
2. α *is a unit in* $\mathcal{O}_K$ *iff* $N_{K/\mathbb{Q}}(\alpha) = \pm 1$*.*

Proof.

Suppose $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots \alpha_n$ are the $K/\mathbb{Q}$-conjugates of α. These are all algebraic integers.

1. $\mathrm{tr}(\alpha) = \alpha_1 + \ldots + \alpha_n$ and $\mathrm{N}(\alpha) = \alpha_1 \ldots \alpha_n$ are algebraic integers and also in $\mathbb{Q}$. Hence they must in fact be in $\mathbb{Z}$.
2. First suppose α is a unit i.e. $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Then $\mathrm{N}(\alpha)\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = \mathrm{N}(1) = 1$. So $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are units of $\mathbb{Z}$, necessarily ± 1.

   Conversely, if $\mathrm{N}(\alpha) = 1$ then $\alpha^{-1} = \pm\alpha_2 \ldots \alpha_n$. So α^{-1} is an algebraic integer and also in K i.e. $\alpha^{-1} \in \mathcal{O}_K$.

$\square$

Theorem (2.4)

Let K be a number field, with $[K : \mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $O_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $O_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^n c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $O_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^n c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq O_K$ and

$$|\Delta^2(\theta)| = c_j^2|\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$.

□

Theorem (2.4)

Let K be a number field, with $[K : \mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $O_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^n c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq O_K$ and

$$|\Delta^2(\theta)| = c_j^2|\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$.

□

Theorem (2.4)

Let K be a number field, with $[K : \mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $O_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^n c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq O_K$ and

$$|\Delta^2(\theta)| = c_j^2|\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$.

□

Theorem (2.4)

Let K be a number field, with $[K : \mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $O_K = \{\sum c_j \omega_j \mid c_j \in \mathbb{Z}\}$.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i \omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^{n} c_j \omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq O_K$ and

$$|\Delta^2(\theta)| = c_j^2 |\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$.

□

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$. Equivalently, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}]=n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1,\ldots,\omega_n\in\mathcal{O}_K$ such that $\mathcal{O}_K=\{\sum c_j\omega_j \mid c_j\in\mathbb{Z}\}$. Equivalently, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof.

- Let $\omega=\{\omega_1,\ldots,\omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega\subseteq\mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M:=\mathbb{Z}\omega_1+\ldots+\mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega)\neq 0$, since $\{\omega_1,\ldots,\omega_n\}$ is linearly independent, and $\Delta^2(\omega)=\det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j))\in\mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M=\mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha\in\mathcal{O}_K$ s.t. $\alpha\notin M$. Let $\alpha=\sum_{j=1}^n c_j\omega_j$ with $c_j\in\mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j|\leq 1/2$, and some $c_j\neq 0$ since $\alpha\notin M$.

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \{\sum c_j \omega_j \mid c_j \in \mathbb{Z}\}$. Equivalently, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^n c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq \mathcal{O}_K$ and

$$|\Delta^2(\theta)| = c_j^2|\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$.

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$. Equivalently, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^n c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq \mathcal{O}_K$ and

$$|\Delta^2(\theta)| = c_j^2|\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$.

□

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$. Equivalently, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^{n} c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq \mathcal{O}_K$ and

$$|\Delta^2(\theta)| = c_j^2|\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$.

Theorem (2.4)

Let K be a number field, with $[K:\mathbb{Q}] = n$. Then $\mathcal{O}_K$ has an integral basis, i.e. we can find $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \{\sum c_j\omega_j \mid c_j \in \mathbb{Z}\}$. Equivalently, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof.

- Let $\omega = \{\omega_1, \ldots, \omega_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each ω_i by a sufficiently large integer, we may suppose that $\omega \subseteq \mathcal{O}_K$, spanning a $\mathbb{Z}$-submodule $M := \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ of $\mathcal{O}_K$.
- The discriminant $\Delta^2(\omega) \neq 0$, since $\{\omega_1, \ldots, \omega_n\}$ is linearly independent, and $\Delta^2(\omega) = \det(\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)) \in \mathbb{Z}$. Thus we may choose M s.t. $|\Delta^2(\omega)|$ is minimal. Claim: ω is an integral basis, i.e. $M = \mathcal{O}_K$.
- Suppose, to the contrary, we can find $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin M$. Let $\alpha = \sum_{j=1}^n c_j\omega_j$ with $c_j \in \mathbb{Q}$. Subtracting the "nearest" element of M, we may suppose each $|c_j| \leq 1/2$, and some $c_j \neq 0$ since $\alpha \notin M$.
- Let θ be the new $\mathbb{Q}$-basis for K obtained from ω by replacing ω_j by α. Then $\theta \subseteq \mathcal{O}_K$ and

$$|\Delta^2(\theta)| = c_j^2|\Delta^2(\omega)| < |\Delta^2(\omega)|,$$

contradicting the minimality of $|\Delta^2(\omega)|$. $\square$

Big Problem: The ring of integers of a number field is not necessarily a unique factorisation domain.

Example: $\mathbb{Q}(\sqrt{-5})$ has ring of integers $\mathbb{Z}[\sqrt{-5}]$. Now consider the factorization

$$2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Now 2 is irreducible, since if $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ with neither a unit, then taking norms we get $2 = a^2 + 5b^2$, which has no solutions for $a, b \in \mathbb{Z}$. But 2 divides neither factor $1 \pm \sqrt{-5}$. (In fact, all the given factors are irreducible, and this is two different factorisations of 6 into products of irreducibles.)

Big Problem: The ring of integers of a number field is not necessarily a unique factorisation domain.

Example: $\mathbb{Q}(\sqrt{-5})$ has ring of integers $\mathbb{Z}[\sqrt{-5}]$. Now consider the factorization

$$2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Now 2 is irreducible, since if $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ with neither a unit, then taking norms we get $2 = a^2 + 5b^2$, which has no solutions for $a, b \in \mathbb{Z}$. But 2 divides neither factor $1 \pm \sqrt{-5}$. (In fact, all the given factors are irreducible, and this is two different factorisations of 6 into products of irreducibles.)

Big Problem: The ring of integers of a number field is not necessarily a unique factorisation domain.

Example: $\mathbb{Q}(\sqrt{-5})$ has ring of integers $\mathbb{Z}[\sqrt{-5}]$. Now consider the factorization

$$2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Now 2 is irreducible, since if $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ with neither a unit, then taking norms we get $2 = a^2 + 5b^2$, which has no solutions for $a, b \in \mathbb{Z}$. But 2 divides neither factor $1 \pm \sqrt{-5}$. (In fact, all the given factors are irreducible, and this is two different factorisations of 6 into products of irreducibles.)

Big Problem: The ring of integers of a number field is not necessarily a unique factorisation domain.

Example: $\mathbb{Q}(\sqrt{-5})$ has ring of integers $\mathbb{Z}[\sqrt{-5}]$. Now consider the factorization

$$2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Now 2 is irreducible, since if $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ with neither a unit, then taking norms we get $2 = a^2 + 5b^2$, which has no solutions for $a, b \in \mathbb{Z}$. But 2 divides neither factor $1 \pm \sqrt{-5}$. (In fact, all the given factors are irreducible, and this is two different factorisations of 6 into products of irreducibles.)

Big Problem: The ring of integers of a number field is not necessarily a unique factorisation domain.

Example: $\mathbb{Q}(\sqrt{-5})$ has ring of integers $\mathbb{Z}[\sqrt{-5}]$. Now consider the factorization

$$2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}).$$

Now 2 is irreducible, since if $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ with neither a unit, then taking norms we get $2 = a^2 + 5b^2$, which has no solutions for $a, b \in \mathbb{Z}$. But 2 divides neither factor $1 \pm \sqrt{-5}$. (In fact, all the given factors are irreducible, and this is two different factorisations of 6 into products of irreducibles.)

Remarkably, unique factorisation can be restored if we work with ideals instead. We recall some basic definitions and conventions: Let R be a commutative ring.

- A non-empty subset I of R is an ideal if $ra + sb \in I$ for all $r, s \in R$, $a, b \in I$ i.e. I is an R-submodule of R. The ideal I is finitely generated if it is finitely generated as an R-module i.e. there are $a_1, \dots, a_n \in R$ such that $I = Ra_1 + \dots + Ra_n =: (a_1, \dots, a_n)$. The ring R is noetherian if every ideal is finitely generated.
- A proper ideal I of R is said to be *prime* if, whenever $ab \in I$, either $a \in I$ or $b \in I$. A *maximal* ideal is a proper ideal which is not contained inside any proper ideal except itself. A proper ideal I is prime iff R/I is an integral domain; it is maximal iff R/I is a field. Maximal ideals are prime.
- If I and J ideals of R, then their product IJ is given by

$$IJ := \left\{ \sum_{i=1}^{k} a_i b_i \mid a_i \in I, b_i \in J, k \geq 1 \right\}.$$

Note that IJ is an ideal, and that if $I = (a_1, \dots, a_m)$ and $J = (b_1, \dots, b_n)$ then IJ is finitely generated with generators $a_i b_j$ where $1 \leq i \leq m, 1 \leq j \leq n$.

Remarkably, unique factorisation can be restored if we work with ideals instead. We recall some basic definitions and conventions: Let R be a commutative ring.

- A non-empty subset I of R is an ideal if $ra + sb \in I$ for all $r, s \in R$, $a, b \in I$ i.e. I is an R-submodule of R. The ideal I is finitely generated if it is finitely generated as an R-module i.e. there are $a_1, \ldots, a_n \in R$ such that $I = Ra_1 + \ldots + Ra_n =: (a_1, \ldots, a_n)$. The ring R is noetherian if every ideal is finitely generated.
- A proper ideal I of R is said to be *prime* if, whenever $ab \in I$, either $a \in I$ or $b \in I$. A *maximal* ideal is a proper ideal which is not contained inside any proper ideal except itself. A proper ideal I is prime iff R/I is an integral domain; it is maximal iff R/I is a field. Maximal ideals are prime.
- If I and J ideals of R, then their product IJ is given by

$$IJ := \left\{ \sum_{i=1}^{k} a_i b_i \mid a_i \in I, b_i \in J, k \geq 1 \right\}.$$

  Note that IJ is an ideal, and that if $I = (a_1, \ldots, a_m)$ and $J = (b_1, \ldots, b_n)$ then IJ is finitely generated with generators $a_i b_j$ where $1 \leq i \leq m, 1 \leq j \leq n$.

Remarkably, unique factorisation can be restored if we work with ideals instead. We recall some basic definitions and conventions: Let R be a commutative ring.

- A non-empty subset I of R is an ideal if $ra + sb \in I$ for all $r, s \in R$, $a, b \in I$ i.e. I is an R-submodule of R. The ideal I is finitely generated if it is finitely generated as an R-module i.e. there are $a_1, \dots, a_n \in R$ such that $I = Ra_1 + \dots + Ra_n =: (a_1, \dots, a_n)$. The ring R is noetherian if every ideal is finitely generated.
- A proper ideal I of R is said to be *prime* if, whenever $ab \in I$, either $a \in I$ or $b \in I$. A *maximal* ideal is a proper ideal which is not contained inside any proper ideal except itself. A proper ideal I is prime iff R/I is an integral domain; it is maximal iff R/I is a field. Maximal ideals are prime.
- If I and J ideals of R, then their product IJ is given by

$$IJ := \left\{ \sum_{i=1}^{k} a_i b_i \mid a_i \in I, b_i \in J, k \geq 1 \right\}.$$

Note that IJ is an ideal, and that if $I = (a_1, \dots, a_m)$ and $J = (b_1, \dots, b_n)$ then IJ is finitely generated with generators $a_i b_j$ where $1 \leq i \leq m, 1 \leq j \leq n$.

Remarkably, unique factorisation can be restored if we work with ideals instead. We recall some basic definitions and conventions: Let R be a commutative ring.

- A non-empty subset I of R is an ideal if $ra + sb \in I$ for all $r, s \in R$, $a, b \in I$ i.e. I is an R-submodule of R. The ideal I is finitely generated if it is finitely generated as an R-module i.e. there are $a_1, \ldots, a_n \in R$ such that $I = Ra_1 + \ldots + Ra_n =: (a_1, \ldots, a_n)$. The ring R is noetherian if every ideal is finitely generated.
- A proper ideal I of R is said to be *prime* if, whenever $ab \in I$, either $a \in I$ or $b \in I$. A *maximal* ideal is a proper ideal which is not contained inside any proper ideal except itself. A proper ideal I is prime iff R/I is an integral domain; it is maximal iff R/I is a field. Maximal ideals are prime.
- If I and J ideals of R, then their product IJ is given by

$$IJ := \left\{ \sum_{i=1}^{k} a_i b_i \mid a_i \in I, b_i \in J, k \geq 1 \right\}.$$

  Note that IJ is an ideal, and that if $I = (a_1, \ldots, a_m)$ and $J = (b_1, \ldots, b_n)$ then IJ is finitely generated with generators $a_i b_j$ where $1 \leq i \leq m, 1 \leq j \leq n$.

Theorem (Dedekind)

Let K be a number field with ring of integers $\mathcal{O}_K$. Any non-zero proper ideal $I \subset \mathcal{O}_K$ can be written as a product of prime ideals $I = P_1 P_2 \dots P_r$, which is unique up to the order of the factors.

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K:\mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. □

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K:\mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. □

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

Corollary (3.2)

1. *Every ideal of $\mathcal{O}$ is finitely generated.*

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K:\mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. $\square$

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

Corollary (3.2)

1. *Every ideal of $\mathcal{O}$ is finitely generated.*
2. *(Ascending chain condition). If $I_1 \subseteq I_2 \subseteq \ldots$ is an increasing chain of ideals of R then there is exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$.*

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K:\mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. $\square$

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

Corollary (3.2)

1. *Every ideal of $\mathcal{O}$ is finitely generated.*
2. *(Ascending chain condition). If $I_1 \subseteq I_2 \subseteq \ldots$ is an increasing chain of ideals of R then there is exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$.*
3. *Every non-empty set S of ideals of R contains a maximal element i.e. there is an ideal I in S such that no ideal $J \in S$ strictly contains I.*

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K : \mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. □

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

Corollary (3.2)

1. *Every ideal of $\mathcal{O}$ is finitely generated.*
2. *(Ascending chain condition). If $I_1 \subseteq I_2 \subseteq \ldots$ is an increasing chain of ideals of R then there is exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$.*
3. *Every non-empty set S of ideals of R contains a maximal element i.e. there is an ideal I in S such that no ideal $J \in S$ strictly contains I.*

In fact the above three properties are equivalent formulations of noetherianness.

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K : \mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. □

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

Corollary (3.2)

1. *Every ideal of $\mathcal{O}$ is finitely generated.*
2. *(Ascending chain condition). If $I_1 \subseteq I_2 \subseteq \ldots$ is an increasing chain of ideals of R then there is exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$.*
3. *Every non-empty set S of ideals of R contains a maximal element i.e. there is an ideal I in S such that no ideal $J \in S$ strictly contains I.*

In fact the above three properties are equivalent formulations of noetherianness.

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K:\mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. □

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

Corollary (3.2)

1. *Every ideal of $\mathcal{O}$ is finitely generated.*
2. *(Ascending chain condition). If $I_1 \subseteq I_2 \subseteq \ldots$ is an increasing chain of ideals of R then there is exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$.*
3. *Every non-empty set S of ideals of R contains a maximal element i.e. there is an ideal I in S such that no ideal $J \in S$ strictly contains I.*

In fact the above three properties are equivalent formulations of noetherianness.

From here on K is a fixed number field, $\mathcal{O}$ its integer ring. The existence of an integral basis implies that $\mathcal{O}$ is noetherian.

Lemma (3.1)

If I is a non-zero ideal of $\mathcal{O}$ then $\mathcal{O}/I$ is finite. The cardinality of $\mathcal{O}/I$ is, by definition, the norm of I and is denoted by $N(I)$.

Proof.

Let $[K:\mathbb{Q}] = n$ and let $w_1, \ldots, w_n$ be an integral basis of $\mathcal{O}$. Pick $0 \neq \alpha \in I$. Then $\alpha\mathcal{O} = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is free $\mathbb{Z}$-submodule of $\mathcal{O}$ of rank n. Thus $\mathcal{O}/\alpha\mathcal{O}$ is finite. As $\alpha\mathcal{O} \subseteq I \subseteq \mathcal{O}$, we also get $\mathcal{O}/I$ is finite. $\square$

It follows easily from the lemma that $\mathcal{O}$ is noetherian:

Corollary (3.2)

1. *Every ideal of $\mathcal{O}$ is finitely generated.*
2. *(Ascending chain condition). If $I_1 \subseteq I_2 \subseteq \ldots$ is an increasing chain of ideals of R then there is exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$.*
3. *Every non-empty set S of ideals of R contains a maximal element i.e. there is an ideal I in S such that no ideal $J \in S$ strictly contains I.*

In fact the above three properties are equivalent formulations of noetherianness.

Remark: If $\alpha \in \mathcal{O}$ with $\alpha \neq 0$ then $N((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Indeed, writing $\mathcal{O} = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ for an integral basis, the index of $(\alpha) = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is the absolute value of the determinant of T_α (the multiplication by α map), which is $\mathrm{N}(\alpha)$.

Theorem (3.3)

1. *$\mathcal{O}$ is Noetherian i.e. every ideal of $\mathcal{O}$ is finitely generated.*
2. *Every non-zero prime ideal of $\mathcal{O}$ is a maximal ideal.*

Remark: If $\alpha \in \mathcal{O}$ with $\alpha \neq 0$ then $N((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Indeed, writing $\mathcal{O} = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ for an integral basis, the index of $(\alpha) = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is the absolute value of the determinant of T_α (the multiplication by α map), which is $\mathrm{N}(\alpha)$.

Theorem (3.3)

1. *$\mathcal{O}$ is Noetherian i.e. every ideal of $\mathcal{O}$ is finitely generated.*
2. *Every non-zero prime ideal of $\mathcal{O}$ is a maximal ideal.*
3. *$\mathcal{O}$ is integrally closed in its field of fractions K: if $\alpha \in K$ is the root of a monic polynomial over $\mathcal{O}$ then $\alpha \in \mathcal{O}$.*

Remark: If $\alpha \in \mathcal{O}$ with $\alpha \neq 0$ then $N((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Indeed, writing $\mathcal{O} = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ for an integral basis, the index of $(\alpha) = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is the absolute value of the determinant of T_α (the multiplication by α map), which is $\mathrm{N}(\alpha)$.

Theorem (3.3)

1. *$\mathcal{O}$ is Noetherian i.e. every ideal of $\mathcal{O}$ is finitely generated.*
2. *Every non-zero prime ideal of $\mathcal{O}$ is a maximal ideal.*
3. *$\mathcal{O}$ is integrally closed in its field of fractions K: if $\alpha \in K$ is the root of a monic polynomial over $\mathcal{O}$ then $\alpha \in \mathcal{O}$.*

For the second part, we use lemma 3.1 to note that if P is prime then $\mathcal{O}/P$ is a finite integral domain; so a field and P is maximal.

Remark: If $\alpha \in \mathcal{O}$ with $\alpha \neq 0$ then $N((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Indeed, writing $\mathcal{O} = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ for an integral basis, the index of $(\alpha) = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is the absolute value of the determinant of T_α (the multiplication by α map), which is $\mathrm{N}(\alpha)$.

Theorem (3.3)

1. *$\mathcal{O}$ is Noetherian i.e. every ideal of $\mathcal{O}$ is finitely generated.*
2. *Every non-zero prime ideal of $\mathcal{O}$ is a maximal ideal.*
3. *$\mathcal{O}$ is integrally closed in its field of fractions K: if $\alpha \in K$ is the root of a monic polynomial over $\mathcal{O}$ then $\alpha \in \mathcal{O}$.*

For the second part, we use lemma 3.1 to note that if P is prime then $\mathcal{O}/P$ is a finite integral domain; so a field and P is maximal.

For the last part, suppose $\alpha \in K$ satisfies $\alpha^d + a_1\alpha^{d-1} + \ldots + a_d = 0$ with a_i's in $\mathcal{O}$. Then $M := \mathcal{O} + \alpha\mathcal{O} + \ldots + \alpha^{d-1}$ is a non-zero finitely generated $\mathbb{Z}$ submodule of K such that $\alpha M \subseteq M$. Thus α is an algebraic integer and hence in $\mathcal{O}$.

Remark: If $\alpha \in \mathcal{O}$ with $\alpha \neq 0$ then $N((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Indeed, writing $\mathcal{O} = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ for an integral basis, the index of $(\alpha) = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is the absolute value of the determinant of T_α (the multiplication by α map), which is $\mathrm{N}(\alpha)$.

Theorem (3.3)

1. *$\mathcal{O}$ is Noetherian i.e. every ideal of $\mathcal{O}$ is finitely generated.*
2. *Every non-zero prime ideal of $\mathcal{O}$ is a maximal ideal.*
3. *$\mathcal{O}$ is integrally closed in its field of fractions K: if $\alpha \in K$ is the root of a monic polynomial over $\mathcal{O}$ then $\alpha \in \mathcal{O}$.*

For the second part, we use lemma 3.1 to note that if P is prime then $\mathcal{O}/P$ is a finite integral domain; so a field and P is maximal.

For the last part, suppose $\alpha \in K$ satisfies $\alpha^d + a_1\alpha^{d-1} + \ldots + a_d = 0$ with a_i's in $\mathcal{O}$. Then $M := \mathcal{O} + \alpha\mathcal{O} + \ldots + \alpha^{d-1}$ is a non-zero finitely generated $\mathbb{Z}$ submodule of K such that $\alpha M \subseteq M$. Thus α is an algebraic integer and hence in $\mathcal{O}$.

Remark: If $\alpha \in \mathcal{O}$ with $\alpha \neq 0$ then $N((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Indeed, writing $\mathcal{O} = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ for an integral basis, the index of $(\alpha) = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is the absolute value of the determinant of T_α (the multiplication by α map), which is $\mathrm{N}(\alpha)$.

Theorem (3.3)

1. *$\mathcal{O}$ is Noetherian i.e. every ideal of $\mathcal{O}$ is finitely generated.*
2. *Every non-zero prime ideal of $\mathcal{O}$ is a maximal ideal.*
3. *$\mathcal{O}$ is integrally closed in its field of fractions K: if $\alpha \in K$ is the root of a monic polynomial over $\mathcal{O}$ then $\alpha \in \mathcal{O}$.*

For the second part, we use lemma 3.1 to note that if P is prime then $\mathcal{O}/P$ is a finite integral domain; so a field and P is maximal.

For the last part, suppose $\alpha \in K$ satisfies $\alpha^d + a_1\alpha^{d-1} + \ldots + a_d = 0$ with a_i's in $\mathcal{O}$. Then $M := \mathcal{O} + \alpha\mathcal{O} + \ldots + \alpha^{d-1}$ is a non-zero finitely generated $\mathbb{Z}$ submodule of K such that $\alpha M \subseteq M$. Thus α is an algebraic integer and hence in $\mathcal{O}$.

Remark: If $\alpha \in \mathcal{O}$ with $\alpha \neq 0$ then $N((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Indeed, writing $\mathcal{O} = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ for an integral basis, the index of $(\alpha) = \mathbb{Z}\alpha w_1 + \ldots + \mathbb{Z}\alpha w_n$ is the absolute value of the determinant of T_α (the multiplication by α map), which is $\mathrm{N}(\alpha)$.

Theorem (3.3)

1. *$\mathcal{O}$ is Noetherian i.e. every ideal of $\mathcal{O}$ is finitely generated.*
2. *Every non-zero prime ideal of $\mathcal{O}$ is a maximal ideal.*
3. *$\mathcal{O}$ is integrally closed in its field of fractions K: if $\alpha \in K$ is the root of a monic polynomial over $\mathcal{O}$ then $\alpha \in \mathcal{O}$.*

For the second part, we use lemma 3.1 to note that if P is prime then $\mathcal{O}/P$ is a finite integral domain; so a field and P is maximal.

For the last part, suppose $\alpha \in K$ satisfies $\alpha^d + a_1\alpha^{d-1} + \ldots + a_d = 0$ with a_i's in $\mathcal{O}$. Then $M := \mathcal{O} + \alpha\mathcal{O} + \ldots + \alpha^{d-1}$ is a non-zero finitely generated $\mathbb{Z}$ submodule of K such that $\alpha M \subseteq M$. Thus α is an algebraic integer and hence in $\mathcal{O}$.

Containment of ideals is essentially divisibility: we shall say that an ideal I divides J if $I \supseteq J$. For instance m divides n in $\mathbb{Z}$ iff $n\mathbb{Z} \subseteq m\mathbb{Z}$.

Lemma (3.4)

Every ideal of $\mathcal{O}$ contains a product of prime ideals.

Thus every ideal divides a product of prime ideals, which is one step towards proving that every ideal is the product prime ideals.

Proof.

Suppose false; let S be the set of all ideals of $\mathcal{O}$ which fail to contain a product of prime ideals. Let I be a maximal element of S. Then I is not a prime ideal.

Containment of ideals is essentially divisibility: we shall say that an ideal I divides J if $I \supseteq J$. For instance m divides n in $\mathbb{Z}$ iff $n\mathbb{Z} \subseteq m\mathbb{Z}$.

Lemma (3.4)

Every ideal of $\mathcal{O}$ contains a product of prime ideals.

Thus every ideal divides a product of prime ideals, which is one step towards proving that every ideal is the product prime ideals.

Proof.
Suppose false; let S be the set of all ideals of $\mathcal{O}$ which fail to contain a product of prime ideals. Let I be a maximal element of S. Then I is not a prime ideal.

So we can find $a, b \in \mathcal{O}$ such that a, b are not in I but $ab \in I$. Then $(a) + I$, $(b) + I$ are ideals strictly containing I, so they contain product of primes. The lemma follows because $((a) + I)((b) + I) \subseteq I$. $\square$

Containment of ideals is essentially divisibility: we shall say that an ideal I divides J if $I \supseteq J$. For instance m divides n in $\mathbb{Z}$ iff $n\mathbb{Z} \subseteq m\mathbb{Z}$.

Lemma (3.4)

Every ideal of $\mathcal{O}$ contains a product of prime ideals.

Thus every ideal divides a product of prime ideals, which is one step towards proving that every ideal is the product prime ideals.

Proof.

Suppose false; let S be the set of all ideals of $\mathcal{O}$ which fail to contain a product of prime ideals. Let I be a maximal element of S. Then I is not a prime ideal.

So we can find $a, b \in \mathcal{O}$ such that a, b are not in I but $ab \in I$. Then $(a) + I$, $(b) + I$ are ideals strictly containing I, so they contain product of primes. The lemma follows because $((a) + I)((b) + I) \subseteq I$. $\square$

Containment of ideals is essentially divisibility: we shall say that an ideal I divides J if $I \supseteq J$. For instance m divides n in $\mathbb{Z}$ iff $n\mathbb{Z} \subseteq m\mathbb{Z}$.

Lemma (3.4)

Every ideal of $\mathcal{O}$ contains a product of prime ideals.

Thus every ideal divides a product of prime ideals, which is one step towards proving that every ideal is the product prime ideals.

Proof.

Suppose false; let S be the set of all ideals of $\mathcal{O}$ which fail to contain a product of prime ideals. Let I be a maximal element of S. Then I is not a prime ideal.

So we can find $a, b \in \mathcal{O}$ such that a, b are not in I but $ab \in I$. Then $(a) + I$, $(b) + I$ are ideals strictly containing I, so they contain product of primes. The lemma follows because $((a) + I)((b) + I) \subseteq I$. $\square$

Containment of ideals is essentially divisibility: we shall say that an ideal I divides J if $I \supseteq J$. For instance m divides n in $\mathbb{Z}$ iff $n\mathbb{Z} \subseteq m\mathbb{Z}$.

Lemma (3.4)

Every ideal of $\mathcal{O}$ contains a product of prime ideals.

Thus every ideal divides a product of prime ideals, which is one step towards proving that every ideal is the product prime ideals.

Proof.

Suppose false; let S be the set of all ideals of $\mathcal{O}$ which fail to contain a product of prime ideals. Let I be a maximal element of S. Then I is not a prime ideal.

So we can find $a, b \in \mathcal{O}$ such that a, b are not in I but $ab \in I$. Then $(a) + I$, $(b) + I$ are ideals strictly containing I, so they contain product of primes. The lemma follows because $((a) + I)((b) + I) \subseteq I$. $\square$

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. *$A \supseteq B$ if and only if $A|B$.*
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. *$A \supseteq B$ if and only if $A|B$.*
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

The first consequence in the above proposition is immediate from the main statement.

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. *$A \supseteq B$ if and only if $A|B$.*
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

The first consequence in the above proposition is immediate from the main statement. For the second, pick $0 \neq a \in A$. Then $A|(a)$ and so $(a) = AA'$ for some ideal A'. This gives $(a)B = (a)C$; hence $B = C$.

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. $A \supseteq B$ *if and only if* $A|B$.
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

The first consequence in the above proposition is immediate from the main statement. For the second, pick $0 \neq a \in A$. Then $A|(a)$ and so $(a) = AA'$ for some ideal A'. This gives $(a)B = (a)C$; hence $B = C$.

We move on to the proof of Dedekind's Theorem; we will finish off proposition 3.1 later on. But first an observation (the proof is left as an exercise).

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. *$A \supseteq B$ if and only if $A|B$.*
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

The first consequence in the above proposition is immediate from the main statement. For the second, pick $0 \neq a \in A$. Then $A|(a)$ and so $(a) = AA'$ for some ideal A'. This gives $(a)B = (a)C$; hence $B = C$.

We move on to the proof of Dedekind's Theorem; we will finish off proposition 3.1 later on. But first an observation (the proof is left as an exercise).

Lemma (4.2)

Let P be prime ideal. Then: For all ideals I and J, $P \supseteq IJ$ implies $P \supseteq I$ or $P \supseteq J$.

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. *$A \supseteq B$ if and only if $A|B$.*
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

The first consequence in the above proposition is immediate from the main statement. For the second, pick $0 \neq a \in A$. Then $A|(a)$ and so $(a) = AA'$ for some ideal A'. This gives $(a)B = (a)C$; hence $B = C$.

We move on to the proof of Dedekind's Theorem; we will finish off proposition 3.1 later on. But first an observation (the proof is left as an exercise).

Lemma (4.2)

Let P be prime ideal. Then: For all ideals I and J, $P \supseteq IJ$ implies $P \supseteq I$ or $P \supseteq J$.

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. *$A \supseteq B$ if and only if $A|B$.*
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

The first consequence in the above proposition is immediate from the main statement. For the second, pick $0 \neq a \in A$. Then $A|(a)$ and so $(a) = AA'$ for some ideal A'. This gives $(a)B = (a)C$; hence $B = C$.

We move on to the proof of Dedekind's Theorem; we will finish off proposition 3.1 later on. But first an observation (the proof is left as an exercise).

Lemma (4.2)

Let P be prime ideal. Then: For all ideals I and J, $P \supseteq IJ$ implies $P \supseteq I$ or $P \supseteq J$.

K is a number field and $\mathcal{O}$ its integer ring.

Definition

An ideal A divides an ideal B, written $A|B$, if $B = AC$ for some ideal C.

Proposition (4.1)

If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Consequently:

1. *$A \supseteq B$ if and only if $A|B$.*
2. *(Cancellation laws:) Suppose A, B, C are ideals of $\mathcal{O}$. If $AB = AC$ and $A \neq (0)$, then $B = C$.*

The first consequence in the above proposition is immediate from the main statement. For the second, pick $0 \neq a \in A$. Then $A|(a)$ and so $(a) = AA'$ for some ideal A'. This gives $(a)B = (a)C$; hence $B = C$.

We move on to the proof of Dedekind's Theorem; we will finish off proposition 3.1 later on. But first an observation (the proof is left as an exercise).

Lemma (4.2)

Let P be prime ideal. Then: For all ideals I and J, $P \supseteq IJ$ implies $P \supseteq I$ or $P \supseteq J$.

We want to show that every proper non-zero ideal of $\mathcal{O}$ is uniquely a product of prime ideals.

Existence: Suppose false, and pick I maximal in the non-empty set of non-zero proper ideals which cannot be written as a product of prime ideals. Then $I \subseteq P$ for some prime P, and we can then write $I = PJ$. Note that J is non-zero, proper (otherwise $I = P$) and $I \subseteq J$. If $I \neq J$ then we can write J as a product of primes and we are done. So $I = J$ and $I\mathcal{O} = IP$, which gives $P = \mathcal{O}$—contradiction.

We want to show that every proper non-zero ideal of $\mathcal{O}$ is uniquely a product of prime ideals.

Existence: Suppose false, and pick I maximal in the non-empty set of non-zero proper ideals which cannot be written as a product of prime ideals. Then $I \subseteq P$ for some prime P, and we can then write $I = PJ$. Note that J is non-zero, proper (otherwise $I = P$) and $I \subseteq J$. If $I \neq J$ then we can write J as a product of primes and we are done. So $I = J$ and $I\mathcal{O} = IP$, which gives $P = \mathcal{O}$—contradiction.

Uniqueness: Suppose $P_1 \dots P_r = Q_1 \dots Q_s$ where P_i's and Q_i's are non-zero prime ideals of $\mathcal{O}$. Using lemma 3.2 we can assume $P_1 \subseteq Q_1$ and because non-zero primes are maximal $P_1 = Q_1$.

We want to show that every proper non-zero ideal of $\mathcal{O}$ is uniquely a product of prime ideals.

Existence: Suppose false, and pick I maximal in the non-empty set of non-zero proper ideals which cannot be written as a product of prime ideals. Then $I \subseteq P$ for some prime P, and we can then write $I = PJ$. Note that J is non-zero, proper (otherwise $I = P$) and $I \subseteq J$. If $I \neq J$ then we can write J as a product of primes and we are done. So $I = J$ and $I\mathcal{O} = IP$, which gives $P = \mathcal{O}$—contradiction.

Uniqueness: Suppose $P_1 \dots P_r = Q_1 \dots Q_s$ where P_i's and Q_i's are non-zero prime ideals of $\mathcal{O}$. Using lemma 3.2 we can assume $P_1 \subseteq Q_1$ and because non-zero primes are maximal $P_1 = Q_1$. Cancellation then gives $P_2 \dots P_r = Q_2 \dots Q_s$.

We want to show that every proper non-zero ideal of $\mathcal{O}$ is uniquely a product of prime ideals.

Existence: Suppose false, and pick I maximal in the non-empty set of non-zero proper ideals which cannot be written as a product of prime ideals. Then $I \subseteq P$ for some prime P, and we can then write $I = PJ$. Note that J is non-zero, proper (otherwise $I = P$) and $I \subseteq J$. If $I \neq J$ then we can write J as a product of primes and we are done. So $I = J$ and $I\mathcal{O} = IP$, which gives $P = \mathcal{O}$—contradiction.

Uniqueness: Suppose $P_1 \ldots P_r = Q_1 \ldots Q_s$ where P_i's and Q_i's are non-zero prime ideals of $\mathcal{O}$. Using lemma 3.2 we can assume $P_1 \subseteq Q_1$ and because non-zero primes are maximal $P_1 = Q_1$. Cancellation then gives $P_2 \ldots P_r = Q_2 \ldots Q_s$. A straightforward induction completes the proof.

We want to show that every proper non-zero ideal of $\mathcal{O}$ is uniquely a product of prime ideals.

Existence: Suppose false, and pick I maximal in the non-empty set of non-zero proper ideals which cannot be written as a product of prime ideals. Then $I \subseteq P$ for some prime P, and we can then write $I = PJ$. Note that J is non-zero, proper (otherwise $I = P$) and $I \subseteq J$. If $I \neq J$ then we can write J as a product of primes and we are done. So $I = J$ and $I\mathcal{O} = IP$, which gives $P = \mathcal{O}$—contradiction.

Uniqueness: Suppose $P_1 \ldots P_r = Q_1 \ldots Q_s$ where P_i's and Q_i's are non-zero prime ideals of $\mathcal{O}$. Using lemma 3.2 we can assume $P_1 \subseteq Q_1$ and because non-zero primes are maximal $P_1 = Q_1$. Cancellation then gives $P_2 \ldots P_r = Q_2 \ldots Q_s$. A straightforward induction completes the proof.

We want to show that every proper non-zero ideal of $\mathcal{O}$ is uniquely a product of prime ideals.

Existence: Suppose false, and pick I maximal in the non-empty set of non-zero proper ideals which cannot be written as a product of prime ideals. Then $I \subseteq P$ for some prime P, and we can then write $I = PJ$. Note that J is non-zero, proper (otherwise $I = P$) and $I \subseteq J$. If $I \neq J$ then we can write J as a product of primes and we are done. So $I = J$ and $I\mathcal{O} = IP$, which gives $P = \mathcal{O}$—contradiction.

Uniqueness: Suppose $P_1 \dots P_r = Q_1 \dots Q_s$ where P_i's and Q_i's are non-zero prime ideals of $\mathcal{O}$. Using lemma 3.2 we can assume $P_1 \subseteq Q_1$ and because non-zero primes are maximal $P_1 = Q_1$. Cancellation then gives $P_2 \dots P_r = Q_2 \dots Q_s$. A straightforward induction completes the proof.

We want to show that every proper non-zero ideal of $\mathcal{O}$ is uniquely a product of prime ideals.

Existence: Suppose false, and pick I maximal in the non-empty set of non-zero proper ideals which cannot be written as a product of prime ideals. Then $I \subseteq P$ for some prime P, and we can then write $I = PJ$. Note that J is non-zero, proper (otherwise $I = P$) and $I \subseteq J$. If $I \neq J$ then we can write J as a product of primes and we are done. So $I = J$ and $I\mathcal{O} = IP$, which gives $P = \mathcal{O}$—contradiction.

Uniqueness: Suppose $P_1 \ldots P_r = Q_1 \ldots Q_s$ where P_i's and Q_i's are non-zero prime ideals of $\mathcal{O}$. Using lemma 3.2 we can assume $P_1 \subseteq Q_1$ and because non-zero primes are maximal $P_1 = Q_1$. Cancellation then gives $P_2 \ldots P_r = Q_2 \ldots Q_s$. A straightforward induction completes the proof.

Example: What happened in $\mathbb{Z}[\sqrt{-5}]$? Recall that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

so unique factorisation into irreducible elements does not hold. Now set

$$P = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5}),$$
$$Q_1 = (3, 1 + \sqrt{-5}), \quad \text{and}$$
$$Q_2 = (3, 1 - \sqrt{-5}).$$

Then (exercise): P, Q_1, Q_2 are prime ideals, and $(2) = P^2$, $(3) = Q_1 Q_2$, while $(1 + \sqrt{-5}) = PQ_1$ and $(1 - \sqrt{-5}) = PQ_2$, so the apparently different factorisations just become $P^2 Q_1 Q_2 = PQ_1 PQ_2$, i.e. a rearrangement of ideal factors.

Example: What happened in $\mathbb{Z}[\sqrt{-5}]$? Recall that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

so unique factorisation into irreducible elements does not hold. Now set

$$\begin{aligned} P &= (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5}), \\ Q_1 &= (3, 1 + \sqrt{-5}), \quad \text{and} \\ Q_2 &= (3, 1 - \sqrt{-5}). \end{aligned}$$

Then (exercise): P, Q_1, Q_2 are prime ideals, and $(2) = P^2$, $(3) = Q_1 Q_2$, while $(1 + \sqrt{-5}) = PQ_1$ and $(1 - \sqrt{-5}) = PQ_2$, so the apparently different factorisations just become $P^2 Q_1 Q_2 = PQ_1 PQ_2$, i.e. a rearrangement of ideal factors.

Example: What happened in $\mathbb{Z}[\sqrt{-5}]$? Recall that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

so unique factorisation into irreducible elements does not hold. Now set

$$\begin{aligned} P &= (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5}), \\ Q_1 &= (3, 1 + \sqrt{-5}), \quad \text{and} \\ Q_2 &= (3, 1 - \sqrt{-5}). \end{aligned}$$

Then (exercise): P, Q_1, Q_2 are prime ideals, and $(2) = P^2$, $(3) = Q_1 Q_2$, while $(1 + \sqrt{-5}) = PQ_1$ and $(1 - \sqrt{-5}) = PQ_2$, so the apparently different factorisations just become $P^2 Q_1 Q_2 = PQ_1 PQ_2$, i.e. a rearrangement of ideal factors.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Key result: There is a $\alpha \in K \setminus \mathcal{O}$ such that $\dfrac{\alpha}{a}AC \subseteq \mathcal{O}$.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Key result: There is a $\alpha \in K \setminus \mathcal{O}$ such that $\dfrac{\alpha}{a}AC \subseteq \mathcal{O}$.

Assuming the above, we can finish off the proof. Suppose $c \in C$. Then $\alpha c = \frac{\alpha}{a}ac \in \mathcal{O}$. Also $\alpha c A = a(\frac{\alpha}{a})cA \subseteq (a)$, so $\alpha c \in C$.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Key result: There is a $\alpha \in K \setminus \mathcal{O}$ such that $\dfrac{\alpha}{a}AC \subseteq \mathcal{O}$.

Assuming the above, we can finish off the proof. Suppose $c \in C$. Then $\alpha c = \frac{\alpha}{a}ac \in \mathcal{O}$. Also $\alpha c A = a(\frac{\alpha}{a})cA \subseteq (a)$, so $\alpha c \in C$. This gives $\alpha C \subseteq C$.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Key result: There is a $\alpha \in K \setminus \mathcal{O}$ such that $\dfrac{\alpha}{a}AC \subseteq \mathcal{O}$.

Assuming the above, we can finish off the proof. Suppose $c \in C$. Then $\alpha c = \frac{\alpha}{a}ac \in \mathcal{O}$. Also $\alpha c A = a(\frac{\alpha}{a})cA \subseteq (a)$, so $\alpha c \in C$. This gives $\alpha C \subseteq C$. Since C is a finitely generated non-zero submodule of K, therefore $\alpha \in \mathcal{O}$—contradiction.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Key result: There is a $\alpha \in K \setminus \mathcal{O}$ such that $\dfrac{\alpha}{a}AC \subseteq \mathcal{O}$.

Assuming the above, we can finish off the proof. Suppose $c \in C$. Then $\alpha c = \frac{\alpha}{a}ac \in \mathcal{O}$. Also $\alpha c A = a(\frac{\alpha}{a})cA \subseteq (a)$, so $\alpha c \in C$. This gives $\alpha C \subseteq C$. Since C is a finitely generated non-zero submodule of K, therefore $\alpha \in \mathcal{O}$—contradiction.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Key result: There is a $\alpha \in K \setminus \mathcal{O}$ such that $\dfrac{\alpha}{a}AC \subseteq \mathcal{O}$.

Assuming the above, we can finish off the proof. Suppose $c \in C$. Then $\alpha c = \frac{\alpha}{a}ac \in \mathcal{O}$. Also $\alpha c A = a(\frac{\alpha}{a})cA \subseteq (a)$, so $\alpha c \in C$. This gives $\alpha C \subseteq C$. Since C is a finitely generated non-zero submodule of K, therefore $\alpha \in \mathcal{O}$—contradiction.

Now return to main part of proposition 3.1: If A, B are ideals of $\mathcal{O}$ and $A \supseteq B$, then there exists an ideal C such that $B = AC$. Now without any loss of generality, A is a non-zero proper ideal. Secondly, it suffices to prove it in the case when B is a principal ideal (because B is finitely generated). So we prove: Suppose $0 \neq a \in A \neq \mathcal{O}$. Then $(a) = AC$ for some ideal.

To do this, first define $C := \{x \in \mathcal{O} \mid Ax \subseteq (a)\}$. Then C is an ideal of $\mathcal{O}$ and $AC \subseteq (a)$. Assume $AC \neq (a)$; so $\frac{1}{a}AC$ is a proper ideal of $\mathcal{O}$.

Key result: There is a $\alpha \in K \setminus \mathcal{O}$ such that $\dfrac{\alpha}{a}AC \subseteq \mathcal{O}$.

Assuming the above, we can finish off the proof. Suppose $c \in C$. Then $\alpha c = \frac{\alpha}{a}ac \in \mathcal{O}$. Also $\alpha cA = a(\frac{\alpha}{a})cA \subseteq (a)$, so $\alpha c \in C$. This gives $\alpha C \subseteq C$. Since C is a finitely generated non-zero submodule of K, therefore $\alpha \in \mathcal{O}$—contradiction.

Lemma (4.3)

Let I be a proper ideal of $\mathcal{O}$. Then there is an $\alpha \in K \setminus \mathcal{O}$ such that $\alpha I \subseteq \mathcal{O}$.

Proof.

Because every proper ideal is contained in a maximal ideal, we may assume that $I = P$ is a non-zero prime ideal. Now choose $0 \neq a \in P$ with $(a) \neq P$. We then have $(a) \supseteq P_1 \dots P_r$ with P_i's non-zero primes and $r \geq 1$ chosen to be minimal. By lemma 4.2 we can assume $P = P_1$. Now as $(a) \neq P$ we get $r \geq 2$ and the minimality of r then implies (a) does not contain $P_2 \dots P_n$. Hence we can find $y \in P_2 \dots P_n \setminus (a)$.

Lemma (4.3)

Let I be a proper ideal of $\mathcal{O}$. Then there is an $\alpha \in K \setminus \mathcal{O}$ such that $\alpha I \subseteq \mathcal{O}$.

Proof.

Because every proper ideal is contained in a maximal ideal, we may assume that $I = P$ is a non-zero prime ideal. Now choose $0 \neq a \in P$ with $(a) \neq P$. We then have $(a) \supseteq P_1 \dots P_r$ with P_i's non-zero primes and $r \geq 1$ chosen to be minimal. By lemma 4.2 we can assume $P = P_1$. Now as $(a) \neq P$ we get $r \geq 2$ and the minimality of r then implies (a) does not contain $P_2 \dots P_n$. Hence we can find $y \in P_2 \dots P_n \setminus (a)$.
Take $\alpha := y/a$. Then $\alpha \in K \setminus \mathcal{O}$. Also if $x \in P$ then $\alpha x = xy/a \in \mathcal{O}$. $\square$

Lemma (4.3)

Let I be a proper ideal of $\mathcal{O}$. Then there is an $\alpha \in K \setminus \mathcal{O}$ such that $\alpha I \subseteq \mathcal{O}$.

Proof.

Because every proper ideal is contained in a maximal ideal, we may assume that $I = P$ is a non-zero prime ideal. Now choose $0 \neq a \in P$ with $(a) \neq P$. We then have $(a) \supseteq P_1 \dots P_r$ with P_i's non-zero primes and $r \geq 1$ chosen to be minimal. By lemma 4.2 we can assume $P = P_1$. Now as $(a) \neq P$ we get $r \geq 2$ and the minimality of r then implies (a) does not contain $P_2 \dots P_n$. Hence we can find $y \in P_2 \dots P_n \setminus (a)$.

Take $\alpha := y/a$. Then $\alpha \in K \setminus \mathcal{O}$. Also if $x \in P$ then $\alpha x = xy/a \in \mathcal{O}$. □

Lemma (4.3)

Let I be a proper ideal of $\mathcal{O}$. Then there is an $\alpha \in K \setminus \mathcal{O}$ such that $\alpha I \subseteq \mathcal{O}$.

Proof.

Because every proper ideal is contained in a maximal ideal, we may assume that $I = P$ is a non-zero prime ideal. Now choose $0 \neq a \in P$ with $(a) \neq P$. We then have $(a) \supseteq P_1 \ldots P_r$ with P_i's non-zero primes and $r \geq 1$ chosen to be minimal. By lemma 4.2 we can assume $P = P_1$. Now as $(a) \neq P$ we get $r \geq 2$ and the minimality of r then implies (a) does not contain $P_2 \ldots P_n$. Hence we can find $y \in P_2 \ldots P_n \setminus (a)$.
Take $\alpha := y/a$. Then $\alpha \in K \setminus \mathcal{O}$. Also if $x \in P$ then $\alpha x = xy/a \in \mathcal{O}$. □

Lemma (4.3)

Let I be a proper ideal of $\mathcal{O}$. Then there is an $\alpha \in K \setminus \mathcal{O}$ such that $\alpha I \subseteq \mathcal{O}$.

Proof.

Because every proper ideal is contained in a maximal ideal, we may assume that $I = P$ is a non-zero prime ideal. Now choose $0 \neq a \in P$ with $(a) \neq P$. We then have $(a) \supseteq P_1 \dots P_r$ with P_i's non-zero primes and $r \geq 1$ chosen to be minimal. By lemma 4.2 we can assume $P = P_1$. Now as $(a) \neq P$ we get $r \geq 2$ and the minimality of r then implies (a) does not contain $P_2 \dots P_n$. Hence we can find $y \in P_2 \dots P_n \setminus (a)$.
Take $\alpha := y/a$. Then $\alpha \in K \setminus \mathcal{O}$. Also if $x \in P$ then $\alpha x = xy/a \in \mathcal{O}$. □

We can now exploit the equivalence of divisibility and containment, and unique factorization into ideals to record the following: Suppose I and J are non-zero ideals of $\mathcal{O}$ with factorization

$$I = P_1^{i_1} \dots P_k^{i_k} \quad \text{and} \quad J = P_1^{j_1} \dots P_k^{j_k}$$

where the powers are allowed to be zero. The highest common factor of I and J is an ideal that divides I and J with the additional property that any other ideal that divides I and J must divide it. The hcf is therefore $I + J$. Likewise the least common multiple of I and J is $I \cap J$. It is then easy to check that

$$I + J = P_1^{\min(i_1, j_1)} \dots P_k^{\min(i_k, j_k)} \quad \text{and} \quad I \cap J = P_1^{\max(i_1, j_1)} \dots P_k^{\max(i_k, j_k)}.$$

We can now exploit the equivalence of divisibility and containment, and unique factorization into ideals to record the following: Suppose I and J are non-zero ideals of $\mathcal{O}$ with factorization

$$I = P_1^{i_1} \dots P_k^{i_k} \quad \text{and} \quad J = P_1^{j_1} \dots P_k^{j_k}$$

where the powers are allowed to be zero. The highest common factor of I and J is an ideal that divides I and J with the additional property that any other ideal that divides I and J must divide it. The hcf is therefore $I + J$. Likewise the least common multiple of I and J is $I \cap J$. It is then easy to check that

$$I + J = P_1^{\min(i_1, j_1)} \dots P_k^{\min(i_k, j_k)} \quad \text{and} \quad I \cap J = P_1^{\max(i_1, j_1)} \dots P_k^{\max(i_k, j_k)}.$$

Suppose now I and J are coprime i.e. $I + J = \mathcal{O}$. Then $I \cap J = IJ$, and we obtain

$$\mathcal{O}/IJ \cong \mathcal{O}/I \times \mathcal{O}/J.$$

We can now exploit the equivalence of divisibility and containment, and unique factorization into ideals to record the following: Suppose I and J are non-zero ideals of $\mathcal{O}$ with factorization

$$I = P_1^{i_1} \dots P_k^{i_k} \quad \text{and} \quad J = P_1^{j_1} \dots P_k^{j_k}$$

where the powers are allowed to be zero. The highest common factor of I and J is an ideal that divides I and J with the additional property that any other ideal that divides I and J must divide it. The hcf is therefore $I + J$. Likewise the least common multiple of I and J is $I \cap J$. It is then easy to check that

$$I + J = P_1^{\min(i_1, j_1)} \dots P_k^{\min(i_k, j_k)} \quad \text{and} \quad I \cap J = P_1^{\max(i_1, j_1)} \dots P_k^{\max(i_k, j_k)}.$$

Suppose now I and J are coprime i.e. $I + J = \mathcal{O}$. Then $I \cap J = IJ$, and we obtain

$$\mathcal{O}/IJ \cong \mathcal{O}/I \times \mathcal{O}/J.$$

An induction argument then shows

Proposition (Chinese remainder theorem)

If $I_1, \dots, I_k$ are pairwise coprime ideals of $\mathcal{O}$ then $I_1 \cap \dots I_k = I_1 \dots I_k$ and

$$\mathcal{O}/I_1 \dots I_k \cong \mathcal{O}/I_1 \times \dots \times \mathcal{O}/I_k.$$

We can now exploit the equivalence of divisibility and containment, and unique factorization into ideals to record the following: Suppose I and J are non-zero ideals of $\mathcal{O}$ with factorization

$$I = P_1^{i_1} \dots P_k^{i_k} \quad \text{and} \quad J = P_1^{j_1} \dots P_k^{j_k}$$

where the powers are allowed to be zero. The highest common factor of I and J is an ideal that divides I and J with the additional property that any other ideal that divides I and J must divide it. The hcf is therefore $I + J$. Likewise the least common multiple of I and J is $I \cap J$. It is then easy to check that

$$I + J = P_1^{\min(i_1, j_1)} \dots P_k^{\min(i_k, j_k)} \quad \text{and} \quad I \cap J = P_1^{\max(i_1, j_1)} \dots P_k^{\max(i_k, j_k)}.$$

Suppose now I and J are coprime i.e. $I + J = \mathcal{O}$. Then $I \cap J = IJ$, and we obtain

$$\mathcal{O}/IJ \cong \mathcal{O}/I \times \mathcal{O}/J.$$

An induction argument then shows

Proposition (Chinese remainder theorem)

If $I_1, \dots, I_k$ are pairwise coprime ideals of $\mathcal{O}$ then $I_1 \cap \dots I_k = I_1 \dots I_k$ and

$$\mathcal{O}/I_1 \dots I_k \cong \mathcal{O}/I_1 \times \dots \times \mathcal{O}/I_k.$$

We can now exploit the equivalence of divisibility and containment, and unique factorization into ideals to record the following: Suppose I and J are non-zero ideals of $\mathcal{O}$ with factorization

$$I = P_1^{i_1} \dots P_k^{i_k} \quad \text{and} \quad J = P_1^{j_1} \dots P_k^{j_k}$$

where the powers are allowed to be zero. The highest common factor of I and J is an ideal that divides I and J with the additional property that any other ideal that divides I and J must divide it. The hcf is therefore $I + J$. Likewise the least common multiple of I and J is $I \cap J$. It is then easy to check that

$$I + J = P_1^{\min(i_1,j_1)} \dots P_k^{\min(i_k,j_k)} \quad \text{and} \quad I \cap J = P_1^{\max(i_1,j_1)} \dots P_k^{\max(i_k,j_k)}.$$

Suppose now I and J are coprime i.e. $I + J = \mathcal{O}$. Then $I \cap J = IJ$, and we obtain

$$\mathcal{O}/IJ \cong \mathcal{O}/I \times \mathcal{O}/J.$$

An induction argument then shows

Proposition (Chinese remainder theorem)

If $I_1, \dots, I_k$ are pairwise coprime ideals of $\mathcal{O}$ then $I_1 \cap \dots I_k = I_1 \dots I_k$ and

$$\mathcal{O}/I_1 \dots I_k \cong \mathcal{O}/I_1 \times \dots \times \mathcal{O}/I_k.$$

We can now exploit the equivalence of divisibility and containment, and unique factorization into ideals to record the following: Suppose I and J are non-zero ideals of $\mathcal{O}$ with factorization

$$I = P_1^{i_1} \dots P_k^{i_k} \quad \text{and} \quad J = P_1^{j_1} \dots P_k^{j_k}$$

where the powers are allowed to be zero. The highest common factor of I and J is an ideal that divides I and J with the additional property that any other ideal that divides I and J must divide it. The hcf is therefore $I + J$. Likewise the least common multiple of I and J is $I \cap J$. It is then easy to check that

$$I + J = P_1^{\min(i_1,j_1)} \dots P_k^{\min(i_k,j_k)} \quad \text{and} \quad I \cap J = P_1^{\max(i_1,j_1)} \dots P_k^{\max(i_k,j_k)}.$$

Suppose now I and J are coprime i.e. $I + J = \mathcal{O}$. Then $I \cap J = IJ$, and we obtain

$$\mathcal{O}/IJ \cong \mathcal{O}/I \times \mathcal{O}/J.$$

An induction argument then shows

Proposition (Chinese remainder theorem)

If $I_1, \dots, I_k$ are pairwise coprime ideals of $\mathcal{O}$ then $I_1 \cap \dots I_k = I_1 \dots I_k$ and

$$\mathcal{O}/I_1 \dots I_k \cong \mathcal{O}/I_1 \times \dots \times \mathcal{O}/I_k.$$

It follows from the chinese remainder theorem that the norm (of an ideal) is multiplicative: if I, J are non-zero coprime ideals of $\mathcal{O}$ then $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Lemma (4.4)

Let P be a non-zero prime ideal of $\mathcal{O}$. Then $|\mathcal{O}/P| = |P^k/P^{k+1}|$ for any $k \geq 1$. Consequently $N(P^k) = (N(P))^k$ for all $k \geq 1$.

Proof.
Use uniqueness of factorization: $P^k \neq P^{k+1}$, and if we pick $a \in P^k \setminus P^{k+1}$ then $P^k = (a) + P^{k+1}$. Consequently the $\mathcal{O}$ module homomorphism $\mathcal{O} \to P^k/P^{k+1}$ given by $x \to ax \pmod{P^{k+1}}$ is surjective. Since the kernel contains P and 1 is not in the kernel, it must be P. $\square$

Corollary (4.5)

The norm is completely multiplicative: If I and J are non-zero ideals of $\mathcal{O}$ then $N(IJ) = N(I)N(J)$.

It follows from the chinese remainder theorem that the norm (of an ideal) is multiplicative: if I, J are non-zero coprime ideals of $\mathcal{O}$ then $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Lemma (4.4)

Let P be a non-zero prime ideal of $\mathcal{O}$. Then $|\mathcal{O}/P| = |P^k/P^{k+1}|$ for any $k \geq 1$. Consequently $N(P^k) = (N(P))^k$ for all $k \geq 1$.

Proof.

Use uniqueness of factorization: $P^k \neq P^{k+1}$, and if we pick $a \in P^k \setminus P^{k+1}$ then $P^k = (a) + P^{k+1}$. Consequently the $\mathcal{O}$ module homomorphism $\mathcal{O} \to P^k/P^{k+1}$ given by $x \to ax \pmod{P^{k+1}}$ is surjective. Since the kernel contains P and 1 is not in the kernel, it must be P. □

Corollary (4.5)

The norm is completely multiplicative: If I and J are non-zero ideals of $\mathcal{O}$ then $N(IJ) = N(I)N(J)$.

It follows from the chinese remainder theorem that the norm (of an ideal) is multiplicative: if I, J are non-zero coprime ideals of $\mathcal{O}$ then $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Lemma (4.4)

Let P be a non-zero prime ideal of $\mathcal{O}$. Then $|\mathcal{O}/P| = |P^k/P^{k+1}|$ for any $k \geq 1$. Consequently $N(P^k) = (N(P))^k$ for all $k \geq 1$.

Proof.

Use uniqueness of factorization: $P^k \neq P^{k+1}$, and if we pick $a \in P^k \setminus P^{k+1}$ then $P^k = (a) + P^{k+1}$. Consequently the $\mathcal{O}$ module homomorphism $\mathcal{O} \to P^k/P^{k+1}$ given by $x \to ax \pmod{P^{k+1}}$ is surjective. Since the kernel contains P and 1 is not in the kernel, it must be P. $\square$

Corollary (4.5)

The norm is completely multiplicative: If I and J are non-zero ideals of $\mathcal{O}$ then $N(IJ) = N(I)N(J)$.

It follows from the chinese remainder theorem that the norm (of an ideal) is multiplicative: if I, J are non-zero coprime ideals of $\mathcal{O}$ then $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Lemma (4.4)

Let P be a non-zero prime ideal of $\mathcal{O}$. Then $|\mathcal{O}/P| = |P^k/P^{k+1}|$ for any $k \geq 1$. Consequently $N(P^k) = (N(P))^k$ for all $k \geq 1$.

Proof.

Use uniqueness of factorization: $P^k \neq P^{k+1}$, and if we pick $a \in P^k \setminus P^{k+1}$ then $P^k = (a) + P^{k+1}$. Consequently the $\mathcal{O}$ module homomorphism $\mathcal{O} \to P^k/P^{k+1}$ given by $x \to ax \pmod{P^{k+1}}$ is surjective. Since the kernel contains P and 1 is not in the kernel, it must be P. □

Corollary (4.5)

The norm is completely multiplicative: If I and J are non-zero ideals of $\mathcal{O}$ then $N(IJ) = N(I)N(J)$.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K : \mathbb{Q}] = n$.

If P is a non-zero prime ideal of $\mathcal{O}$, then $P \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$, necessarily of the form $p\mathbb{Z}$ for some rational prime p. Hence P lies above p: $P \supseteq pO_K$, i.e. $P \mid (p)$, and P must occur in the factorisation of (p) in $\mathcal{O}$. So:

- $\mathbf{N}(P) = p^f$ for some $f \geq 1$. The index f is called the inertial degree of P. Note that the inertial degree is the degree of the finite field $\mathcal{O}/P$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- $P^e \mid (p)$ but $P^{e+1} \nmid (p)$ for some $e \geq 1$. The index e is the ramification index of P.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K : \mathbb{Q}] = n$.

If P is a non-zero prime ideal of $\mathcal{O}$, then $P \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$, necessarily of the form $p\mathbb{Z}$ for some rational prime p. Hence P lies above p: $P \supseteq pO_K$, i.e. $P \mid (p)$, and P must occur in the factorisation of (p) in $\mathcal{O}$. So:

- $\mathbf{N}(P) = p^f$ for some $f \geq 1$. The index f is called the inertial degree of P. Note that the inertial degree is the degree of the finite field $\mathcal{O}/P$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- $P^e \mid (p)$ but $P^{e+1} \nmid (p)$ for some $e \geq 1$. The index e is the ramification index of P.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K : \mathbb{Q}] = n$.

If P is a non-zero prime ideal of $\mathcal{O}$, then $P \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$, necessarily of the form $p\mathbb{Z}$ for some rational prime p. Hence P lies above p: $P \supseteq pO_K$, i.e. $P \mid (p)$, and P must occur in the factorisation of (p) in $\mathcal{O}$. So:

- $\mathbf{N}(P) = p^f$ for some $f \geq 1$. The index f is called the inertial degree of P. Note that the inertial degree is the degree of the finite field $\mathcal{O}/P$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- $P^e \mid (p)$ but $P^{e+1} \nmid (p)$ for some $e \geq 1$. The index e is the ramification index of P.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K:\mathbb{Q}] = n$.

If P is a non-zero prime ideal of $\mathcal{O}$, then $P \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$, necessarily of the form $p\mathbb{Z}$ for some rational prime p. Hence P lies above p: $P \supseteq pO_K$, i.e. $P \mid (p)$, and P must occur in the factorisation of (p) in $\mathcal{O}$. So:

- $\mathbf{N}(P) = p^f$ for some $f \geq 1$. The index f is called the inertial degree of P. Note that the inertial degree is the degree of the finite field $\mathcal{O}/P$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- $P^e \mid (p)$ but $P^{e+1} \nmid (p)$ for some $e \geq 1$. The index e is the ramification index of P.

Now let p be a rational prime and consider factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k},$$

where the P_i's are the distinct prime ideals of $\mathcal{O}$ over p. Let f_i be the inertial degree of P_i.

- We say that the extension $K/\mathbb{Q}$ is unramified at p, or simply p is unramified, if all the ramification indices e_i are 1. If some $e_i \geq 2$ then p is ramified.
- If $e_1 = \dots = e_k = f_1 = \dots = f_k = 1$ then we say p splits completely in K.
- We say that p is inert if (p) is a prime ideal of $\mathcal{O}$.

Now let p be a rational prime and consider factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k},$$

where the P_i's are the distinct prime ideals of $\mathcal{O}$ over p. Let f_i be the inertial degree of P_i.

- We say that the extension $K/\mathbb{Q}$ is unramified at p, or simply p is unramified, if all the ramification indices e_i are 1. If some $e_i \geq 2$ then p is ramified.
- If $e_1 = \dots = e_k = f_1 = \dots = f_k = 1$ then we say p splits completely in K.
- We say that p is inert if (p) is a prime ideal of $\mathcal{O}$.
- Taking norms we get $p^n = \mathbf{N}(P_1)^{e_1} \dots \mathbf{N}(P_k)^{e_k}$. Using $\mathbf{N}(P_i) = p^{f_i}$, we get the following **degree-ramification formula**:

$$n = e_1 f_1 + \dots + e_k f_k.$$

Now let p be a rational prime and consider factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k},$$

where the P_i's are the distinct prime ideals of $\mathcal{O}$ over p. Let f_i be the inertial degree of P_i.

- We say that the extension $K/\mathbb{Q}$ is unramified at p, or simply p is unramified, if all the ramification indices e_i are 1. If some $e_i \geq 2$ then p is ramified.
- If $e_1 = \dots = e_k = f_1 = \dots = f_k = 1$ then we say p splits completely in K.
- We say that p is inert if (p) is a prime ideal of $\mathcal{O}$.
- Taking norms we get $p^n = \mathbf{N}(P_1)^{e_1} \dots \mathbf{N}(P_k)^{e_k}$. Using $\mathbf{N}(P_i) = p^{f_i}$, we get the following **degree-ramification formula**:

$$n = e_1 f_1 + \dots + e_k f_k.$$

Now let p be a rational prime and consider factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k},$$

where the P_i's are the distinct prime ideals of $\mathcal{O}$ over p. Let f_i be the inertial degree of P_i.

- We say that the extension $K/\mathbb{Q}$ is unramified at p, or simply p is unramified, if all the ramification indices e_i are 1. If some $e_i \geq 2$ then p is ramified.
- If $e_1 = \dots = e_k = f_1 = \dots = f_k = 1$ then we say p splits completely in K.
- We say that p is inert if (p) is a prime ideal of $\mathcal{O}$.
- Taking norms we get $p^n = \mathbf{N}(P_1)^{e_1} \dots \mathbf{N}(P_k)^{e_k}$. Using $\mathbf{N}(P_i) = p^{f_i}$, we get the following **degree-ramification formula**:

$$n = e_1 f_1 + \dots + e_k f_k.$$

Now let p be a rational prime and consider factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k},$$

where the P_i's are the distinct prime ideals of $\mathcal{O}$ over p. Let f_i be the inertial degree of P_i.

- We say that the extension $K/\mathbb{Q}$ is unramified at p, or simply p is unramified, if all the ramification indices e_i are 1. If some $e_i \geq 2$ then p is ramified.
- If $e_1 = \dots = e_k = f_1 = \dots = f_k = 1$ then we say p splits completely in K.
- We say that p is inert if (p) is a prime ideal of $\mathcal{O}$.
- Taking norms we get $p^n = \mathbf{N}(P_1)^{e_1} \dots \mathbf{N}(P_k)^{e_k}$. Using $\mathbf{N}(P_i) = p^{f_i}$, we get the following **degree-ramification formula**:

$$n = e_1 f_1 + \dots + e_k f_k.$$

Theorem (5.1)

Suppose $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}$ and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, necessarily of degree n. Suppose we are given a rational prime p which we want to factorise in $\mathcal{O}$.

Choose monic polynomials $g_1(x), \ldots, g_k(x) \in \mathbb{Z}[x]$ such that the $\overline{g_i}$'s, the mod p reduction of g_i's, are the distinct irreducible factors of $\overline{f}(x) \in \mathbb{F}_p[x]$ and we have the factorisation

$$\overline{f}(x) = \overline{g_1}(x)^{e_1} \ldots \overline{g_k}(x)^{e_k}.$$

Assume that p does not divide $[\mathcal{O} : \mathbb{Z}[\alpha]]$, the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}$. Then each $P_i := (p, g_i(\alpha))$ is a prime ideal of $\mathcal{O}$; $P_1, \ldots, P_k$ are the prime ideals of $\mathcal{O}$ dividing p and we have the factorisation

$$(p) = P_1^{e_1} \ldots P_k^{e_k}.$$

Theorem (5.1)

Suppose $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}$ and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, necessarily of degree n. Suppose we are given a rational prime p which we want to factorise in $\mathcal{O}$.
Choose monic polynomials $g_1(x), \dots, g_k(x) \in \mathbb{Z}[x]$ such that the $\overline{g_i}$'s, the mod p reduction of g_i's, are the distinct irreducible factors of $\overline{f}(x) \in \mathbb{F}_p[x]$ and we have the factorisation

$$\overline{f}(x) = \overline{g_1}(x)^{e_1} \dots \overline{g_k}(x)^{e_k}.$$

Assume that p does not divide $[\mathcal{O} : \mathbb{Z}[\alpha]]$, the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}$. Then each $P_i := (p, g_i(\alpha))$ is a prime ideal of $\mathcal{O}$; $P_1, \dots, P_k$ are the prime ideals of $\mathcal{O}$ dividing p and we have the factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k}.$$

Proof.

- $p \nmid [\mathcal{O} : \mathbb{Z}[\alpha]]$, so if $\beta \in O_K$ and $p\beta \in \mathbb{Z}[\alpha]$ then $\beta \in \mathbb{Z}[\alpha]$. Consequently the kernel of the natural homomorphism $\mathbb{Z}[\alpha] \to \mathcal{O}/p\mathcal{O}$ is precisely $p\mathbb{Z}[\alpha]$, and we get an injection $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}/p\mathcal{O}$. Both sides have order p^n, so this must be an isomorphism.

Theorem (5.1)

Suppose $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}$ and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, necessarily of degree n. Suppose we are given a rational prime p which we want to factorise in $\mathcal{O}$.
Choose monic polynomials $g_1(x), \dots, g_k(x) \in \mathbb{Z}[x]$ such that the $\overline{g_i}$'s, the mod p reduction of g_i's, are the distinct irreducible factors of $\overline{f}(x) \in \mathbb{F}_p[x]$ and we have the factorisation

$$\overline{f}(x) = \overline{g_1}(x)^{e_1} \dots \overline{g_k}(x)^{e_k}.$$

Assume that p does not divide $[\mathcal{O} : \mathbb{Z}[\alpha]]$, the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}$. Then each $P_i := (p, g_i(\alpha))$ is a prime ideal of $\mathcal{O}$; $P_1, \dots, P_k$ are the prime ideals of $\mathcal{O}$ dividing p and we have the factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k}.$$

Proof.

- $p \nmid [\mathcal{O} : \mathbb{Z}[\alpha]]$, so if $\beta \in O_K$ and $p\beta \in \mathbb{Z}[\alpha]$ then $\beta \in \mathbb{Z}[\alpha]$. Consequently the kernel of the natural homomorphism $\mathbb{Z}[\alpha] \to \mathcal{O}/p\mathcal{O}$ is precisely $p\mathbb{Z}[\alpha]$, and we get an injection $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}/p\mathcal{O}$. Both sides have order p^n, so this must be an isomorphism.

Theorem (5.1)

Suppose $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}$ and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, necessarily of degree n. Suppose we are given a rational prime p which we want to factorise in $\mathcal{O}$.
Choose monic polynomials $g_1(x), \dots, g_k(x) \in \mathbb{Z}[x]$ such that the $\overline{g_i}$'s, the mod p reduction of g_i's, are the distinct irreducible factors of $\overline{f}(x) \in \mathbb{F}_p[x]$ and we have the factorisation

$$\overline{f}(x) = \overline{g_1}(x)^{e_1} \dots \overline{g_k}(x)^{e_k}.$$

Assume that p does not divide $[\mathcal{O} : \mathbb{Z}[\alpha]]$, the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}$. Then each $P_i := (p, g_i(\alpha))$ is a prime ideal of $\mathcal{O}$; $P_1, \dots, P_k$ are the prime ideals of $\mathcal{O}$ dividing p and we have the factorisation

$$(p) = P_1^{e_1} \dots P_k^{e_k}.$$

Proof.

- $p \nmid [\mathcal{O} : \mathbb{Z}[\alpha]]$, so if $\beta \in O_K$ and $p\beta \in \mathbb{Z}[\alpha]$ then $\beta \in \mathbb{Z}[\alpha]$. Consequently the kernel of the natural homomorphism $\mathbb{Z}[\alpha] \to \mathcal{O}/p\mathcal{O}$ is precisely $p\mathbb{Z}[\alpha]$, and we get an injection $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}/p\mathcal{O}$. Both sides have order p^n, so this must be an isomorphism.

Theorem (5.1)

Suppose $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}$ and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, necessarily of degree n. Suppose we are given a rational prime p which we want to factorise in $\mathcal{O}$.
Choose monic polynomials $g_1(x), \ldots, g_k(x) \in \mathbb{Z}[x]$ such that the $\overline{g_i}$'s, the mod p reduction of g_i's, are the distinct irreducible factors of $\overline{f}(x) \in \mathbb{F}_p[x]$ and we have the factorisation

$$\overline{f}(x) = \overline{g_1}(x)^{e_1} \ldots \overline{g_k}(x)^{e_k}.$$

Assume that p does not divide $[\mathcal{O} : \mathbb{Z}[\alpha]]$, the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}$. Then each $P_i := (p, g_i(\alpha))$ is a prime ideal of $\mathcal{O}$; $P_1, \ldots, P_k$ are the prime ideals of $\mathcal{O}$ dividing p and we have the factorisation

$$(p) = P_1^{e_1} \ldots P_k^{e_k}.$$

Proof.

- $p \nmid [\mathcal{O} : \mathbb{Z}[\alpha]]$, so if $\beta \in O_K$ and $p\beta \in \mathbb{Z}[\alpha]$ then $\beta \in \mathbb{Z}[\alpha]$. Consequently the kernel of the natural homomorphism $\mathbb{Z}[\alpha] \to \mathcal{O}/p\mathcal{O}$ is precisely $p\mathbb{Z}[\alpha]$, and we get an injection $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}/p\mathcal{O}$. Both sides have order p^n, so this must be an isomorphism.

- We have

$$\mathcal{O}/p\mathcal{O} \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, f(x)) \simeq \mathbb{F}_p[x]/(\overline{f}(x)),$$

and so there is a one-to-one correspondence between prime ideals of $\mathcal{O}$ containing $p\mathcal{O}$ and prime ideals of $\mathbb{F}_p[x]$ containing $\overline{f}(x)$. These latter prime ideals are generated by the irreducible factors $\overline{g_i}(x)$ of $\overline{f}(x)$, which correspond to $P_i = (p, g_i(\alpha))$. This shows then that this P_i is a prime ideal dividing (p), and the P_i's are distinct.

- Now

$$\prod P_i^{e_i} = \prod (p, g_i(\alpha))^{e_i} \subseteq \prod (p, g_i(\alpha)^{e_i}) \subseteq (p, \prod g_i(\alpha)^{e_i}) \subseteq (p),$$

the last inclusion because $\prod g_i(x) \equiv f(x) \pmod p$, and $f(\alpha) = 0$. As $\mathbf{N}(P_i) = |\mathbb{F}_p[x]/\overline{g_i}(x)| = p^{\deg(g_i)}$, we get

$$\mathbf{N}(\prod P_i^{e_i}) = p^{\sum e_i \deg g_i} = p^{\deg(f)} = p^n = \mathbf{N}((p)).$$

Hence $\prod P_i^{e_i} = (p)$. $\square$

- We have

$$\mathcal{O}/p\mathcal{O} \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, f(x)) \simeq \mathbb{F}_p[x]/(\overline{f}(x)),$$

  and so there is a one-to-one correspondence between prime ideals of $\mathcal{O}$ containing $p\mathcal{O}$ and prime ideals of $\mathbb{F}_p[x]$ containing $\overline{f}(x)$. These latter prime ideals are generated by the irreducible factors $\overline{g_i}(x)$ of $\overline{f}(x)$, which correspond to $P_i = (p, g_i(\alpha))$. This shows then that this P_i is a prime ideal dividing (p), and the P_i's are distinct.

- Now

$$\prod P_i^{e_i} = \prod (p, g_i(\alpha))^{e_i} \subseteq \prod (p, g_i(\alpha)^{e_i}) \subseteq (p, \prod g_i(\alpha)^{e_i}) \subseteq (p),$$

  the last inclusion because $\prod g_i(x) \equiv f(x) \pmod{p}$, and $f(\alpha) = 0$. As $\mathbf{N}(P_i) = |\mathbb{F}_p[x]/\overline{g_i}(x)| = p^{\deg(g_i)}$, we get

$$\mathbf{N}(\prod P_i^{e_i}) = p^{\sum e_i \deg g_i} = p^{\deg(f)} = p^n = \mathbf{N}((p)).$$

  Hence $\prod P_i^{e_i} = (p)$. $\square$

- We have

$$\mathcal{O}/p\mathcal{O} \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, f(x)) \simeq \mathbb{F}_p[x]/(\overline{f}(x)),$$

  and so there is a one-to-one correspondence between prime ideals of $\mathcal{O}$ containing $p\mathcal{O}$ and prime ideals of $\mathbb{F}_p[x]$ containing $\overline{f}(x)$. These latter prime ideals are generated by the irreducible factors $\overline{g_i}(x)$ of $\overline{f}(x)$, which correspond to $P_i = (p, g_i(\alpha))$. This shows then that this P_i is a prime ideal dividing (p), and the P_i's are distinct.

- Now

$$\prod P_i^{e_i} = \prod (p, g_i(\alpha))^{e_i} \subseteq \prod (p, g_i(\alpha)^{e_i}) \subseteq (p, \prod g_i(\alpha)^{e_i}) \subseteq (p),$$

  the last inclusion because $\prod g_i(x) \equiv f(x) \pmod{p}$, and $f(\alpha) = 0$. As $\mathbf{N}(P_i) = |\mathbb{F}_p[x]/\overline{g_i}(x)| = p^{\deg(g_i)}$, we get

$$\mathbf{N}(\prod P_i^{e_i}) = p^{\sum e_i \deg g_i} = p^{\deg(f)} = p^n = \mathbf{N}((p)).$$

  Hence $\prod P_i^{e_i} = (p)$. $\square$

Remarks:

- In general, suppose $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and p ramifies. Then by the theorem, $\overline{f}(x)$ has a repeated root in $\overline{\mathbb{F}}_p$. Hence in a sufficiently large number field L, some divisor of $p\mathcal{O}_L$ divides some difference of roots $\alpha_i - \alpha_j$ of $f(x)$. It follows that $p \mid \Delta^2(1, \alpha, \ldots, \alpha^{n-1})$. In particular, there are only finitely many ramified primes.
- In fact, something stronger is true. p ramifies if and only if $p \mid \Delta^2(O_K)$. (The Ramification Theorem.) We probably won't get round to proving this.

Remarks:

- In general, suppose $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and p ramifies. Then by the theorem, $\overline{f}(x)$ has a repeated root in $\overline{\mathbb{F}}_p$. Hence in a sufficiently large number field L, some divisor of $p\mathcal{O}_L$ divides some difference of roots $\alpha_i - \alpha_j$ of $f(x)$. It follows that $p \mid \Delta^2(1, \alpha, \ldots, \alpha^{n-1})$. In particular, there are only finitely many ramified primes.
- In fact, something stronger is true. p ramifies if and only if $p \mid \Delta^2(O_K)$. (The Ramification Theorem.) We probably won't get round to proving this.

Example. Take $K = \mathbb{Q}(\sqrt{-5})$ and $\alpha = \sqrt{-5}$. We know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Thus we will know how a prime p factorises in $\mathcal{O}_K$ if we know how $f(x) := x^2 + 5$ behaves modulo p.

- Since $f(x) \equiv (x+1)^2 \pmod 2$ and $f(x) \equiv x^2 \pmod 5$ we get $(2) = (2, \sqrt{-5}+1)^2$ and $(5) = (5, \sqrt{-5})^2 = (\sqrt{-5})^2$. These are the ramified primes.
- Now let p be a prime different from 2 or 5. If $\left(\frac{-5}{p}\right) = -1$, then (x^2+5) is irreducible mod p, so (p) remains prime (i.e. p is inert). However, if $\left(\frac{-5}{p}\right) = +1$ then $x^2 + 5 \equiv (x-a)(x+a) \pmod p$, where $a^2 \equiv -5 \pmod p$. So $(p) = P_1 P_2$ *splits* as a product of two distinct primes $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$.

Example. Take $K = \mathbb{Q}(\sqrt{-5})$ and $\alpha = \sqrt{-5}$. We know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Thus we will know how a prime p factorises in $\mathcal{O}_K$ if we know how $f(x) := x^2 + 5$ behaves modulo p.

- Since $f(x) \equiv (x+1)^2 \pmod 2$ and $f(x) \equiv x^2 \pmod 5$ we get $(2) = (2, \sqrt{-5}+1)^2$ and $(5) = (5, \sqrt{-5})^2 = (\sqrt{-5})^2$. These are the ramified primes.
- Now let p be a prime different from 2 or 5. If $\left(\frac{-5}{p}\right) = -1$, then (x^2+5) is irreducible mod p, so (p) remains prime (i.e. p is inert). However, if $\left(\frac{-5}{p}\right) = +1$ then $x^2 + 5 \equiv (x-a)(x+a) \pmod p$, where $a^2 \equiv -5 \pmod p$. So $(p) = P_1 P_2$ *splits* as a product of two distinct primes $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$.
- $\left(\frac{-5}{p}\right) = +1$ iff either $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1$, or $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$. Using Quadratic Reciprocity, this is equivalent to $p \equiv 1, 3, 7$ or $9 \pmod{20}$.

Example. Take $K = \mathbb{Q}(\sqrt{-5})$ and $\alpha = \sqrt{-5}$. We know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Thus we will know how a prime p factorises in $\mathcal{O}_K$ if we know how $f(x) := x^2 + 5$ behaves modulo p.

- Since $f(x) \equiv (x+1)^2 \pmod 2$ and $f(x) \equiv x^2 \pmod 5$ we get $(2) = (2, \sqrt{-5}+1)^2$ and $(5) = (5, \sqrt{-5})^2 = (\sqrt{-5})^2$. These are the ramified primes.
- Now let p be a prime different from 2 or 5. If $\left(\frac{-5}{p}\right) = -1$, then (x^2+5) is irreducible mod p, so (p) remains prime (i.e. p is inert). However, if $\left(\frac{-5}{p}\right) = +1$ then $x^2 + 5 \equiv (x-a)(x+a) \pmod p$, where $a^2 \equiv -5 \pmod p$. So $(p) = P_1 P_2$ *splits* as a product of two distinct primes $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$.
- $\left(\frac{-5}{p}\right) = +1$ iff either $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1$, or $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$. Using Quadratic Reciprocity, this is equivalent to $p \equiv 1, 3, 7$ or $9 \pmod{20}$. More generally, the splitting of a prime in the ring of integers of a quadratic field is determined by a congruence condition (modulo the discriminant).

Example. Take $K = \mathbb{Q}(\sqrt{-5})$ and $\alpha = \sqrt{-5}$. We know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Thus we will know how a prime p factorises in $\mathcal{O}_K$ if we know how $f(x) := x^2 + 5$ behaves modulo p.

- Since $f(x) \equiv (x+1)^2 \pmod 2$ and $f(x) \equiv x^2 \pmod 5$ we get $(2) = (2, \sqrt{-5}+1)^2$ and $(5) = (5, \sqrt{-5})^2 = (\sqrt{-5})^2$. These are the ramified primes.
- Now let p be a prime different from 2 or 5. If $\left(\frac{-5}{p}\right) = -1$, then (x^2+5) is irreducible mod p, so (p) remains prime (i.e. p is inert). However, if $\left(\frac{-5}{p}\right) = +1$ then $x^2 + 5 \equiv (x-a)(x+a) \pmod p$, where $a^2 \equiv -5 \pmod p$. So $(p) = P_1 P_2$ *splits* as a product of two distinct primes $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$.
- $\left(\frac{-5}{p}\right) = +1$ iff either $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1$, or $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$. Using Quadratic Reciprocity, this is equivalent to $p \equiv 1, 3, 7$ or $9 \pmod{20}$. More generally, the splitting of a prime in the ring of integers of a quadratic field is determined by a congruence condition (modulo the discriminant).

Example. Take $K = \mathbb{Q}(\sqrt{-5})$ and $\alpha = \sqrt{-5}$. We know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Thus we will know how a prime p factorises in $\mathcal{O}_K$ if we know how $f(x) := x^2 + 5$ behaves modulo p.

- Since $f(x) \equiv (x+1)^2 \pmod 2$ and $f(x) \equiv x^2 \pmod 5$ we get $(2) = (2, \sqrt{-5}+1)^2$ and $(5) = (5, \sqrt{-5})^2 = (\sqrt{-5})^2$. These are the ramified primes.
- Now let p be a prime different from 2 or 5. If $\left(\frac{-5}{p}\right) = -1$, then (x^2+5) is irreducible mod p, so (p) remains prime (i.e. p is inert). However, if $\left(\frac{-5}{p}\right) = +1$ then $x^2 + 5 \equiv (x-a)(x+a) \pmod p$, where $a^2 \equiv -5 \pmod p$. So $(p) = P_1 P_2$ *splits* as a product of two distinct primes $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$.
- $\left(\frac{-5}{p}\right) = +1$ iff either $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1$, or $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$. Using Quadratic Reciprocity, this is equivalent to $p \equiv 1, 3, 7$ or $9 \pmod{20}$. More generally, the splitting of a prime in the ring of integers of a quadratic field is determined by a congruence condition (modulo the discriminant).

Example. Take $K = \mathbb{Q}(\sqrt{-5})$ and $\alpha = \sqrt{-5}$. We know that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Thus we will know how a prime p factorises in $\mathcal{O}_K$ if we know how $f(x) := x^2 + 5$ behaves modulo p.

- Since $f(x) \equiv (x+1)^2 \pmod 2$ and $f(x) \equiv x^2 \pmod 5$ we get $(2) = (2, \sqrt{-5}+1)^2$ and $(5) = (5, \sqrt{-5})^2 = (\sqrt{-5})^2$. These are the ramified primes.
- Now let p be a prime different from 2 or 5. If $\left(\frac{-5}{p}\right) = -1$, then (x^2+5) is irreducible mod p, so (p) remains prime (i.e. p is inert). However, if $\left(\frac{-5}{p}\right) = +1$ then $x^2 + 5 \equiv (x-a)(x+a) \pmod p$, where $a^2 \equiv -5 \pmod p$. So $(p) = P_1 P_2$ *splits* as a product of two distinct primes $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$.
- $\left(\frac{-5}{p}\right) = +1$ iff either $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1$, or $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$. Using Quadratic Reciprocity, this is equivalent to $p \equiv 1, 3, 7$ or $9 \pmod{20}$. More generally, the splitting of a prime in the ring of integers of a quadratic field is determined by a congruence condition (modulo the discriminant).

Back to a number field K and $\mathcal{O}$. Say two non-zero ideals I, J are principally equivalent, written $I \sim J$, if $aI = bJ$ for some $0 \neq a, b \in \mathcal{O}$. Equivalently, $I \sim J$ if $I = \gamma J$ for some $0 \neq \gamma \in K$. This is indeed an equivalence relation.

Theorem (5.2)

The equivalence classes of non-zero ideals of $\mathcal{O}$ under principal equivalence is a finite abelian group under multiplication, called the class group of K.

That the ideal classes form a group follows easily from proposition 4.1. The finiteness of the class group follows from the next proposition using the observation that there are only finitely many ideals of a given norm.

Back to a number field K and $\mathcal{O}$. Say two non-zero ideals I, J are principally equivalent, written $I \sim J$, if $aI = bJ$ for some $0 \neq a, b \in \mathcal{O}$. Equivalently, $I \sim J$ if $I = \gamma J$ for some $0 \neq \gamma \in K$. This is indeed an equivalence relation.

Theorem (5.2)

The equivalence classes of non-zero ideals of $\mathcal{O}$ under principal equivalence is a finite abelian group under multiplication, called the class group of K.

That the ideal classes form a group follows easily from proposition 4.1. The finiteness of the class group follows from the next proposition using the observation that there are only finitely many ideals of a given norm.

Back to a number field K and $\mathcal{O}$. Say two non-zero ideals I, J are principally equivalent, written $I \sim J$, if $aI = bJ$ for some $0 \neq a, b \in \mathcal{O}$. Equivalently, $I \sim J$ if $I = \gamma J$ for some $0 \neq \gamma \in K$. This is indeed an equivalence relation.

Theorem (5.2)

The equivalence classes of non-zero ideals of $\mathcal{O}$ under principal equivalence is a finite abelian group under multiplication, called the class group of K.

That the ideal classes form a group follows easily from proposition 4.1. The finiteness of the class group follows from the next proposition using the observation that there are only finitely many ideals of a given norm.

First some notation. Let r be the number of real embeddings $K \to \mathbb{R}$ and $2s$ the number of complex embeddings $\sigma : K \to \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Denote by d_K the discriminant of an integral basis of K. Set

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

The constant M_K is called Minkowski's constant.

Proposition (5.3)

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq M_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq M_K$.*

We prove the first part later. For part (2), assuming (1):

First some notation. Let r be the number of real embeddings $K \to \mathbb{R}$ and $2s$ the number of complex embeddings $\sigma : K \to \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Denote by d_K the discriminant of an integral basis of K. Set

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

The constant M_K is called Minkowski's constant.

Proposition (5.3)

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq M_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq M_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $M_K \mathbf{N}(I)$.

First some notation. Let r be the number of real embeddings $K \to \mathbb{R}$ and $2s$ the number of complex embeddings $\sigma : K \to \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Denote by d_K the discriminant of an integral basis of K. Set

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d_K|}.$$

The constant M_K is called Minkowski's constant.

Proposition (5.3)

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq M_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq M_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $M_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A.

First some notation. Let r be the number of real embeddings $K \to \mathbb{R}$ and $2s$ the number of complex embeddings $\sigma : K \to \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Denote by d_K the discriminant of an integral basis of K. Set

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

The constant M_K is called Minkowski's constant.

Proposition (5.3)

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq M_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq M_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $M_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativy of the norm we get $\mathbf{N}(A) \leq M_K$; by definition $A \in \mathcal{A}$.

First some notation. Let r be the number of real embeddings $K \to \mathbb{R}$ and $2s$ the number of complex embeddings $\sigma : K \to \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Denote by d_K the discriminant of an integral basis of K. Set

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

The constant M_K is called Minkowski's constant.

Proposition (5.3)

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq M_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq M_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $M_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativy of the norm we get $\mathbf{N}(A) \leq M_K$; by definition $A \in \mathcal{A}$.

First some notation. Let r be the number of real embeddings $K \to \mathbb{R}$ and $2s$ the number of complex embeddings $\sigma : K \to \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Denote by d_K the discriminant of an integral basis of K. Set

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

The constant M_K is called Minkowski's constant.

Proposition (5.3)

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq M_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq M_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $M_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativy of the norm we get $\mathbf{N}(A) \leq M_K$; by definition $A \in \mathcal{A}$.

First some notation. Let r be the number of real embeddings $K \to \mathbb{R}$ and $2s$ the number of complex embeddings $\sigma : K \to \mathbb{C}$ with $\sigma(K) \not\subset \mathbb{R}$. Denote by d_K the discriminant of an integral basis of K. Set

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

The constant M_K is called Minkowski's constant.

Proposition (5.3)

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq M_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq M_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $M_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativy of the norm we get $\mathbf{N}(A) \leq M_K$; by definition $A \in \mathcal{A}$.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K : \mathbb{Q}] = n$. We will now investigate the structures of two objects associated to a number field: the ideal class group and the group of units. The proofs of the key propositions use properties of lattices in euclidean spaces (Minkowski theory).

Say two non-zero ideals I, J are principally equivalent, written $I \sim J$, if $aI = bJ$ for some $0 \neq a, b \in \mathcal{O}$. Equivalently, $I \sim J$ if $I = \gamma J$ for some $0 \neq \gamma \in K$. This is indeed an equivalence relation.

Theorem

The equivalence classes of non-zero ideals of $\mathcal{O}$ under principal equivalence is a finite abelian group under multiplication, called the ideal class group, or simply the class group, of K.

That the ideal classes form a group follows easily from proposition 4.1. The finiteness of the class group follows from the next proposition using the observation that there are only finitely many ideals of a given norm.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K:\mathbb{Q}]=n$. We will now investigate the structures of two objects associated to a number field: the ideal class group and the group of units. The proofs of the key propositions use properties of lattices in euclidean spaces (Minkowski theory).

Say two non-zero ideals I, J are principally equivalent, written $I \sim J$, if $aI = bJ$ for some $0 \neq a, b \in \mathcal{O}$. Equivalently, $I \sim J$ if $I = \gamma J$ for some $0 \neq \gamma \in K$. This is indeed an equivalence relation.

Theorem

The equivalence classes of non-zero ideals of $\mathcal{O}$ under principal equivalence is a finite abelian group under multiplication, called the ideal class group, or simply the class group, of K.

That the ideal classes form a group follows easily from proposition 4.1. The finiteness of the class group follows from the next proposition using the observation that there are only finitely many ideals of a given norm.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K:\mathbb{Q}] = n$. We will now investigate the structures of two objects associated to a number field: the ideal class group and the group of units. The proofs of the key propositions use properties of lattices in euclidean spaces (Minkowski theory).

Say two non-zero ideals I, J are principally equivalent, written $I \sim J$, if $aI = bJ$ for some $0 \neq a, b \in \mathcal{O}$. Equivalently, $I \sim J$ if $I = \gamma J$ for some $0 \neq \gamma \in K$. This is indeed an equivalence relation.

Theorem

The equivalence classes of non-zero ideals of $\mathcal{O}$ under principal equivalence is a finite abelian group under multiplication, called the ideal class group, or simply the class group, of K.

That the ideal classes form a group follows easily from proposition 4.1. The finiteness of the class group follows from the next proposition using the observation that there are only finitely many ideals of a given norm.

As always K is a number field, $\mathcal{O}$ its ring of integers. Let $[K : \mathbb{Q}] = n$. We will now investigate the structures of two objects associated to a number field: the ideal class group and the group of units. The proofs of the key propositions use properties of lattices in euclidean spaces (Minkowski theory).

Say two non-zero ideals I, J are principally equivalent, written $I \sim J$, if $aI = bJ$ for some $0 \neq a, b \in \mathcal{O}$. Equivalently, $I \sim J$ if $I = \gamma J$ for some $0 \neq \gamma \in K$. This is indeed an equivalence relation.

Theorem

The equivalence classes of non-zero ideals of $\mathcal{O}$ under principal equivalence is a finite abelian group under multiplication, called the ideal class group, or simply the class group, of K.

That the ideal classes form a group follows easily from proposition 4.1. The finiteness of the class group follows from the next proposition using the observation that there are only finitely many ideals of a given norm.

First some notation. The number field K has n distinct embeddings $K \hookrightarrow \mathbb{C}$. Recall that if $K = \mathbb{Q}(\alpha)$ and if $\alpha_1, \ldots, \alpha_n$ are the n roots of the minimal polynomial of α, then the embeddings come from an identification $\alpha \to \alpha_i$. Note that the non-real roots come in pairs (by complex conjugation). We set:

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.

- d_K denotes the discriminant of an integral basis of K, and

$$C_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

  The constant C_K is called Minkowski's constant.

- $\mu(K)$ denotes the roots of unity in K^*. (In general, the group of units i.e. invertible elements of a ring R will be denoted by R^*.) Note that $\mu(K)$ is finite; it is the torsion subgroup of $\mathcal{O}^*$.

First some notation. The number field K has n distinct embeddings $K \hookrightarrow \mathbb{C}$. Recall that if $K = \mathbb{Q}(\alpha)$ and if $\alpha_1, \ldots, \alpha_n$ are the n roots of the minimal polynomial of α, then the embeddings come from an identification $\alpha \to \alpha_i$. Note that the non-real roots come in pairs (by complex conjugation). We set:

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.

- d_K denotes the discriminant of an integral basis of K, and

$$C_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

  The constant C_K is called Minkowski's constant.

- $\mu(K)$ denotes the roots of unity in K^*. (In general, the group of units i.e. invertible elements of a ring R will be denoted by R^*.) Note that $\mu(K)$ is finite; it is the torsion subgroup of $\mathcal{O}^*$.

First some notation. The number field K has n distinct embeddings $K \hookrightarrow \mathbb{C}$. Recall that if $K = \mathbb{Q}(\alpha)$ and if $\alpha_1, \ldots, \alpha_n$ are the n roots of the minimal polynomial of α, then the embeddings come from an identification $\alpha \to \alpha_i$. Note that the non-real roots come in pairs (by complex conjugation). We set:

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.

- d_K denotes the discriminant of an integral basis of K, and

$$C_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

  The constant C_K is called Minkowski's constant.

- $\mu(K)$ denotes the roots of unity in K^*. (In general, the group of units i.e. invertible elements of a ring R will be denoted by R^*.) Note that $\mu(K)$ is finite; it is the torsion subgroup of $\mathcal{O}^*$.

First some notation. The number field K has n distinct embeddings $K \hookrightarrow \mathbb{C}$. Recall that if $K = \mathbb{Q}(\alpha)$ and if $\alpha_1, \ldots, \alpha_n$ are the n roots of the minimal polynomial of α, then the embeddings come from an identification $\alpha \to \alpha_i$. Note that the non-real roots come in pairs (by complex conjugation). We set:

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.

- d_K denotes the discriminant of an integral basis of K, and

$$C_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}.$$

  The constant C_K is called Minkowski's constant.

- $\mu(K)$ denotes the roots of unity in K^*. (In general, the group of units i.e. invertible elements of a ring R will be denoted by R^*.) Note that $\mu(K)$ is finite; it is the torsion subgroup of $\mathcal{O}^*$.

Proposition

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq C_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $C_K \mathbf{N}(I)$.

Proposition

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq C_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $C_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A.

Proposition

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq C_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $C_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativity of the norm we get $\mathbf{N}(A) \leq C_K$; by definition $A \in \mathcal{A}$.

Proposition

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq C_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $C_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativity of the norm we get $\mathbf{N}(A) \leq C_K$; by definition $A \in \mathcal{A}$.

Remark

By unique factorisation, the ideal class is generated by prime ideals of norm at most C_K. So, in calculations, we need to look at how small primes factorise and discover relations.

Proposition

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq C_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $C_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativity of the norm we get $\mathbf{N}(A) \leq C_K$; by definition $A \in \mathcal{A}$.

Remark

By unique factorisation, the ideal class is generated by prime ideals of norm at most C_K. So, in calculations, we need to look at how small primes factorise and discover relations.

Proposition

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq C_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $C_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativity of the norm we get $\mathbf{N}(A) \leq C_K$; by definition $A \in \mathcal{A}$.

Remark

By unique factorisation, the ideal class is generated by prime ideals of norm at most C_K. So, in calculations, we need to look at how small primes factorise and discover relations.

Proposition

1. *If I is a non-zero ideal then there exists $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.*
2. *Every ideal class contains an ideal A with $\mathbf{N}(A) \leq C_K$.*

We prove the first part later. For part (2), assuming (1): Fix an ideal class $\mathcal{A}$ and pick an ideal I in the inverse of $\mathcal{A}$. Now I contains a non-zero element b with norm at most $C_K \mathbf{N}(I)$. Since I divides (b) we can write $(b) = AI$ for some ideal A. By the multiplicativity of the norm we get $\mathbf{N}(A) \leq C_K$; by definition $A \in \mathcal{A}$.

Remark

By unique factorisation, the ideal class is generated by prime ideals of norm at most C_K. So, in calculations, we need to look at how small primes factorise and discover relations.

Theorem (Dirichlet's unit theorem)

Let K be a number field, r, s as before. Then $\mathcal{O}_K^*/\mu(K)$ is a free abelian group of rank $r+s-1$.

- A set of units which freely generate $\mathcal{O}_K^*/\mu(K)$ is often referred to as a set/system of fundamental units.
- Units have norm ± 1. This directly shows that if K is a quadratic imaginary field then $\mathcal{O}_K^* = \mu(K)$. Also if $K = \mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer then $\mu(K)$ is $\{\pm 1\}$ if $d \neq 1, 3$. When $d = 1$ the group of units is $\{\pm 1, \pm i\}$; when $d = 3$ it is $\{\pm 1, \pm e^{2\pi i/3}, \pm e^{4\pi i/3}\}$.
- Suppose $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free positive integer. Then $\mathcal{O}_K^* \cong \pm\delta^{\mathbb{Z}}$ for some fundamental unit δ.

Theorem (Dirichlet's unit theorem)

Let K be a number field, r, s as before. Then $\mathcal{O}_K^*/\mu(K)$ is a free abelian group of rank $r+s-1$.

- A set of units which freely generate $\mathcal{O}_K^*/\mu(K)$ is often referred to as a set/system of fundamental units.
- Units have norm ± 1. This directly shows that if K is a quadratic imaginary field then $\mathcal{O}_K^* = \mu(K)$. Also if $K = \mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer then $\mu(K)$ is $\{\pm 1\}$ if $d \neq 1, 3$. When $d = 1$ the group of units is $\{\pm 1, \pm i\}$; when $d = 3$ it is $\{\pm 1, \pm e^{2\pi i/3}, \pm e^{4\pi i/3}\}$.
- Suppose $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free positive integer. Then $\mathcal{O}_K^* \cong \pm \delta^{\mathbb{Z}}$ for some fundamental unit δ.

  Suppose $d \not\equiv 1 \pmod 4$. Then we can write $\delta = a + \sqrt{b}$ where a, b are positive integers and $a^2 - db^2 = \pm 1$. This is constructive: the fundamental unit can be found by considering $\pm 1 + dy^2$ as y runs through positive integers and searching for the first time the expression is a square.

Theorem (Dirichlet's unit theorem)

Let K be a number field, r, s as before. Then $\mathcal{O}_K^*/\mu(K)$ is a free abelian group of rank $r+s-1$.

- A set of units which freely generate $\mathcal{O}_K^*/\mu(K)$ is often referred to as a set/system of fundamental units.
- Units have norm ± 1. This directly shows that if K is a quadratic imaginary field then $\mathcal{O}_K^* = \mu(K)$. Also if $K = \mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer then $\mu(K)$ is $\{\pm 1\}$ if $d \neq 1, 3$. When $d = 1$ the group of units is $\{\pm 1, \pm i\}$; when $d = 3$ it is $\{\pm 1, \pm e^{2\pi i/3}, \pm e^{4\pi i/3}\}$.
- Suppose $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free positive integer. Then $\mathcal{O}_K^* \cong \pm\delta^{\mathbb{Z}}$ for some fundamental unit δ.

  Suppose $d \not\equiv 1 \pmod 4$. Then we can write $\delta = a + \sqrt{b}$ where a, b are positive integers and $a^2 - db^2 = \pm 1$. This is constructive: the fundamental unit can be found by considering $\pm 1 + dy^2$ as y runs through positive integers and searching for the first time the expression is a square.

  When $d \equiv 1 \pmod 4$ take $\delta = \frac{a+\sqrt{b}}{2}$ and solve $a^2 - db^2 = \pm 4$.

Theorem (Dirichlet's unit theorem)

Let K be a number field, r, s as before. Then $\mathcal{O}_K^*/\mu(K)$ is a free abelian group of rank $r+s-1$.

- A set of units which freely generate $\mathcal{O}_K^*/\mu(K)$ is often referred to as a set/system of fundamental units.
- Units have norm ± 1. This directly shows that if K is a quadratic imaginary field then $\mathcal{O}_K^* = \mu(K)$. Also if $K = \mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer then $\mu(K)$ is $\{\pm 1\}$ if $d \neq 1, 3$. When $d = 1$ the group of units is $\{\pm 1, \pm i\}$; when $d = 3$ it is $\{\pm 1, \pm e^{2\pi i/3}, \pm e^{4\pi i/3}\}$.
- Suppose $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free positive integer. Then $\mathcal{O}_K^* \cong \pm\delta^{\mathbb{Z}}$ for some fundamental unit δ.

  Suppose $d \not\equiv 1 \pmod 4$. Then we can write $\delta = a + \sqrt{b}$ where a, b are positive integers and $a^2 - db^2 = \pm 1$. This is constructive: the fundamental unit can be found by considering $\pm 1 + dy^2$ as y runs through positive integers and searching for the first time the expression is a square.

  When $d \equiv 1 \pmod 4$ take $\delta = \frac{a+\sqrt{b}}{2}$ and solve $a^2 - db^2 = \pm 4$.

Theorem (Dirichlet's unit theorem)

Let K be a number field, r, s as before. Then $\mathcal{O}_K^*/\mu(K)$ is a free abelian group of rank $r+s-1$.

- A set of units which freely generate $\mathcal{O}_K^*/\mu(K)$ is often referred to as a set/system of fundamental units.
- Units have norm ± 1. This directly shows that if K is a quadratic imaginary field then $\mathcal{O}_K^* = \mu(K)$. Also if $K = \mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer then $\mu(K)$ is $\{\pm 1\}$ if $d \neq 1, 3$. When $d = 1$ the group of units is $\{\pm 1, \pm i\}$; when $d = 3$ it is $\{\pm 1, \pm e^{2\pi i/3}, \pm e^{4\pi i/3}\}$.
- Suppose $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free positive integer. Then $\mathcal{O}_K^* \cong \pm \delta^{\mathbb{Z}}$ for some fundamental unit δ.

  Suppose $d \not\equiv 1 \pmod 4$. Then we can write $\delta = a + \sqrt{b}$ where a, b are positive integers and $a^2 - db^2 = \pm 1$. This is constructive: the fundamental unit can be found by considering $\pm 1 + dy^2$ as y runs through positive integers and searching for the first time the expression is a square.

  When $d \equiv 1 \pmod 4$ take $\delta = \frac{a+\sqrt{b}}{2}$ and solve $a^2 - db^2 = \pm 4$.

Theorem (Dirichlet's unit theorem)

Let K be a number field, r, s as before. Then $\mathcal{O}_K^*/\mu(K)$ is a free abelian group of rank $r+s-1$.

- A set of units which freely generate $\mathcal{O}_K^*/\mu(K)$ is often referred to as a set/system of fundamental units.
- Units have norm ± 1. This directly shows that if K is a quadratic imaginary field then $\mathcal{O}_K^* = \mu(K)$. Also if $K = \mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer then $\mu(K)$ is $\{\pm 1\}$ if $d \neq 1, 3$. When $d = 1$ the group of units is $\{\pm 1, \pm i\}$; when $d = 3$ it is $\{\pm 1, \pm e^{2\pi i/3}, \pm e^{4\pi i/3}\}$.
- Suppose $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free positive integer. Then $\mathcal{O}_K^* \cong \pm \delta^{\mathbb{Z}}$ for some fundamental unit δ.

  Suppose $d \not\equiv 1 \pmod 4$. Then we can write $\delta = a + \sqrt{b}$ where a, b are positive integers and $a^2 - db^2 = \pm 1$. This is constructive: the fundamental unit can be found by considering $\pm 1 + dy^2$ as y runs through positive integers and searching for the first time the expression is a square.

  When $d \equiv 1 \pmod 4$ take $\delta = \frac{a+\sqrt{b}}{2}$ and solve $a^2 - db^2 = \pm 4$.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

- Or even more directly,

$$\begin{aligned} Q^2 &= (9, 3\sqrt{82}+3, 83+2\sqrt{82}) \\ &= (9, 3\sqrt{82}+3, 2+2\sqrt{82}) \\ &= (9, 1+\sqrt{82}) = (9, 10+\sqrt{82}), \quad \text{and so} \\ 2Q^2 &= (18, 20+2\sqrt{82}) = (10+\sqrt{82})(10-\sqrt{82}, 2) = (10+\sqrt{82})P. \end{aligned}$$

- Suppose P is principal, say $P = (a + b\sqrt{82})$ where $a, b \in \mathbb{Z}$. In favourable circumstances consideration of the norm is often enough: for instance we get $a^2 - 82b^2 = \pm 2$ and so if ± 2 weren't a quadratic residue modulo 41 then we can get a contradiction. Unfortunately this method fails here.

  We get around this by making use of the fact that $P^2 = (2)$. Thus $(a + b\sqrt{82})^2 = 2u$ where u is a unit. Now $\mathbf{N}(u) = 1$ and $\gamma := 8 + \sqrt{82}$ is a fundamental unit with norm -1. Hence $u = \gamma^{2k}$ for some $k \in \mathbb{Z}$. Thus without loss of generality $(a + b\sqrt{82})^2 = 2$—which gives a contradiction.

- Or even more directly,

$$
\begin{aligned}
Q^2 &= (9, 3\sqrt{82}+3, 83+2\sqrt{82}) \\
&= (9, 3\sqrt{82}+3, 2+2\sqrt{82}) \\
&= (9, 1+\sqrt{82}) = (9, 10+\sqrt{82}), \quad \text{and so} \\
2Q^2 &= (18, 20+2\sqrt{82}) = (10+\sqrt{82})(10-\sqrt{82}, 2) = (10+\sqrt{82})P.
\end{aligned}
$$

- Suppose P is principal, say $P = (a + b\sqrt{82})$ where $a, b \in \mathbb{Z}$. In favourable circumstances consideration of the norm is often enough: for instance we get $a^2 - 82b^2 = \pm 2$ and so if ± 2 weren't a quadratic residue modulo 41 then we can get a contradiction. Unfortunately this method fails here.

  We get around this by making use of the fact that $P^2 = (2)$. Thus $(a + b\sqrt{82})^2 = 2u$ where u is a unit. Now $\mathbf{N}(u) = 1$ and $\gamma := 8 + \sqrt{82}$ is a fundamental unit with norm -1. Hence $u = \gamma^{2k}$ for some $k \in \mathbb{Z}$. Thus without loss of generality $(a + b\sqrt{82})^2 = 2$—which gives a contradiction.

- Or even more directly,

$$\begin{aligned} Q^2 &= (9, 3\sqrt{82}+3, 83+2\sqrt{82}) \\ &= (9, 3\sqrt{82}+3, 2+2\sqrt{82}) \\ &= (9, 1+\sqrt{82}) = (9, 10+\sqrt{82}), \quad \text{and so} \\ 2Q^2 &= (18, 20+2\sqrt{82}) = (10+\sqrt{82})(10-\sqrt{82}, 2) = (10+\sqrt{82})P. \end{aligned}$$

- Suppose P is principal, say $P = (a + b\sqrt{82})$ where $a, b \in \mathbb{Z}$. In favourable circumstances consideration of the norm is often enough: for instance we get $a^2 - 82b^2 = \pm 2$ and so if ± 2 weren't a quadratic residue modulo 41 then we can get a contradiction. Unfortunately this method fails here.

  We get around this by making use of the fact that $P^2 = (2)$. Thus $(a + b\sqrt{82})^2 = 2u$ where u is a unit. Now $\mathbf{N}(u) = 1$ and $\gamma := 8 + \sqrt{82}$ is a fundamental unit with norm -1. Hence $u = \gamma^{2k}$ for some $k \in \mathbb{Z}$. Thus without loss of generality $(a + b\sqrt{82})^2 = 2$—which gives a contradiction.

Example 2. $K = \mathbb{Q}(\sqrt{-163})$. The ring of integers is $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-163}}{2}$. The discriminant of K is -163; Minkowski's constant is $2\sqrt{163}/\pi \approx 8$. Thus the class group is generated by primes above 2, 3, 5 and 7.

The minimal polynomial of α is $x^2 - x + 41$. This is irreducible mod 2 so (2) is a prime ideal. For odd primes p the reducibility of $x^2 - x + 41$ mod p is equivalent to the equation $x^2 + 163 = 0$ having a solution mod p i.e. $\left(\frac{-163}{p}\right) = 1$. One can do this explicitly when p is 3 or 5 or 7, or use quadratic reciprocity, and conclude that (3), 5, (7) are primes in $\mathcal{O}_K$.

Conclusion: $\mathbb{Z}[\alpha]$ is a PID.

Example 2. $K = \mathbb{Q}(\sqrt{-163})$. The ring of integers is $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-163}}{2}$. The discriminant of K is -163; Minkowski's constant is $2\sqrt{163}/\pi \approx 8$. Thus the class group is generated by primes above 2, 3, 5 and 7.

The minimal polynomial of α is $x^2 - x + 41$. This is irreducible mod 2 so (2) is a prime ideal. For odd primes p the reducibility of $x^2 - x + 41$ mod p is equivalent to the equation $x^2 + 163 = 0$ having a solution mod p i.e. $(\frac{-163}{p}) = 1$. One can do this explicitly when p is 3 or 5 or 7, or use quadratic reciprocity, and conclude that (3), 5, (7) are primes in $\mathcal{O}_K$.

Conclusion: $\mathbb{Z}[\alpha]$ is a PID.

Example 2. $K = \mathbb{Q}(\sqrt{-163})$. The ring of integers is $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-163}}{2}$. The discriminant of K is -163; Minkowski's constant is $2\sqrt{163}/\pi \approx 8$. Thus the class group is generated by primes above 2, 3, 5 and 7.

The minimal polynomial of α is $x^2 - x + 41$. This is irreducible mod 2 so (2) is a prime ideal. For odd primes p the reducibility of $x^2 - x + 41$ mod p is equivalent to the equation $x^2 + 163 = 0$ having a solution mod p i.e. $(\frac{-163}{p}) = 1$. One can do this explicitly when p is 3 or 5 or 7, or use quadratic reciprocity, and conclude that (3), 5, (7) are primes in $\mathcal{O}_K$.

Conclusion: $\mathbb{Z}[\alpha]$ is a PID.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

Example 1. We look at the field $K = \mathbb{Q}(\sqrt{82})$. The integer ring is $\mathbb{Z}[\sqrt{82}]$.

- K has discriminant $4 \cdot 82$ and $9 + \sqrt{82}$ is a fundamental unit.
- Minkowski's constant $C_K = \sqrt{82}$, so every ideal class contains an ideal of norm less than or equal to 9 and the ideal class group is generated by primes above 2, 3, 5 and 7. Now $x^2 - 82$ is irreducible mod 5 and 7, so (5) and (7) are primes. Also $x^2 - 82$ is x^2 mod 2 and $(x-1)(x+1)$ mod 3; so we have factorizations $(2) = P^2$ and $(3) = QQ'$ where

$$P = (2, \sqrt{82}),\ Q = (3, \sqrt{82} + 1) \quad \text{and} \quad Q' = (3, \sqrt{82} - 1).$$

- Thus the ideal class group is generated by P and Q. If we can show that P is not principal and $Q^2 \sim P$ then we'd have established that the ideal class group of $\mathbb{Q}(\sqrt{82})$ is a cyclic group of order 4 and the class of Q is a generator.
- To get relations we look at norms of some elements i.e. consider $a^2 - 82b^2$ for choices of a, b. We notice that $\mathbf{N}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$ and as $3 \notin (10 + \sqrt{82})$, the ideal $(10 + \sqrt{82})$ will factorise as PQ^2 or PQ'^2. Since Q' is the inverse of Q we can conclude that the order of Q divides 4 and $Q^2 \sim P$.

- Or even more directly,

$$\begin{aligned} Q^2 &= (9, 3\sqrt{82}+3, 83+2\sqrt{82}) \\ &= (9, 3\sqrt{82}+3, 2+2\sqrt{82}) \\ &= (9, 1+\sqrt{82}) = (9, 10+\sqrt{82}), \quad \text{and so} \\ 2Q^2 &= (18, 20+2\sqrt{82}) = (10+\sqrt{82})(10-\sqrt{82}, 2) = (10+\sqrt{82})P. \end{aligned}$$

- Suppose P is principal, say $P = (a+b\sqrt{82})$ where $a, b \in \mathbb{Z}$. In favourable circumstances consideration of the norm is often enough: for instance we get $a^2 - 82b^2 = \pm 2$ and so if ± 2 weren't a quadratic residue modulo 41 then we can get a contradiction. Unfortunately this method fails here.

  We get around this by making use of the fact that $P^2 = (2)$. Thus $(a+b\sqrt{82})^2 = 2u$ where u is a unit. Now $\mathbf{N}(u) = 1$ and $\gamma := 8+\sqrt{82}$ is a fundamental unit with norm -1. Hence $u = \gamma^{2k}$ for some $k \in \mathbb{Z}$. Thus without loss of generality $(a+b\sqrt{82})^2 = 2$—which gives a contradiction.

- Or even more directly,

$$\begin{aligned} Q^2 &= (9, 3\sqrt{82}+3, 83+2\sqrt{82}) \\ &= (9, 3\sqrt{82}+3, 2+2\sqrt{82}) \\ &= (9, 1+\sqrt{82}) = (9, 10+\sqrt{82}), \quad \text{and so} \\ 2Q^2 &= (18, 20+2\sqrt{82}) = (10+\sqrt{82})(10-\sqrt{82}, 2) = (10+\sqrt{82})P. \end{aligned}$$

- Suppose P is principal, say $P = (a + b\sqrt{82})$ where $a, b \in \mathbb{Z}$. In favourable circumstances consideration of the norm is often enough: for instance we get $a^2 - 82b^2 = \pm 2$ and so if ± 2 weren't a quadratic residue modulo 41 then we can get a contradiction. Unfortunately this method fails here.

  We get around this by making use of the fact that $P^2 = (2)$. Thus $(a + b\sqrt{82})^2 = 2u$ where u is a unit. Now $\mathbf{N}(u) = 1$ and $\gamma := 8 + \sqrt{82}$ is a fundamental unit with norm -1. Hence $u = \gamma^{2k}$ for some $k \in \mathbb{Z}$. Thus without loss of generality $(a + b\sqrt{82})^2 = 2$—which gives a contradiction.

- Or even more directly,

$$
\begin{aligned}
Q^2 &= (9, 3\sqrt{82}+3, 83+2\sqrt{82}) \\
&= (9, 3\sqrt{82}+3, 2+2\sqrt{82}) \\
&= (9, 1+\sqrt{82}) = (9, 10+\sqrt{82}), \quad \text{and so} \\
2Q^2 &= (18, 20+2\sqrt{82}) = (10+\sqrt{82})(10-\sqrt{82}, 2) = (10+\sqrt{82})P.
\end{aligned}
$$

- Suppose P is principal, say $P = (a + b\sqrt{82})$ where $a, b \in \mathbb{Z}$. In favourable circumstances consideration of the norm is often enough: for instance we get $a^2 - 82b^2 = \pm 2$ and so if ± 2 weren't a quadratic residue modulo 41 then we can get a contradiction. Unfortunately this method fails here.

  We get around this by making use of the fact that $P^2 = (2)$. Thus $(a + b\sqrt{82})^2 = 2u$ where u is a unit. Now $\mathbf{N}(u) = 1$ and $\gamma := 8 + \sqrt{82}$ is a fundamental unit with norm -1. Hence $u = \gamma^{2k}$ for some $k \in \mathbb{Z}$. Thus without loss of generality $(a + b\sqrt{82})^2 = 2$—which gives a contradiction.

Example 2. $K = \mathbb{Q}(\sqrt{-163})$. The ring of integers is $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-163}}{2}$. The discriminant of K is -163; Minkowski's constant is $2\sqrt{163}/\pi \approx 8$. Thus the class group is generated by primes above 2, 3, 5 and 7.

The minimal polynomial of α is $x^2 - x + 41$. This is irreducible mod 2 so (2) is a prime ideal. For odd primes p the reducibility of $x^2 - x + 41$ mod p is equivalent to the equation $x^2 + 163 = 0$ having a solution mod p i.e. $(\frac{-163}{p}) = 1$. One can do this explicitly when p is 3 or 5 or 7, or use quadratic reciprocity, and conclude that (3), (5), (7) are primes in $\mathcal{O}_K$.

Conclusion: $\mathbb{Z}[\alpha]$ is a PID.

Example 2. $K = \mathbb{Q}(\sqrt{-163})$. The ring of integers is $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-163}}{2}$. The discriminant of K is -163; Minkowski's constant is $2\sqrt{163}/\pi \approx 8$. Thus the class group is generated by primes above 2, 3, 5 and 7.

The minimal polynomial of α is $x^2 - x + 41$. This is irreducible mod 2 so (2) is a prime ideal. For odd primes p the reducibility of $x^2 - x + 41$ mod p is equivalent to the equation $x^2 + 163 = 0$ having a solution mod p i.e. $(\frac{-163}{p}) = 1$. One can do this explicitly when p is 3 or 5 or 7, or use quadratic reciprocity, and conclude that (3), (5), (7) are primes in $\mathcal{O}_K$.

Conclusion: $\mathbb{Z}[\alpha]$ is a PID.

Example 2. $K = \mathbb{Q}(\sqrt{-163})$. The ring of integers is $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-163}}{2}$. The discriminant of K is -163; Minkowski's constant is $2\sqrt{163}/\pi \approx 8$. Thus the class group is generated by primes above 2, 3, 5 and 7.

The minimal polynomial of α is $x^2 - x + 41$. This is irreducible mod 2 so (2) is a prime ideal. For odd primes p the reducibility of $x^2 - x + 41$ mod p is equivalent to the equation $x^2 + 163 = 0$ having a solution mod p i.e. $(\frac{-163}{p}) = 1$. One can do this explicitly when p is 3 or 5 or 7, or use quadratic reciprocity, and conclude that (3), (5), (7) are primes in $\mathcal{O}_K$.

Conclusion: $\mathbb{Z}[\alpha]$ is a PID.

Example 3. Let $K = \mathbb{Q}(\sqrt{-6}$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, Minkowski's constant is $4\sqrt{6}/\pi \approx 3.1$. Hence the class group is generated by the classes of prime ideals of norm ≤ 3.

Now $x^2 + 6 \equiv x^2$ modulo 2 and 3, so $(2) = (2, \sqrt{-6})^2 = P_2^2$, say, and $(3) = (3, \sqrt{-6})^2 = P_3^2$, say. One checks that P_2 and P_3 have order 2. Since $\mathbf{N}_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, we must have $(\sqrt{-6}) = P_2 P_3$, so in fact $[P_2] = [P_3]^{-1} = [P_3]$, and C_K is cyclic of order 2.

As an application, we find all integer solutions of the equation $y^2 + 54 = x^3$.

We begin by showing that y is coprime to 6. If y is even then $2|x^3$ but $4 \nmid x^3$, contradiction. If $3 \mid y$ but $9 \nmid y$ then $9 \mid x^3$ but $27 \nmid x^3$, again impossible.

Example 3. Let $K = \mathbb{Q}(\sqrt{-6}$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, Minkowski's constant is $4\sqrt{6}/\pi \approx 3.1$. Hence the class group is generated by the classes of prime ideals of norm ≤ 3.

Now $x^2 + 6 \equiv x^2$ modulo 2 and 3, so $(2) = (2, \sqrt{-6})^2 = P_2^2$, say, and $(3) = (3, \sqrt{-6})^2 = P_3^2$, say. One checks that P_2 and P_3 have order 2. Since $\mathbf{N}_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, we must have $(\sqrt{-6}) = P_2 P_3$, so in fact $[P_2] = [P_3]^{-1} = [P_3]$, and C_K is cyclic of order 2.

As an application, we find all integer solutions of the equation $y^2 + 54 = x^3$.

We begin by showing that y is coprime to 6. If y is even then $2|x^3$ but $4 \nmid x^3$, contradiction. If $3 \mid y$ but $9 \nmid y$ then $9 \mid x^3$ but $27 \nmid x^3$, again impossible. Finally, if $9|y$, say $y = 9y_1, x = 3x_1$, then $3y_1^2 + 2 = x_1^3$ but $\mathrm{LHS} \equiv 2$ or $5 \pmod 9$ so is not a cube.

Example 3. Let $K = \mathbb{Q}(\sqrt{-6}$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, Minkowski's constant is $4\sqrt{6}/\pi \approx 3.1$. Hence the class group is generated by the classes of prime ideals of norm ≤ 3.

Now $x^2 + 6 \equiv x^2$ modulo 2 and 3, so $(2) = (2, \sqrt{-6})^2 = P_2^2$, say, and $(3) = (3, \sqrt{-6})^2 = P_3^2$, say. One checks that P_2 and P_3 have order 2. Since $\mathbf{N}_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, we must have $(\sqrt{-6}) = P_2 P_3$, so in fact $[P_2] = [P_3]^{-1} = [P_3]$, and C_K is cyclic of order 2.

As an application, we find all integer solutions of the equation $y^2 + 54 = x^3$.

We begin by showing that y is coprime to 6. If y is even then $2|x^3$ but $4 \nmid x^3$, contradiction. If $3 \mid y$ but $9 \nmid y$ then $9 \mid x^3$ but $27 \nmid x^3$, again impossible. Finally, if $9|y$, say $y = 9y_1, x = 3x_1$, then $3y_1^2 + 2 = x_1^3$ but $\mathrm{LHS} \equiv 2$ or $5 \pmod 9$ so is not a cube.

Example 3. Let $K = \mathbb{Q}(\sqrt{-6}$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, Minkowski's constant is $4\sqrt{6}/\pi \approx 3.1$. Hence the class group is generated by the classes of prime ideals of norm ≤ 3.

Now $x^2 + 6 \equiv x^2$ modulo 2 and 3, so $(2) = (2, \sqrt{-6})^2 = P_2^2$, say, and $(3) = (3, \sqrt{-6})^2 = P_3^2$, say. One checks that P_2 and P_3 have order 2. Since $\mathbf{N}_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, we must have $(\sqrt{-6}) = P_2 P_3$, so in fact $[P_2] = [P_3]^{-1} = [P_3]$, and C_K is cyclic of order 2.

As an application, we find all integer solutions of the equation $y^2 + 54 = x^3$.

We begin by showing that y is coprime to 6. If y is even then $2|x^3$ but $4 \nmid x^3$, contradiction. If $3 \mid y$ but $9 \nmid y$ then $9 \mid x^3$ but $27 \nmid x^3$, again impossible. Finally, if $9|y$, say $y = 9y_1, x = 3x_1$, then $3y_1^2 + 2 = x_1^3$ but $\mathrm{LHS} \equiv 2$ or $5 \pmod 9$ so is not a cube.

Example 3. Let $K = \mathbb{Q}(\sqrt{-6}$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, Minkowski's constant is $4\sqrt{6}/\pi \approx 3.1$. Hence the class group is generated by the classes of prime ideals of norm ≤ 3.

Now $x^2 + 6 \equiv x^2$ modulo 2 and 3, so $(2) = (2, \sqrt{-6})^2 = P_2^2$, say, and $(3) = (3, \sqrt{-6})^2 = P_3^2$, say. One checks that P_2 and P_3 have order 2. Since $\mathbf{N}_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, we must have $(\sqrt{-6}) = P_2 P_3$, so in fact $[P_2] = [P_3]^{-1} = [P_3]$, and C_K is cyclic of order 2.

As an application, we find all integer solutions of the equation $y^2 + 54 = x^3$.

We begin by showing that y is coprime to 6. If y is even then $2|x^3$ but $4 \nmid x^3$, contradiction. If $3 \mid y$ but $9 \nmid y$ then $9 \mid x^3$ but $27 \nmid x^3$, again impossible. Finally, if $9|y$, say $y = 9y_1, x = 3x_1$, then $3y_1^2 + 2 = x_1^3$ but $\mathrm{LHS} \equiv 2$ or $5 \pmod 9$ so is not a cube.

We now consider the factorization $(y+3\sqrt{-6})(y-3\sqrt{-6}) = x^3$.

If $P \mid (y+3\sqrt{-6})$ and $P \mid (y-3\sqrt{-6})$, where P is a prime ideal, then, taking the difference, $P \mid (6\sqrt{-6}) = P_2^3 P_3^3$, so $P = P_2$ or P_3.
But then $P \mid 3\sqrt{-6}$, so $P \mid y$, contrary to $(y,6)=1$ in $\mathbb{Z}$ (take norms). Hence $(y+3\sqrt{-6})$ and $(y-3\sqrt{-6})$ are coprime ideals. By unique factorisation of ideals, each must be the cube of an ideal, say $(y+3\sqrt{-6}) = A^3$.
Now $A^3 = (y+3\sqrt{-6})$ is principal, and A^2 is principal, since $h_K = 2$, hence A is principal, so $(y+3\sqrt{-6})$ is the cube of a principal ideal.

Thus $y+3\sqrt{-6} = u\alpha^3$, with $\alpha \in \mathcal{O}_K$ and u a unit. But the units ± 1 are cubes, so u may be absorbed into the cube, and $y+3\sqrt{-6} = \alpha^3$. Say $\alpha = a + b\sqrt{-6}$, with $a, b \in \mathbb{Z}$.

Then $y+3\sqrt{-6} = (a+b\sqrt{-6})^3 = (a^3 - 18b^2a) + (3a^2b - 6b^3)\sqrt{-6}$.
Comparing coefficients of $\sqrt{-6}$ gives $3 = 3b(a^2-2b^2)$, so $1 = b(a^2-2b^2)$. If $b=1$ then $a^2 = 3$, impossible, hence $b=-1$ and $a^2=1$.

We now consider the factorization $(y + 3\sqrt{-6})(y - 3\sqrt{-6}) = x^3$.

If $P \mid (y + 3\sqrt{-6})$ and $P \mid (y - 3\sqrt{-6})$, where P is a prime ideal, then, taking the difference, $P \mid (6\sqrt{-6}) = P_2^3 P_3^3$, so $P = P_2$ or P_3.
But then $P \mid 3\sqrt{-6}$, so $P \mid y$, contrary to $(y, 6) = 1$ in $\mathbb{Z}$ (take norms). Hence $(y + 3\sqrt{-6})$ and $(y - 3\sqrt{-6})$ are coprime ideals. By unique factorisation of ideals, each must be the cube of an ideal, say $(y + 3\sqrt{-6}) = A^3$.
Now $A^3 = (y + 3\sqrt{-6})$ is principal, and A^2 is principal, since $h_K = 2$, hence A is principal, so $(y + 3\sqrt{-6})$ is the cube of a principal ideal.

Thus $y + 3\sqrt{-6} = u\alpha^3$, with $\alpha \in \mathcal{O}_K$ and u a unit. But the units ± 1 are cubes, so u may be absorbed into the cube, and $y + 3\sqrt{-6} = \alpha^3$. Say $\alpha = a + b\sqrt{-6}$, with $a, b \in \mathbb{Z}$.

Then $y + 3\sqrt{-6} = (a + b\sqrt{-6})^3 = (a^3 - 18b^2 a) + (3a^2 b - 6b^3)\sqrt{-6}$.
Comparing coefficients of $\sqrt{-6}$ gives $3 = 3b(a^2 - 2b^2)$, so $1 = b(a^2 - 2b^2)$. If $b = 1$ then $a^2 = 3$, impossible, hence $b = -1$ and $a^2 = 1$. So $y = a(a^2 - 18b^2) = \pm 17$, and the only solutions are $x = 7, y = \pm 17$.

We now consider the factorization $(y+3\sqrt{-6})(y-3\sqrt{-6}) = x^3$.

If $P \mid (y+3\sqrt{-6})$ and $P \mid (y-3\sqrt{-6})$, where P is a prime ideal, then, taking the difference, $P \mid (6\sqrt{-6}) = P_2^3 P_3^3$, so $P = P_2$ or P_3.
But then $P \mid 3\sqrt{-6}$, so $P \mid y$, contrary to $(y,6)=1$ in $\mathbb{Z}$ (take norms). Hence $(y+3\sqrt{-6})$ and $(y-3\sqrt{-6})$ are coprime ideals. By unique factorisation of ideals, each must be the cube of an ideal, say $(y+3\sqrt{-6}) = A^3$.
Now $A^3 = (y+3\sqrt{-6})$ is principal, and A^2 is principal, since $h_K = 2$, hence A is principal, so $(y+3\sqrt{-6})$ is the cube of a principal ideal.

Thus $y+3\sqrt{-6} = u\alpha^3$, with $\alpha \in \mathcal{O}_K$ and u a unit. But the units ± 1 are cubes, so u may be absorbed into the cube, and $y+3\sqrt{-6} = \alpha^3$. Say $\alpha = a+b\sqrt{-6}$, with $a,b \in \mathbb{Z}$.

Then $y+3\sqrt{-6} = (a+b\sqrt{-6})^3 = (a^3-18b^2a)+(3a^2b-6b^3)\sqrt{-6}$.
Comparing coefficients of $\sqrt{-6}$ gives $3 = 3b(a^2-2b^2)$, so $1 = b(a^2-2b^2)$. If $b=1$ then $a^2=3$, impossible, hence $b=-1$ and $a^2=1$. So $y = a(a^2-18b^2) = \pm 17$, and the only solutions are $x=7, y=\pm 17$.

We now consider the factorization $(y+3\sqrt{-6})(y-3\sqrt{-6}) = x^3$.

If $P \mid (y+3\sqrt{-6})$ and $P \mid (y-3\sqrt{-6})$, where P is a prime ideal, then, taking the difference, $P \mid (6\sqrt{-6}) = P_2^3 P_3^3$, so $P = P_2$ or P_3.
But then $P \mid 3\sqrt{-6}$, so $P \mid y$, contrary to $(y,6) = 1$ in $\mathbb{Z}$ (take norms). Hence $(y+3\sqrt{-6})$ and $(y-3\sqrt{-6})$ are coprime ideals. By unique factorisation of ideals, each must be the cube of an ideal, say $(y+3\sqrt{-6}) = A^3$.
Now $A^3 = (y+3\sqrt{-6})$ is principal, and A^2 is principal, since $h_K = 2$, hence A is principal, so $(y+3\sqrt{-6})$ is the cube of a principal ideal.

Thus $y+3\sqrt{-6} = u\alpha^3$, with $\alpha \in \mathcal{O}_K$ and u a unit. But the units ± 1 are cubes, so u may be absorbed into the cube, and $y+3\sqrt{-6} = \alpha^3$. Say $\alpha = a+b\sqrt{-6}$, with $a, b \in \mathbb{Z}$.

Then $y+3\sqrt{-6} = (a+b\sqrt{-6})^3 = (a^3-18b^2a)+(3a^2b-6b^3)\sqrt{-6}$.
Comparing coefficients of $\sqrt{-6}$ gives $3 = 3b(a^2-2b^2)$, so $1 = b(a^2-2b^2)$. If $b=1$ then $a^2=3$, impossible, hence $b=-1$ and $a^2=1$. So $y = a(a^2-18b^2) = \pm 17$, and the only solutions are $x=7, y=\pm 17$.

We now consider the factorization $(y+3\sqrt{-6})(y-3\sqrt{-6})=x^3$.

If $P \mid (y+3\sqrt{-6})$ and $P \mid (y-3\sqrt{-6})$, where P is a prime ideal, then, taking the difference, $P \mid (6\sqrt{-6}) = P_2^3 P_3^3$, so $P = P_2$ or P_3.
But then $P \mid 3\sqrt{-6}$, so $P \mid y$, contrary to $(y,6)=1$ in $\mathbb{Z}$ (take norms). Hence $(y+3\sqrt{-6})$ and $(y-3\sqrt{-6})$ are coprime ideals. By unique factorisation of ideals, each must be the cube of an ideal, say $(y+3\sqrt{-6}) = A^3$.
Now $A^3 = (y+3\sqrt{-6})$ is principal, and A^2 is principal, since $h_K = 2$, hence A is principal, so $(y+3\sqrt{-6})$ is the cube of a principal ideal.

Thus $y+3\sqrt{-6} = u\alpha^3$, with $\alpha \in \mathcal{O}_K$ and u a unit. But the units ± 1 are cubes, so u may be absorbed into the cube, and $y+3\sqrt{-6}=\alpha^3$. Say $\alpha = a + b\sqrt{-6}$, with $a, b \in \mathbb{Z}$.

Then $y+3\sqrt{-6} = (a+b\sqrt{-6})^3 = (a^3 - 18b^2a) + (3a^2b - 6b^3)\sqrt{-6}$.
Comparing coefficients of $\sqrt{-6}$ gives $3 = 3b(a^2-2b^2)$, so $1 = b(a^2-2b^2)$. If $b=1$ then $a^2=3$, impossible, hence $b=-1$ and $a^2=1$. So $y = a(a^2-18b^2) = \pm 17$, and the only solutions are $x=7, y=\pm 17$.

Definition

Let V be a real vector space of dimension n. A lattice L of rank m in V is a subgroup of the form $\mathbb{Z}w_1 + \ldots + \mathbb{Z}w_m$ with $w_1, \ldots, w_m$ linearly independent vectors in V. A full lattice is a lattice of rank n.

Recall that $X \subset \mathbb{R}^n$ is discrete iff $X \cap B$ is a finite set for bounded $B \subset \mathbb{R}^n$. We then have the following characterisation of lattices.

Lemma

An additive subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.

We sketch a proof for the *if* part: Let L be a discrete subgroup of $\mathbb{R}^n$. Take V to be the $\mathbb{R}$-span of L, then choose a basis $v_1, \ldots v_n$ of V from R and set $\Gamma := \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$. Now every vector in V can be written modulo Γ as $x_1 v_1 + \ldots + x_m v_m$ with $0 \leq x_1, \ldots, x_m < 1$. This implies, by discreteness, that L/Γ is finite. Thus we can find $d \geq 1$ such that $dL \subseteq \Gamma$ i.e.

$$\mathbb{Z}\frac{v_1}{d} + \ldots + \mathbb{Z}\frac{v_m}{d} \supseteq L \supseteq \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m,$$

and the result follows from standard results on modules over principal ideal domains.

Suppose $\Gamma := \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n \subset \mathbb{R}^n$. We will think of $\mathbb{R}^n$ as column vectors. Then Γ is a full lattice if and only if $\det(w_1|\cdots|w_n) \neq 0$. The region

$$\{x_1w_1 + \ldots + x_nw_n | 0 \leq x_1, \ldots, x_n < 1\}$$

is often called the fundamental parallelotope for Γ; it is a fundamental domain for $\mathbb{R}^n/\Gamma$. Note that $|\det(w_1|\cdots|w_n)|$ is the volume of the fundamental parallelotope. We will simply refer to this as the volume of the lattice and denote it by $\mathrm{vol}(\Gamma)$. This is independent of the choice of a basis for the lattice.

Suppose Λ is a second lattice with basis $v_1, \ldots, v_n$ with transition matrix from $w_1, \ldots, w_n$ given by A i.e. $(v_1 \cdots v_n) = A(w_1 \cdots w_n)$ then

$$\mathrm{vol}(\Lambda) = |\det(A)|\mathrm{vol}(\Gamma).$$

If $\Lambda \subseteq \Gamma$ is a sublattice then $|\det(A)| = [\Gamma : \Lambda]$ and so $\mathrm{vol}(\Lambda) = [\Gamma : \Lambda]\mathrm{vol}(\Gamma)$.

Suppose $\Gamma := \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n \subset \mathbb{R}^n$. We will think of $\mathbb{R}^n$ as column vectors. Then Γ is a full lattice if and only if $\det(w_1|\cdots|w_n) \neq 0$. The region

$$\{x_1w_1 + \ldots + x_nw_n | 0 \leq x_1, \ldots, x_n < 1\}$$

is often called the fundamental parallelotope for Γ; it is a fundamental domain for $\mathbb{R}^n/\Gamma$. Note that $|\det(w_1|\cdots|w_n)|$ is the volume of the fundamental parallelotope. We will simply refer to this as the volume of the lattice and denote it by $\mathrm{vol}(\Gamma)$. This is independent of the choice of a basis for the lattice.

Suppose Λ is a second lattice with basis $v_1, \ldots, v_n$ with transition matrix from $w_1, \ldots, w_n$ given by A i.e. $(v_1 \cdots v_n) = A(w_1 \cdots w_n)$ then

$$\mathrm{vol}(\Lambda) = |\det(A)|\mathrm{vol}(\Gamma).$$

If $\Lambda \subseteq \Gamma$ is a sublattice then $|\det(A)| = [\Gamma : \Lambda]$ and so $\mathrm{vol}(\Lambda) = [\Gamma : \Lambda]\mathrm{vol}(\Gamma)$.

Lemma (7.1)

Let $\Gamma \subset \mathbb{R}^n$ be a full lattice. If $S \subset \mathbb{R}^n$ is measurable and $vol(S) > vol(\Gamma)$, then there exist distinct $s_1, s_2 \in S$ such that $s_1 - s_2 \in \Gamma$.

Proof.

Write $\Gamma = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ and let D be the fundamental parallelotope $\{x_1 w_1 + \ldots + x_n w_n | 0 \leq x_1, \ldots, x_n < 1\}$. Then

$$S = S \cap \mathbb{R}^n = S \cap \Big(\bigcup_{\gamma \in \Gamma} D + \gamma \Big) = \bigcup_{\gamma \in \Gamma} (S \cap (D + \gamma)).$$

Since the unions are disjoint we get

$$\mathrm{vol}(S) = \sum_{\gamma \in \Gamma} \mathrm{vol}\big(S \cap (D + \gamma)\big) = \sum_{\gamma \in \Gamma} \mathrm{vol}\big((S - \gamma) \cap D\big).$$

Now if the sets $S - \gamma$, $\gamma \in \Gamma$, are disjoint then

$$\mathrm{vol}(S) = \mathrm{vol}\big(\bigcup_{\gamma \in \Gamma} (S - \gamma) \cap D \big) \leq \mathrm{vol}(D)$$

which contradicts the hypothesis. So we can find $s_1, s_2 \in S$ and distinct $\gamma_1, \gamma_2 \in \Gamma$ such that $s_1 - \gamma_1 = s_2 - \gamma_2$. This gives $0 \neq s_1 - s_2 = \gamma_1 - \gamma_2 \in \Gamma$. $\square$

Theorem (Minkowski)

Let X be a convex, centrally symmetric measurable subset of $\mathbb{R}^n$ and let Γ be a full lattice in $\mathbb{R}^n$. If $vol(X) > 2^n vol(\Gamma)$ then X contains a non-zero lattice point of Γ.
If in addition X is compact then X contains non-zero lattice points even when $vol(X) = 2^n vol(\Gamma)$.

Recall: convex means that $\lambda x + (1-\lambda)y \in X$ whenever $x, y \in X$ and $0 \leq \lambda \leq 1$; centrally symmetric means $-x \in X$ whenever $x \in X$.
The theorem follows on applying lemma 7.1 to $\frac{1}{2}X$; for the compact case consider tX for $t > 1$. The details are left as an exercise.
Before we return to number fields we record the following:

Lemma (7.2)

Let $n = r + 2s$. Think of vectors in $\mathbb{R}^n$ as $(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s)$ and let $X(t)$ be the domain consisting of vectors satisfying

$$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t.$$

Then $vol(X(t)) = 2^r \pi^s \dfrac{t^n}{n!}$.

Summary of results on lattices

- Let V be a real vector space of dimension n. A lattice L of rank m in V is a subgroup of the form $\mathbb{Z}w_1 + \ldots + \mathbb{Z}w_m$ with $w_1, \ldots, w_m$ linearly independent vectors in V. A full lattice is a lattice of rank n.
- An additive subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.
- (Minkowski) Let X be a convex, centrally symmetric measurable subset of $\mathbb{R}^n$ and let Γ be a full lattice in $\mathbb{R}^n$. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$ then X contains a non-zero lattice point of Γ.
  If in addition X is compact then X contains non-zero lattice points even when $\mathrm{vol}(X) = 2^n \mathrm{vol}(\Gamma)$.
- Let $n = r + 2s$. Think of vectors in $\mathbb{R}^n$ as $(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s)$ and let $X(t)$ be the domain consisting of vectors satisfying
  $$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \le t.$$
  Then $\mathrm{vol}(X(t)) = 2^r \pi^s \dfrac{t^n}{2^s n!}$.

Summary of results on lattices

- Let V be a real vector space of dimension n. A lattice L of rank m in V is a subgroup of the form $\mathbb{Z}w_1 + \ldots + \mathbb{Z}w_m$ with $w_1, \ldots, w_m$ linearly independent vectors in V. A full lattice is a lattice of rank n.
- An additive subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.
- (Minkowski) Let X be a convex, centrally symmetric measurable subset of $\mathbb{R}^n$ and let Γ be a full lattice in $\mathbb{R}^n$. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$ then X contains a non-zero lattice point of Γ.
  If in addition X is compact then X contains non-zero lattice points even when $\mathrm{vol}(X) = 2^n \mathrm{vol}(\Gamma)$.
- Let $n = r + 2s$. Think of vectors in $\mathbb{R}^n$ as $(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s)$ and let $X(t)$ be the domain consisting of vectors satisfying

  $$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t.$$

  Then $\mathrm{vol}(X(t)) = 2^r \pi^s \dfrac{t^n}{2^s n!}$.

Summary of results on lattices

- Let V be a real vector space of dimension n. A lattice L of rank m in V is a subgroup of the form $\mathbb{Z}w_1 + \ldots + \mathbb{Z}w_m$ with $w_1, \ldots, w_m$ linearly independent vectors in V. A full lattice is a lattice of rank n.
- An additive subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.
- (Minkowski) Let X be a convex, centrally symmetric measurable subset of $\mathbb{R}^n$ and let Γ be a full lattice in $\mathbb{R}^n$. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$ then X contains a non-zero lattice point of Γ.
  If in addition X is compact then X contains non-zero lattice points even when $\mathrm{vol}(X) = 2^n \mathrm{vol}(\Gamma)$.
- Let $n = r + 2s$. Think of vectors in $\mathbb{R}^n$ as $(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s)$ and let $X(t)$ be the domain consisting of vectors satisfying

$$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t.$$

  Then $\mathrm{vol}(X(t)) = 2^r \pi^s \dfrac{t^n}{2^s n!}$.

Summary of results on lattices

- Let V be a real vector space of dimension n. A lattice L of rank m in V is a subgroup of the form $\mathbb{Z}w_1 + \ldots + \mathbb{Z}w_m$ with $w_1, \ldots, w_m$ linearly independent vectors in V. A full lattice is a lattice of rank n.
- An additive subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.
- (Minkowski) Let X be a convex, centrally symmetric measurable subset of $\mathbb{R}^n$ and let Γ be a full lattice in $\mathbb{R}^n$. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$ then X contains a non-zero lattice point of Γ.
  If in addition X is compact then X contains non-zero lattice points even when $\mathrm{vol}(X) = 2^n \mathrm{vol}(\Gamma)$.
- Let $n = r + 2s$. Think of vectors in $\mathbb{R}^n$ as $(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s)$ and let $X(t)$ be the domain consisting of vectors satisfying

  $$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t.$$

  Then $\mathrm{vol}(X(t)) = 2^r \pi^s \dfrac{t^n}{2^s n!}$.

Now let K be a number field of degree n with r real embeddings and $2s$ non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

for the real and non-real embeddings. This gives us an embedding of vector spaces $K \to \mathbb{R}^r \times \mathbb{C}^s$; identifying $\mathbb{C}$ with $\mathbb{R}^2$ by taking real and imaginary parts gives the map $j : K \to \mathbb{R}^n$ with

$$j(\alpha) = \big(\rho_1(\alpha), \ldots, \rho_r(\alpha), \mathrm{Re}(\sigma_1(\alpha)), \mathrm{Im}(\sigma_1(\alpha)), \ldots, \mathrm{Re}(\sigma_s(\alpha)), \mathrm{Im}(\sigma_s(\alpha))\big)^T$$

(and the $--^T$ denotes transpose). We will denote the discriminant of K by d_K.

Lemma

Let I be a non-zero ideal of $\mathcal{O}_K$. Then $j(I)$ is a full lattice in $\mathbb{R}^n$ and has volume $\dfrac{\sqrt{|d_K|}}{2^s}\mathbf{N}(I)$.

Sketch of proof. Suppose $I = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Then one sees that

$$|\Delta(\alpha_1, \ldots, \alpha_n)| = 2^s |\det\big(j(\alpha_1), \ldots, j(\alpha_n)\big)|.$$

It follows that $j(I)$ is a full lattice and has volume as claimed.

Now let K be a number field of degree n with r real embeddings and $2s$ non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

for the real and non-real embeddings. This gives us an embedding of vector spaces $K \to \mathbb{R}^r \times \mathbb{C}^s$; identifying $\mathbb{C}$ with $\mathbb{R}^2$ by taking real and imaginary parts gives the map $j : K \to \mathbb{R}^n$ with

$$j(\alpha) = \big(\rho_1(\alpha), \ldots, \rho_r(\alpha), \mathrm{Re}(\sigma_1(\alpha)), \mathrm{Im}(\sigma_1(\alpha)), \ldots, \mathrm{Re}(\sigma_s(\alpha)), \mathrm{Im}(\sigma_s(\alpha))\big)^T$$

(and the $--^T$ denotes transpose). We will denote the discriminant of K by d_K.

Lemma

Let I be a non-zero ideal of $\mathcal{O}_K$. Then $j(I)$ is a full lattice in $\mathbb{R}^n$ and has volume $\frac{\sqrt{|d_K|}}{2^s}\mathbf{N}(I)$.

Sketch of proof. Suppose $I = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Then one sees that

$$|\Delta(\alpha_1, \ldots, \alpha_n)| = 2^s |\det\big(j(\alpha_1), \ldots, j(\alpha_n)\big)|.$$

It follows that $j(I)$ is a full lattice and has volume as claimed.

Now let K be a number field of degree n with r real embeddings and $2s$ non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

for the real and non-real embeddings. This gives us an embedding of vector spaces $K \to \mathbb{R}^r \times \mathbb{C}^s$; identifying $\mathbb{C}$ with $\mathbb{R}^2$ by taking real and imaginary parts gives the map $j : K \to \mathbb{R}^n$ with

$$j(\alpha) = \big(\rho_1(\alpha), \ldots, \rho_r(\alpha), \mathrm{Re}(\sigma_1(\alpha)), \mathrm{Im}(\sigma_1(\alpha)), \ldots, \mathrm{Re}(\sigma_s(\alpha)), \mathrm{Im}(\sigma_s(\alpha))\big)^T$$

(and the $--^T$ denotes transpose). We will denote the discriminant of K by d_K.

Lemma

Let I be a non-zero ideal of $\mathcal{O}_K$. Then $j(I)$ is a full lattice in $\mathbb{R}^n$ and has volume $\dfrac{\sqrt{|d_K|}}{2^s}\mathbf{N}(I)$.

Sketch of proof. Suppose $I = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Then one sees that

$$|\Delta(\alpha_1, \ldots, \alpha_n)| = 2^s |\det\big(j(\alpha_1), \ldots, j(\alpha_n)\big)|.$$

It follows that $j(I)$ is a full lattice and has volume as claimed.

We shall now prove the key proposition from week 6: I a non-zero ideal of $\mathcal{O}_K$. Then we can find $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.

Take $X(t) \subset \mathbb{R}^n$ to be the domain consisting of vectors satisfying

$$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t$$

and choose t so that $\mathrm{vol}(X(t)) = 2^n \mathrm{vol}(j(I))$ i.e.

$$2^r \pi^s \frac{t^n}{2^s n!} = 2^n \frac{\sqrt{|d_K|}}{2^s} \mathbf{N}(I).$$

Then $X(t)$ contains a non-zero $j(b), b \in I$. For such a b, we have

$$\begin{aligned}
|\mathbf{N}(b)| &= |\rho_1(b)| \ldots |\rho_r(b)| |\sigma_1(b)|^2 \ldots |\sigma_s(b)|^2 \\
&\leq \left(\frac{|\rho_1(b)| + \ldots + |\rho_r(b)| + 2|\sigma_1(b)| + \ldots + 2|\sigma_s(b)|}{n} \right)^n \\
&\leq \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|} \mathbf{N}(I).
\end{aligned}$$

We shall now prove the key proposition from week 6: I a non-zero ideal of $\mathcal{O}_K$. Then we can find $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.

Take $X(t) \subset \mathbb{R}^n$ to be the domain consisting of vectors satisfying

$$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t$$

and choose t so that $\mathrm{vol}(X(t)) = 2^n \mathrm{vol}(j(I))$ i.e.

$$2^r \pi^s \frac{t^n}{2^s n!} = 2^n \frac{\sqrt{|d_K|}}{2^s} \mathbf{N}(I).$$

Then $X(t)$ contains a non-zero $j(b), b \in I$. For such a b, we have

$$\begin{aligned}|\mathbf{N}(b)| &= |\rho_1(b)| \ldots |\rho_r(b)| |\sigma_1(b)|^2 \ldots |\sigma_s(b)|^2 \\ &\leq \left(\frac{|\rho_1(b)| + \ldots + |\rho_r(b)| + 2|\sigma_1(b)| + \ldots + 2|\sigma_s(b)|}{n}\right)^n \\ &\leq \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|} \mathbf{N}(I).\end{aligned}$$

We shall now prove the key proposition from week 6: I a non-zero ideal of $\mathcal{O}_K$. Then we can find $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.

Take $X(t) \subset \mathbb{R}^n$ to be the domain consisting of vectors satisfying

$$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t$$

and choose t so that $\mathrm{vol}(X(t)) = 2^n \mathrm{vol}(j(I))$ i.e.

$$2^r \pi^s \frac{t^n}{2^s n!} = 2^n \frac{\sqrt{|d_K|}}{2^s} \mathbf{N}(I).$$

Then $X(t)$ contains a non-zero $j(b), b \in I$. For such a b, we have

$$\begin{aligned}
|\mathbf{N}(b)| &= |\rho_1(b)| \ldots |\rho_r(b)| |\sigma_1(b)|^2 \ldots |\sigma_s(b)|^2 \\
&\leq \left(\frac{|\rho_1(b)| + \ldots + |\rho_r(b)| + 2|\sigma_1(b)| + \ldots + 2|\sigma_s(b)|}{n} \right)^n \\
&\leq \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|} \mathbf{N}(I).
\end{aligned}$$

We shall now prove the key proposition from week 6: I a non-zero ideal of $\mathcal{O}_K$. Then we can find $0 \neq b \in I$ such that $|\mathbf{N}(b)| \leq C_K \mathbf{N}(I)$.

Take $X(t) \subset \mathbb{R}^n$ to be the domain consisting of vectors satisfying

$$|x_1| + \ldots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_s^2 + z_s^2} \leq t$$

and choose t so that $\mathrm{vol}(X(t)) = 2^n \mathrm{vol}(j(I))$ i.e.

$$2^r \pi^s \frac{t^n}{2^s n!} = 2^n \frac{\sqrt{|d_K|}}{2^s} \mathbf{N}(I).$$

Then $X(t)$ contains a non-zero $j(b), b \in I$. For such a b, we have

$$\begin{aligned}
|\mathbf{N}(b)| &= |\rho_1(b)| \ldots |\rho_r(b)||\sigma_1(b)|^2 \ldots |\sigma_s(b)|^2 \\
&\leq \left(\frac{|\rho_1(b)| + \ldots + |\rho_r(b)| + 2|\sigma_1(b)| + \ldots + 2|\sigma_s(b)|}{n} \right)^n \\
&\leq \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|} \mathbf{N}(I).
\end{aligned}$$

Define the logarithmic embedding $\lambda : K^* \to \mathbb{R}^{r+s}$ by

$$\lambda(a) := \big(\ln|\rho_1(a)|, \ldots, \ln|\rho_r(a)|, 2\ln|\sigma_1(a)|, \ldots, 2\ln|\sigma_s(a)|\big)^T.$$

Note that λ is a group homomorphism of the multiplicative group K^* into the additive group $\mathbb{R}^{r+s}$; its kernel is $\mu(K)$ (why?). The image $\lambda(\mathcal{O}^*)$ lies in the hyperplane

$$H := \{(x_1, \ldots, x_{r+s})^T | x_1 + \ldots + x_{r+s} = 0\}.$$

We will show that $\lambda(\mathcal{O}^*)$ is in fact a full lattice in H.

The first observation is that $\lambda(\mathcal{O}^*)$ is discrete i.e. is a lattice. (This follows from the fact that $j(\mathcal{O})$ is a lattice in $\mathbb{R}^n$.)

The next step is to produce units u such that $|\sigma(u)| < 1$ for all but one of the embeddings of K into $\mathbb{C}$.

Define the logarithmic embedding $\lambda : K^* \to \mathbb{R}^{r+s}$ by

$$\lambda(a) := \big(\ln|\rho_1(a)|, \dots, \ln|\rho_r(a)|, 2\ln|\sigma_1(a)|, \dots, 2\ln|\sigma_s(a)|\big)^T.$$

Note that λ is a group homomorphism of the multiplicative group K^* into the additive group $\mathbb{R}^{r+s}$; its kernel is $\mu(K)$ (why?). The image $\lambda(\mathcal{O}^*)$ lies in the hyperplane

$$H := \{(x_1, \dots, x_{r+s})^T | x_1 + \dots + x_{r+s} = 0\}.$$

We will show that $\lambda(\mathcal{O}^*)$ is in fact a full lattice in H.

The first observation is that $\lambda(\mathcal{O}^*)$ is discrete i.e. is a lattice. (This follows from the fact that $j(\mathcal{O})$ is a lattice in $\mathbb{R}^n$.)

The next step is to produce units u such that $|\sigma(u)| < 1$ for all but one of the embeddings of K into $\mathbb{C}$.

Define the logarithmic embedding $\lambda : K^* \to \mathbb{R}^{r+s}$ by

$$\lambda(a) := \big(\ln|\rho_1(a)|, \ldots, \ln|\rho_r(a)|, 2\ln|\sigma_1(a)|, \ldots, 2\ln|\sigma_s(a)|\big)^T.$$

Note that λ is a group homomorphism of the multiplicative group K^* into the additive group $\mathbb{R}^{r+s}$; its kernel is $\mu(K)$ (why?). The image $\lambda(\mathcal{O}^*)$ lies in the hyperplane

$$H := \{(x_1, \ldots, x_{r+s})^T | x_1 + \ldots + x_{r+s} = 0\}.$$

We will show that $\lambda(\mathcal{O}^*)$ is in fact a full lattice in H.

The first observation is that $\lambda(\mathcal{O}^*)$ is discrete i.e. is a lattice. (This follows from the fact that $j(\mathcal{O})$ is a lattice in $\mathbb{R}^n$.)

The next step is to produce units u such that $|\sigma(u)| < 1$ for all but one of the embeddings of K into $\mathbb{C}$.

Lemma (8.1)

Let $c_1, \ldots, c_{r+s}$ be positive real numbers satisfying $c_1 \ldots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then we can find $0 \neq a \in \mathcal{O}$ such that $|\rho_i(a)| \leq c_i$ and $|\sigma_j(a)|^2 \leq c_{r+j}$.

To prove the lemma, apply Minkowski's Theorem to the region in $\mathbb{R}^n$ given by

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r,$$
$$y_1^2 + z_1^2 \leq c_{r+1}, \ldots, y_s^2 + z_s^2 \leq c_{r+s}.$$

By applying the lemma inductively, we can find a sequence of non-zero algebraic integers $a_k \in \mathcal{O}$ with the following property: $|\mathbf{N}(a_k)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$, $|\rho_i(a_k)| > |\rho_i(a_{k+1})|$ for $i = 2, \ldots, r$ and $|\sigma_j(a_k)| > |\sigma_j(a_{k+1})|$ for $j = 1, \ldots, s$.

Since there are only finitely many ideals of a given norm, two of the a_k's must be associates. This gives us a unit $u_1 \in \mathcal{O}^*$ such that

$$|\rho_i(u_1)| < 1 \quad \text{for} \quad i = 2, \ldots r, \quad \text{and} \quad |\sigma_j(u_1)| < 1 \quad \text{for} \quad j = 1, \ldots s.$$

Of course $|\rho_1(u_1)| > 1$ necessarily.

Lemma (8.1)

Let $c_1, \ldots, c_{r+s}$ be positive real numbers satisfying $c_1 \ldots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then we can find $0 \neq a \in \mathcal{O}$ such that $|\rho_i(a)| \leq c_i$ and $|\sigma_j(a)|^2 \leq c_{r+j}$.

To prove the lemma, apply Minkowski's Theorem to the region in $\mathbb{R}^n$ given by

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r,$$
$$y_1^2 + z_1^2 \leq c_{r+1}, \ldots, y_s^2 + z_s^2 \leq c_{r+s}.$$

By applying the lemma inductively, we can find a sequence of non-zero algebraic integers $a_k \in \mathcal{O}$ with the following property: $|\mathbf{N}(a_k)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$, $|\rho_i(a_k)| > |\rho_i(a_{k+1})|$ for $i = 2, \ldots, r$ and $|\sigma_j(a_k)| > |\sigma_j(a_{k+1})|$ for $j = 1, \ldots, s$.

Since there are only finitely many ideals of a given norm, two of the a_k's must be associates. This gives us a unit $u_1 \in \mathcal{O}^*$ such that

$$|\rho_i(u_1)| < 1 \quad \text{for} \quad i = 2, \ldots r, \quad \text{and} \quad |\sigma_j(u_1)| < 1 \quad \text{for} \quad j = 1, \ldots s.$$

Of course $|\rho_1(u_1)| > 1$ necessarily.

Similarly construct units $u_2, \ldots, u_{r+s}$.

Lemma (8.1)

Let $c_1, \ldots, c_{r+s}$ be positive real numbers satisfying $c_1 \ldots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then we can find $0 \neq a \in \mathcal{O}$ such that $|\rho_i(a)| \leq c_i$ and $|\sigma_j(a)|^2 \leq c_{r+j}$.

To prove the lemma, apply Minkowski's Theorem to the region in $\mathbb{R}^n$ given by

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r,$$
$$y_1^2 + z_1^2 \leq c_{r+1}, \ldots, y_s^2 + z_s^2 \leq c_{r+s}.$$

By applying the lemma inductively, we can find a sequence of non-zero algebraic integers $a_k \in \mathcal{O}$ with the following property: $|\mathbf{N}(a_k)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$, $|\rho_i(a_k)| > |\rho_i(a_{k+1})|$ for $i = 2, \ldots, r$ and $|\sigma_j(a_k)| > |\sigma_j(a_{k+1})|$ for $j = 1, \ldots, s$.

Since there are only finitely many ideals of a given norm, two of the a_k's must be associates. This gives us a unit $u_1 \in \mathcal{O}^*$ such that

$$|\rho_i(u_1)| < 1 \quad \text{for} \quad i = 2, \ldots r, \quad \text{and} \quad |\sigma_j(u_1)| < 1 \quad \text{for} \quad j = 1, \ldots s.$$

Of course $|\rho_1(u_1)| > 1$ necessarily.

Similarly construct units $u_2, \ldots, u_{r+s}$.

Lemma (8.1)

Let $c_1, \ldots, c_{r+s}$ be positive real numbers satisfying $c_1 \ldots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then we can find $0 \neq a \in \mathcal{O}$ such that $|\rho_i(a)| \leq c_i$ and $|\sigma_j(a)|^2 \leq c_{r+j}$.

To prove the lemma, apply Minkowski's Theorem to the region in $\mathbb{R}^n$ given by

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r,$$
$$y_1^2 + z_1^2 \leq c_{r+1}, \ldots, y_s^2 + z_s^2 \leq c_{r+s}.$$

By applying the lemma inductively, we can find a sequence of non-zero algebraic integers $a_k \in \mathcal{O}$ with the following property: $|\mathbf{N}(a_k)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$, $|\rho_i(a_k)| > |\rho_i(a_{k+1})|$ for $i = 2, \ldots, r$ and $|\sigma_j(a_k)| > |\sigma_j(a_{k+1})|$ for $j = 1, \ldots, s$.

Since there are only finitely many ideals of a given norm, two of the a_k's must be associates. This gives us a unit $u_1 \in \mathcal{O}^*$ such that

$$|\rho_i(u_1)| < 1 \quad \text{for} \quad i = 2, \ldots r, \quad \text{and} \quad |\sigma_j(u_1)| < 1 \quad \text{for} \quad j = 1, \ldots s.$$

Of course $|\rho_1(u_1)| > 1$ necessarily.

Similarly construct units $u_2, \ldots, u_{r+s}$.

Lemma (8.1)

Let $c_1, \ldots, c_{r+s}$ *be positive real numbers satisfying* $c_1 \ldots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$*.*
Then we can find $0 \neq a \in \mathcal{O}$ *such that* $|\rho_i(a)| \leq c_i$ *and* $|\sigma_j(a)|^2 \leq c_{r+j}$*.*

To prove the lemma, apply Minkowski's Theorem to the region in $\mathbb{R}^n$ given by

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r,$$
$$y_1^2 + z_1^2 \leq c_{r+1}, \ldots, y_s^2 + z_s^2 \leq c_{r+s}.$$

By applying the lemma inductively, we can find a sequence of non-zero algebraic integers $a_k \in \mathcal{O}$ with the following property: $|\mathbf{N}(a_k)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$, $|\rho_i(a_k)| > |\rho_i(a_{k+1})|$ for $i = 2, \ldots, r$ and $|\sigma_j(a_k)| > |\sigma_j(a_{k+1})|$ for $j = 1, \ldots, s$.
Since there are only finitely many ideals of a given norm, two of the a_k's must be associates. This gives us a unit $u_1 \in \mathcal{O}^*$ such that

$$|\rho_i(u_1)| < 1 \quad \text{for} \quad i = 2, \ldots r, \quad \text{and} \quad |\sigma_j(u_1)| < 1 \quad \text{for} \quad j = 1, \ldots s.$$

Of course $|\rho_1(u_1)| > 1$ necessarily.

Similarly construct units $u_2, \ldots, u_{r+s}$.

To conclude the proof, we show that $\lambda(u_1), \ldots, \lambda(u_{r+s})$ spans H. This follows from the following bit of linear algebra:

Lemma (8.2)

Let (a_{ij}) be an $m \times m$ real matrix such that

- $a_{ii} > 0$ *for all* i *and* $a_{ij} < 0$ *whenever* $i \neq j$*,*
- $a_{i1} + \ldots + a_{im} = 0$ *for* $i = 1, \ldots, m$*.*

Then (a_{ij}) has rank $m-1$.

Let $\underline{a}_i$ be the i-th column and suppose that $x_1\underline{a}_1 + \ldots + x_{m-1}\underline{a}_{m-1} = 0$ with $0 < x_k := \max\{x_1, \ldots, x_{m-1}\}$. Then

$$\begin{aligned} 0 &= x_1 a_{k1} + \ldots + x_k a_{kk} + \ldots + x_{m-1} a_{k,m-1} \\ -x_k a_{km} &= x_k a_{k1} + \ldots + x_k a_{kk} + \ldots + x_k a_{k,m-1} \end{aligned}$$

and so

$$0 < -x_k a_{km} = (x_k - x_1)a_{k1} + \ldots + (x_k - x_{m-1})a_{k,m-1} \leq 0$$

which is a contradiction.

To conclude the proof, we show that $\lambda(u_1), \ldots, \lambda(u_{r+s})$ spans H. This follows from the following bit of linear algebra:

Lemma (8.2)

Let (a_{ij}) be an $m \times m$ real matrix such that

- $a_{ii} > 0$ *for all* i *and* $a_{ij} < 0$ *whenever* $i \neq j$,
- $a_{i1} + \ldots + a_{im} = 0$ *for* $i = 1, \ldots, m$.

Then (a_{ij}) has rank $m - 1$.

Let $\underline{a}_i$ be the i-th column and suppose that $x_1\underline{a}_1 + \ldots + x_{m-1}\underline{a}_{m-1} = 0$ with $0 < x_k := \max\{x_1, \ldots, x_{m-1}\}$. Then

$$\begin{aligned} 0 &= x_1 a_{k1} + \ldots + x_k a_{kk} + \ldots + x_{m-1} a_{k,m-1} \\ -x_k a_{km} &= x_k a_{k1} + \ldots + x_k a_{kk} + \ldots + x_k a_{k,m-1} \end{aligned}$$

and so

$$0 < -x_k a_{km} = (x_k - x_1)a_{k1} + \ldots + (x_k - x_{m-1})a_{k,m-1} \leq 0$$

which is a contradiction.

To conclude the proof, we show that $\lambda(u_1), \ldots, \lambda(u_{r+s})$ spans H. This follows from the following bit of linear algebra:

Lemma (8.2)

Let (a_{ij}) *be an* $m \times m$ *real matrix such that*

- $a_{ii} > 0$ *for all* i *and* $a_{ij} < 0$ *whenever* $i \neq j$*,*
- $a_{i1} + \ldots + a_{im} = 0$ *for* $i = 1, \ldots, m$*.*

Then (a_{ij}) *has rank* $m - 1$*.*

Let $\underline{a}_i$ be the i-th column and suppose that $x_1 \underline{a}_1 + \ldots + x_{m-1} \underline{a}_{m-1} = 0$ with $0 < x_k := \max\{x_1, \ldots, x_{m-1}\}$. Then

$$\begin{aligned} 0 &= x_1 a_{k1} + \ldots + x_k a_{kk} + \ldots + x_{m-1} a_{k,m-1} \\ -x_k a_{km} &= x_k a_{k1} + \ldots + x_k a_{kk} + \ldots + x_k a_{k,m-1} \end{aligned}$$

and so

$$0 < -x_k a_{km} = (x_k - x_1) a_{k1} + \ldots + (x_k - x_{m-1}) a_{k,m-1} \leq 0$$

which is a contradiction.

To conclude the proof, we show that $\lambda(u_1), \ldots, \lambda(u_{r+s})$ spans H. This follows from the following bit of linear algebra:

Lemma (8.2)

Let (a_{ij}) be an $m \times m$ real matrix such that

- $a_{ii} > 0$ *for all* i *and* $a_{ij} < 0$ *whenever* $i \neq j$,
- $a_{i1} + \ldots + a_{im} = 0$ *for* $i = 1, \ldots, m$.

Then (a_{ij}) has rank $m - 1$.

Let $\underline{a}_i$ be the i-th column and suppose that $x_1\underline{a}_1 + \ldots + x_{m-1}\underline{a}_{m-1} = 0$ with $0 < x_k := \max\{x_1, \ldots, x_{m-1}\}$. Then

$$\begin{aligned} 0 &= x_1 a_{k1} + \ldots + x_k a_{kk} + \ldots + x_{m-1} a_{k,m-1} \\ -x_k a_{km} &= x_k a_{k1} + \ldots + x_k a_{kk} + \ldots + x_k a_{k,m-1} \end{aligned}$$

and so

$$0 < -x_k a_{km} = (x_k - x_1)a_{k1} + \ldots + (x_k - x_{m-1})a_{k,m-1} \leq 0$$

which is a contradiction.

There are three zeta functions relevant to our story. These are defined as Dirichlet series initially and then analytically continued and they have Euler product expansions (reflecting factorisation into primes).

- The Riemann zeta funtion:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

- Dedekind zeta function of a number field K:

$$\zeta_K(s) = \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \frac{1}{(\mathbf{N}I)^s} = \prod_{\text{non-zero prime ideals } P} \left(1 - \frac{1}{(\mathbf{N}P)^s}\right)^{-1}.$$

There are three zeta functions relevant to our story. These are defined as Dirichlet series initially and then analytically continued and they have Euler product expansions (reflecting factorisation into primes).

- The Riemann zeta funtion:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

- Dedekind zeta function of a number field K:

$$\zeta_K(s) = \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \frac{1}{(\mathbf{N}I)^s} = \prod_{\text{non-zero prime ideals } P} \left(1 - \frac{1}{(\mathbf{N}P)^s}\right)^{-1}.$$

- Dirichlet L-function of a character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

  Here $\chi(n) = \chi(n \mod N)$ when $(n, N) = 1$ and $\chi(n) = 0$ when $(n, N) \neq 1$.

There are three zeta functions relevant to our story. These are defined as Dirichlet series initially and then analytically continued and they have Euler product expansions (reflecting factorisation into primes).

- The Riemann zeta funtion:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

- Dedekind zeta function of a number field K:

$$\zeta_K(s) = \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \frac{1}{(\mathbf{N}I)^s} = \prod_{\text{non-zero prime ideals } P} \left(1 - \frac{1}{(\mathbf{N}P)^s}\right)^{-1}.$$

- Dirichlet L-function of a character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Here $\chi(n) = \chi(n \mod N)$ when $(n,N) = 1$ and $\chi(n) = 0$ when $(n,N) \neq 1$.

There are three zeta functions relevant to our story. These are defined as Dirichlet series initially and then analytically continued and they have Euler product expansions (reflecting factorisation into primes).

- The Riemann zeta funtion:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

- Dedekind zeta function of a number field K:

$$\zeta_K(s) = \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \frac{1}{(\mathbf{N}I)^s} = \prod_{\text{non-zero prime ideals } P} \left(1 - \frac{1}{(\mathbf{N}P)^s}\right)^{-1}.$$

- Dirichlet L-function of a character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

  Here $\chi(n) = \chi(n \mod N)$ when $(n,N) = 1$ and $\chi(n) = 0$ when $(n,N) \neq 1$.

There are three zeta functions relevant to our story. These are defined as Dirichlet series initially and then analytically continued and they have Euler product expansions (reflecting factorisation into primes).

- The Riemann zeta funtion:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

- Dedekind zeta function of a number field K:

$$\zeta_K(s) = \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \frac{1}{(\mathbf{N}I)^s} = \prod_{\text{non-zero prime ideals } P} \left(1 - \frac{1}{(\mathbf{N}P)^s}\right)^{-1}.$$

- Dirichlet L-function of a character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

  Here $\chi(n) = \chi(n \mod N)$ when $(n, N) = 1$ and $\chi(n) = 0$ when $(n, N) \neq 1$.

Remarks:

- It is clear that the series and product expansions hold as long as $\mathrm{Re}(s) \gg 1$. In fact the series and product expansions are valid for $\mathrm{Re}(s) > 1$. (This is easy to see for $\zeta(s)$ and $L(s,\chi)$ but requires more work for the Dedekind zeta function.)
- $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Note that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.
- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a character. When χ is non-trivial the partial sums $\chi(1) + \ldots + \chi(n)$ are bounded and consequently, by Abel's theorem, the series for $L(s,\chi)$ converges and defines an analytic function on $\mathrm{Re}(s) > 0$.

Remarks:

- It is clear that the series and product expansions hold as long as $\mathrm{Re}(s) \gg 1$. In fact the series and product expansions are valid for $\mathrm{Re}(s) > 1$. (This is easy to see for $\zeta(s)$ and $L(s,\chi)$ but requires more work for the Dedekind zeta function.)
- $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Note that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.
- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a character. When χ is non-trivial the partial sums $\chi(1) + \ldots + \chi(n)$ are bounded and consequently, by Abel's theorem, the series for $L(s,\chi)$ converges and defines an analytic function on $\mathrm{Re}(s) > 0$.

  If χ is the trivial character then $L(s,\chi) = \zeta(s)\prod_{p|N}(1 - p^{-s})$.

Remarks:

- It is clear that the series and product expansions hold as long as $\mathrm{Re}(s) \gg 1$. In fact the series and product expansions are valid for $\mathrm{Re}(s) > 1$. (This is easy to see for $\zeta(s)$ and $L(s,\chi)$ but requires more work for the Dedekind zeta function.)
- $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Note that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.
- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a character. When χ is non-trivial the partial sums $\chi(1) + \ldots + \chi(n)$ are bounded and consequently, by Abel's theorem, the series for $L(s,\chi)$ converges and defines an analytic function on $\mathrm{Re}(s) > 0$.

  If χ is the trivial character then $L(s,\chi) = \zeta(s) \prod_{p|N} (1 - p^{-s})$.
- Let $K = \mathbb{Q}(e^{\frac{2\pi i}{N}})$. It is then not hard to show that

$$\zeta_K(s) = G(s) \prod_{\chi} L(s,\chi)$$

  where the product runs over all characters $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ and $G(s) := \prod_{P|m} (1 - (\mathbf{N}P)^{-s})^{-1}$ with the product running over all prime ideals of $\mathcal{O}_K$ dividing m. The value, or rather the residue, at $s = 1$ reflects the arithmetic of K strongly while the right hand side can be computed analytically.

Remarks:

- It is clear that the series and product expansions hold as long as $\mathrm{Re}(s) \gg 1$. In fact the series and product expansions are valid for $\mathrm{Re}(s) > 1$. (This is easy to see for $\zeta(s)$ and $L(s,\chi)$ but requires more work for the Dedekind zeta function.)
- $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Note that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.
- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a character. When χ is non-trivial the partial sums $\chi(1) + \ldots + \chi(n)$ are bounded and consequently, by Abel's theorem, the series for $L(s,\chi)$ converges and defines an analytic function on $\mathrm{Re}(s) > 0$.

  If χ is the trivial character then $L(s,\chi) = \zeta(s) \prod_{p|N}(1 - p^{-s})$.
- Let $K = \mathbb{Q}(e^{\frac{2\pi i}{N}})$. It is then not hard to show that

$$\zeta_K(s) = G(s) \prod_{\chi} L(s,\chi)$$

where the product runs over all characters $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ and $G(s) := \prod_{P|m}(1 - (\mathbf{N}P)^{-s})^{-1}$ with the product running over all prime ideals of $\mathcal{O}_K$ dividing m. The value, or rather the residue, at $s = 1$ reflects the arithmetic of K strongly while the right hand side can be computed analytically.

Remarks:

- It is clear that the series and product expansions hold as long as $\mathrm{Re}(s) \gg 1$. In fact the series and product expansions are valid for $\mathrm{Re}(s) > 1$. (This is easy to see for $\zeta(s)$ and $L(s,\chi)$ but requires more work for the Dedekind zeta function.)
- $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Note that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.
- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a character. When χ is non-trivial the partial sums $\chi(1) + \ldots + \chi(n)$ are bounded and consequently, by Abel's theorem, the series for $L(s,\chi)$ converges and defines an analytic function on $\mathrm{Re}(s) > 0$.

  If χ is the trivial character then $L(s,\chi) = \zeta(s) \prod_{p|N} (1 - p^{-s})$.
- Let $K = \mathbb{Q}(e^{\frac{2\pi i}{N}})$. It is then not hard to show that

$$\zeta_K(s) = G(s) \prod_{\chi} L(s,\chi)$$

  where the product runs over all characters $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ and $G(s) := \prod_{P|m} (1 - (\mathbf{N}P)^{-s})^{-1}$ with the product running over all prime ideals of $\mathcal{O}_K$ dividing m. The value, or rather the residue, at $s = 1$ reflects the arithmetic of K strongly while the right hand side can be computed analytically.

Remarks:

- It is clear that the series and product expansions hold as long as $\mathrm{Re}(s) \gg 1$. In fact the series and product expansions are valid for $\mathrm{Re}(s) > 1$. (This is easy to see for $\zeta(s)$ and $L(s,\chi)$ but requires more work for the Dedekind zeta function.)
- $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. Note that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.
- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a character. When χ is non-trivial the partial sums $\chi(1) + \ldots + \chi(n)$ are bounded and consequently, by Abel's theorem, the series for $L(s,\chi)$ converges and defines an analytic function on $\mathrm{Re}(s) > 0$.

  If χ is the trivial character then $L(s,\chi) = \zeta(s) \displaystyle\prod_{p|N} (1 - p^{-s})$.
- Let $K = \mathbb{Q}(e^{\frac{2\pi i}{N}})$. It is then not hard to show that

$$\zeta_K(s) = G(s) \prod_{\chi} L(s,\chi)$$

  where the product runs over all characters $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ and $G(s) := \prod_{P|m} (1 - (\mathbf{N}P)^{-s})^{-1}$ with the product running over all prime ideals of $\mathcal{O}_K$ dividing m. The value, or rather the residue, at $s = 1$ reflects the arithmetic of K strongly while the right hand side can be computed analytically.

Example. Let $K = \mathbb{Q}(\sqrt{-q})$ where q is an odd prime congruent to 3 modulo 4. Let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \{\pm 1\}$ be the unique character of order 2 i.e. $\chi(x) = \left(\frac{x}{q}\right)$. We will verify that $\zeta_K(s) = \zeta(s)L(s,\chi)$.

The integer ring of K is $\mathbb{Z}[w]$ where $w = \frac{1+\sqrt{-q}}{2}$. The minimal polynomial of w is $f_w := x^2 - x + \frac{1+q}{4}$. To study how a rational prime p factorises we need to consider f_w modulo p.

If p is an odd prime then we can write f_w as $(x - \frac{1}{2})^2 + \frac{q}{4}$. If further $p \neq q$ then f_w splits as a product of two linear factors iff $\left(\frac{-q}{p}\right) = 1$. By quadratic reciprocity

$$\begin{aligned}\left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\\ &= (-1)^{p-1}\left(\frac{p}{q}\right) = \chi(p).\end{aligned}$$

We can now match Euler factors to verify $\zeta_K(s) = \zeta(s)L(s,\chi)$.

Example. Let $K = \mathbb{Q}(\sqrt{-q})$ where q is an odd prime congruent to 3 modulo 4. Let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \{\pm 1\}$ be the unique character of order 2 i.e. $\chi(x) = \left(\frac{x}{q}\right)$. We will verify that $\zeta_K(s) = \zeta(s)L(s,\chi)$.

The integer ring of K is $\mathbb{Z}[w]$ where $w = \frac{1+\sqrt{-q}}{2}$. The minimal polynomial of w is $f_w := x^2 - x + \frac{1+q}{4}$. To study how a rational prime p factorises we need to consider f_w modulo p.

If p is an odd prime then we can write f_w as $(x - \frac{1}{2})^2 + \frac{q}{4}$. If further $p \neq q$ then f_w splits as a product of two linear factors iff $\left(\frac{-q}{p}\right) = 1$. By quadratic reciprocity

$$\begin{aligned}\left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\\ &= (-1)^{p-1}\left(\frac{p}{q}\right) = \chi(p).\end{aligned}$$

We can now match Euler factors to verify $\zeta_K(s) = \zeta(s)L(s,\chi)$.

Example. Let $K = \mathbb{Q}(\sqrt{-q})$ where q is an odd prime congruent to 3 modulo 4. Let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \{\pm 1\}$ be the unique character of order 2 i.e. $\chi(x) = \left(\frac{x}{q}\right)$. We will verify that $\zeta_K(s) = \zeta(s)L(s,\chi)$.

The integer ring of K is $\mathbb{Z}[w]$ where $w = \frac{1+\sqrt{-q}}{2}$. The minimal polynomial of w is $f_w := x^2 - x + \frac{1+q}{4}$. To study how a rational prime p factorises we need to consider f_w modulo p.

If p is an odd prime then we can write f_w as $(x - \frac{1}{2})^2 + \frac{q}{4}$. If further $p \neq q$ then f_w splits as a product of two linear factors iff $\left(\frac{-q}{p}\right) = 1$. By quadratic reciprocity

$$\begin{aligned}
\left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \\
&= (-1)^{p-1}\left(\frac{p}{q}\right) = \chi(p).
\end{aligned}$$

We can now match Euler factors to verify $\zeta_K(s) = \zeta(s)L(s,\chi)$.

Example. Let $K = \mathbb{Q}(\sqrt{-q})$ where q is an odd prime congruent to 3 modulo 4. Let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \{\pm 1\}$ be the unique character of order 2 i.e. $\chi(x) = \left(\frac{x}{q}\right)$. We will verify that $\zeta_K(s) = \zeta(s)L(s,\chi)$.

The integer ring of K is $\mathbb{Z}[w]$ where $w = \frac{1+\sqrt{-q}}{2}$. The minimal polynomial of w is $f_w := x^2 - x + \frac{1+q}{4}$. To study how a rational prime p factorises we need to consider f_w modulo p.

If p is an odd prime then we can write f_w as $(x-\frac{1}{2})^2 + \frac{q}{4}$. If further $p \neq q$ then f_w splits as a product of two linear factors iff $\left(\frac{-q}{p}\right) = 1$. By quadratic reciprocity

$$\begin{aligned}\left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\\ &= (-1)^{p-1}\left(\frac{p}{q}\right) = \chi(p).\end{aligned}$$

We can now match Euler factors to verify $\zeta_K(s) = \zeta(s)L(s,\chi)$.

Consider the Euler factors at an odd prime $p \neq q$.

If $-q$ is not a square mod p then $\chi(p) = -1$ and f_w is irreducible over $\mathbb{F}_p$. So (p) is a prime ideal in $\mathbb{Z}[w]$ and $\mathbf{N}(p) = p^2$. Euler factor for $\zeta_K(s)$ is $(1 - p^{-2s})^{-1}$; the Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - p^{-s})^{-1}(1 - \chi(p)p^{-s})^{-1} = (1 - p^{-2s})^{-1},$$

and they match.

If $-q$ is a square mod p then $\chi(p) = 1$ and f_w factorises as a product of two linear factors. So $(p) = P_1 P_2$ where P_1, P_2 are the distinct prime ideals above p. As $\mathbf{N}(P_1) = \mathbf{N}(P_2) = p$ the Euler factor for $\zeta_K(s)$ is

$$(1 - \mathbf{N}(P_1)^{-s})^{-1}(1 - \mathbf{N}(P_2)^{-s})^{-1} = (1 - p^{-s})^{-2}.$$

Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - p^{-s})^{-1}(1 - \chi(p)p^{-s})^{-1} = (1 - p^{-s})^{-2},$$

and they match.

Now q ramifies: $(q) = P^2$ where the prime P has norm q. The Euler factor for $\zeta_K(s)$ is $(1 - q^{-s})^{-1}$. Since $\chi(q) = 0$ this is also the Euler factor for $\zeta(s)L(s, \chi)$.

Consider the Euler factors at an odd prime $p \neq q$.

If $-q$ is not a square mod p then $\chi(p) = -1$ and f_w is irreducible over $\mathbb{F}_p$. So (p) is a prime ideal in $\mathbb{Z}[w]$ and $\mathbf{N}(p) = p^2$. Euler factor for $\zeta_K(s)$ is $(1 - p^{-2s})^{-1}$; the Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - p^{-s})^{-1}(1 - \chi(p)p^{-s})^{-1} = (1 - p^{-2s})^{-1},$$

and they match.

If $-q$ is a square mod p then $\chi(p) = 1$ and f_w factorises as a product of two linear factors. So $(p) = P_1 P_2$ where P_1, P_2 are the distinct prime ideals above p. As $\mathbf{N}(P_1) = \mathbf{N}(P_2) = p$ the Euler factor for $\zeta_K(s)$ is

$$(1 - \mathbf{N}(P_1)^{-s})^{-1}(1 - \mathbf{N}(P_2)^{-s})^{-1} = (1 - p^{-s})^{-2}.$$

Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - p^{-s})^{-1}(1 - \chi(p)p^{-s})^{-1} = (1 - p^{-s})^{-2},$$

and they match.

Now q ramifies: $(q) = P^2$ where the prime P has norm q. The Euler factor for $\zeta_K(s)$ is $(1 - q^{-s})^{-1}$. Since $\chi(q) = 0$ this is also the Euler factor for $\zeta(s)L(s, \chi)$.

Consider the Euler factors at an odd prime $p \neq q$.

If $-q$ is not a square mod p then $\chi(p) = -1$ and f_w is irreducible over $\mathbb{F}_p$. So (p) is a prime ideal in $\mathbb{Z}[w]$ and $\mathbf{N}(p) = p^2$. Euler factor for $\zeta_K(s)$ is $(1 - p^{-2s})^{-1}$; the Euler factor for $\zeta(s)L(s,\chi)$ is

$$(1 - p^{-s})^{-1}(1 - \chi(p)p^{-s})^{-1} = (1 - p^{-2s})^{-1},$$

and they match.

If $-q$ is a square mod p then $\chi(p) = 1$ and f_w factorises as a product of two linear factors. So $(p) = P_1 P_2$ where P_1, P_2 are the distinct prime ideals above p. As $\mathbf{N}(P_1) = \mathbf{N}(P_2) = p$ the Euler factor for $\zeta_K(s)$ is

$$(1 - \mathbf{N}(P_1)^{-s})^{-1}(1 - \mathbf{N}(P_2)^{-s})^{-1} = (1 - p^{-s})^{-2}.$$

Euler factor for $\zeta(s)L(s,\chi)$ is

$$(1 - p^{-s})^{-1}(1 - \chi(p)p^{-s})^{-1} = (1 - p^{-s})^{-2},$$

and they match.

Now q ramifies: $(q) = P^2$ where the prime P has norm q. The Euler factor for $\zeta_K(s)$ is $(1 - q^{-s})^{-1}$. Since $\chi(q) = 0$ this is also the Euler factor for $\zeta(s)L(s,\chi)$.

Now for $p = 2$. If $q \equiv 3 \pmod 8$ then $f_w = x^2 + x + 1$ modulo 2 and is irreducible over $\mathbb{F}_2$. Hence (2) is a prime and $\mathbf{N}(2) = 2^2$. Also $\chi(2) = -1$. Euler factor for $\zeta_K(s)$ is $(1 - 2^{-2s})^{-1}$. Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - 2^{-s})^{-1}(1 - \chi(2)2^{-s})^{-1} = (1 - 2^{-2s})^{-1},$$

and they match.

If $q \equiv 7 \pmod 8$ then $f_w = x^2 + x$ modulo 2. Hence $(2) = P_1 P_2$ where P_1, P_2 are the distinct prime ideals above 2. Also $\mathbf{N}(P_1) = \mathbf{N}(P_2) = 2$ and $\chi(2) = 1$. Euler factor for $\zeta_K(s)$ is $(1 - \mathbf{N}(P_1)^{-s})^{-1}(1 - \mathbf{N}(P_2)^{-s})^{-1}$ which is $(1 - 2^{-s})^{-2}$. Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - 2^{-s})^{-1}(1 - \chi(2)2^{-s})^{-1} = (1 - 2^{-2s})^{-1},$$

and they match.

Now for $p = 2$. If $q \equiv 3 \pmod 8$ then $f_w = x^2 + x + 1$ modulo 2 and is irreducible over $\mathbb{F}_2$. Hence (2) is a prime and $\mathbf{N}(2) = 2^2$. Also $\chi(2) = -1$. Euler factor for $\zeta_K(s)$ is $(1 - 2^{-2s})^{-1}$. Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - 2^{-s})^{-1}(1 - \chi(2)2^{-s})^{-1} = (1 - 2^{-2s})^{-1},$$

and they match.

If $q \equiv 7 \pmod 8$ then $f_w = x^2 + x$ modulo 2. Hence $(2) = P_1 P_2$ where P_1, P_2 are the distinct prime ideals above 2. Also $\mathbf{N}(P_1) = \mathbf{N}(P_2) = 2$ and $\chi(2) = 1$. Euler factor for $\zeta_K(s)$ is $(1 - \mathbf{N}(P_1)^{-s})^{-1}(1 - \mathbf{N}(P_2)^{-s})^{-1}$ which is $(1 - 2^{-s})^{-2}$. Euler factor for $\zeta(s)L(s, \chi)$ is

$$(1 - 2^{-s})^{-1}(1 - \chi(2)2^{-s})^{-1} = (1 - 2^{-2s})^{-1},$$

and they match.

Theorem (Analytic class number formula)

Let K be a number field. Then $\zeta_K(s)$ extends to an analytic function on $\mathbb{C}$ except for a simple pole at $s = 1$. Furthermore, the residue at $s = 1$ is given by

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r+s}\pi^s h_K R_K}{w_K \sqrt{|d_K|}}$$

where

$$\begin{aligned}
r &:= \text{ number of real embeddings } K \to \mathbb{R}, \\
s &:= \text{ number of non-real embeddings } K \to \mathbb{C} \text{ up to conjugacy}, \\
d_K &:= \text{ discriminant of } K \text{ i.e. the discriminant of an integral basis of } \mathcal{O}_K, \\
h_K &:= \text{ the class number of } K, \\
R_K &:= \text{ the regulator of } K, \\
w_K &:= \text{ the number of roots of unity in } K.
\end{aligned}$$

We still need to explain what the regulator is. Recall the logarithmic embedding $\lambda : K \to \mathbb{R}^{r+s}$ given by

$$\lambda(a) := \big(\ln|\rho_1(a)|, \ldots, \ln|\rho_r(a)|, 2\ln|\sigma_1(a)|, \ldots, 2\ln|\sigma_s(a)|\big)^T.$$

- The regulator R is 1 when $r+s=1$ i.e. when K is $\mathbb{Q}$ or a quadratic imaginary field.
- When $r+s>1$ let $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ be a system of fundamental units for $\mathcal{O}_K^*$ i.e. $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ is a basis of the free abelian group $\lambda(\mathcal{O}_K^*)$. Then the regulator R is the absolute value of the determinant of any $(r+s-1)\times(r+s-1)$ submatrix of the $(r+s)\times(r+s-1)$ matrix

$$\Big(\lambda(\varepsilon_1) \mid \cdots \mid \lambda(\varepsilon_{r+s-1})\Big).$$

- Note that when $r+s=2$ (so $\mathcal{O}_K^*$ modulo torsion is cyclic) the regulator is the absolute value of the logarithm of a fundamental unit.

We still need to explain what the regulator is. Recall the logarithmic embedding $\lambda : K \to \mathbb{R}^{r+s}$ given by

$$\lambda(a) := \big(\ln|\rho_1(a)|, \ldots, \ln|\rho_r(a)|, 2\ln|\sigma_1(a)|, \ldots, 2\ln|\sigma_s(a)|\big)^T.$$

- The regulator R is 1 when $r+s=1$ i.e. when K is $\mathbb{Q}$ or a quadratic imaginary field.
- When $r+s>1$ let $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ be a system of fundamental units for $\mathcal{O}_K^*$ i.e. $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ is a basis of the free abelian group $\lambda(\mathcal{O}_K^*)$. Then the regulator R is the absolute value of the determinant of any $(r+s-1)\times(r+s-1)$ submatrix of the $(r+s)\times(r+s-1)$ matrix

$$\Big(\lambda(\varepsilon_1) \mid \cdots \mid \lambda(\varepsilon_{r+s-1})\Big).$$

- Note that when $r+s=2$ (so $\mathcal{O}_K^*$ modulo torsion is cyclic) the regulator is the absolute value of the logarithm of a fundamental unit.

We still need to explain what the regulator is. Recall the logarithmic embedding $\lambda : K \to \mathbb{R}^{r+s}$ given by

$$\lambda(a) := \big(\ln|\rho_1(a)|, \ldots, \ln|\rho_r(a)|, 2\ln|\sigma_1(a)|, \ldots, 2\ln|\sigma_s(a)|\big)^T.$$

- The regulator R is 1 when $r+s=1$ i.e. when K is $\mathbb{Q}$ or a quadratic imaginary field.
- When $r+s>1$ let $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ be a system of fundamental units for $\mathcal{O}_K^*$ i.e. $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ is a basis of the free abelian group $\lambda(\mathcal{O}_K^*)$. Then the regulator R is the absolute value of the determinant of any $(r+s-1) \times (r+s-1)$ submatrix of the $(r+s) \times (r+s-1)$ matrix

$$\Big(\lambda(\varepsilon_1) \mid \cdots \mid \lambda(\varepsilon_{r+s-1})\Big).$$

- Note that when $r+s=2$ (so $\mathcal{O}_K^*$ modulo torsion is cyclic) the regulator is the absolute value of the logarithm of a fundamental unit.

We still need to explain what the regulator is. Recall the logarithmic embedding $\lambda : K \to \mathbb{R}^{r+s}$ given by

$$\lambda(a) := \big(\ln|\rho_1(a)|, \ldots, \ln|\rho_r(a)|, 2\ln|\sigma_1(a)|, \ldots, 2\ln|\sigma_s(a)|\big)^T.$$

- The regulator R is 1 when $r+s=1$ i.e. when K is $\mathbb{Q}$ or a quadratic imaginary field.
- When $r+s>1$ let $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ be a system of fundamental units for $\mathcal{O}_K^*$ i.e. $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ is a basis of the free abelian group $\lambda(\mathcal{O}_K^*)$. Then the regulator R is the absolute value of the determinant of any $(r+s-1)\times(r+s-1)$ submatrix of the $(r+s)\times(r+s-1)$ matrix

$$\Big(\lambda(\varepsilon_1) \mid \cdots \mid \lambda(\varepsilon_{r+s-1})\Big).$$

- Note that when $r+s=2$ (so $\mathcal{O}_K^*$ modulo torsion is cyclic) the regulator is the absolute value of the logarithm of a fundamental unit.

- When $K = \mathbb{Q}$ we have $r = 1$, $s = 0$, $w_K = 2$, $h_K = 1$, $|d_K| = 1$ and the class number formula then says that the residue of $\zeta(s)$ at $s = 1$, which is 1, must be equal to $\dfrac{2^{1+0} \times 1 \times 1}{2 \times \sqrt{1}}$.
- If $K = \mathbb{Q}(\sqrt{-d})$ where d is a squarefree positive integer. Then $r = 0$, $s = 1$, $R = 1$, w_K is 2 (resp. 4, 6) when $d \geq 5$ (resp. $d = 1$, $d = 3$) and d_K is $-d$ or $-4d$ according as $d \equiv 3 \pmod 4$ or $d \equiv 1, 2 \pmod 4$.

  Suppose now $K = \mathbb{Q}(\sqrt{-q})$ where $q \equiv 3 \pmod 4$ is a prime bigger than 3, we get $\dfrac{2h_K}{2q} = L(1, \chi)$ where $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ is the unique character of order 2. So we can find the class number by evaluating the series $\sum \frac{1}{n} \left(\frac{n}{q}\right)$.

- When $K=\mathbb{Q}$ we have $r = 1$, $s = 0$, $w_K = 2$, $h_K = 1$, $|d_K| = 1$ and the class number formula then says that the residue of $\zeta(s)$ at $s = 1$, which is 1, must be equal to $\dfrac{2^{1+0} \times 1 \times 1}{2 \times \sqrt{1}}$.
- If $K = \mathbb{Q}(\sqrt{-d})$ where d is a squarefree positive integer. Then $r = 0$, $s = 1$, $R = 1$, w_K is 2 (resp. 4, 6) when $d \geq 5$ (resp. $d = 1$, $d = 3$) and d_K is $-d$ or $-4d$ according as $d \equiv 3 \pmod 4$ or $d \equiv 1, 2 \pmod 4$.

Suppose now $K = \mathbb{Q}(\sqrt{-q})$ where $q \equiv 3 \pmod 4$ is a prime bigger than 3, we get $\dfrac{2h_K}{2q} = L(1, \chi)$ where $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ is the unique character of order 2. So we can find the class number by evaluating the series $\sum \dfrac{1}{n} \left(\dfrac{n}{q}\right)$.

- When $K = \mathbb{Q}$ we have $r = 1$, $s = 0$, $w_K = 2$, $h_K = 1$, $|d_K| = 1$ and the class number formula then says that the residue of $\zeta(s)$ at $s = 1$, which is 1, must be equal to $\dfrac{2^{1+0} \times 1 \times 1}{2 \times \sqrt{1}}$.
- If $K = \mathbb{Q}(\sqrt{-d})$ where d is a squarefree positive integer. Then $r = 0$, $s = 1$, $R = 1$, w_K is 2 (resp. 4, 6) when $d \geq 5$ (resp. $d = 1$, $d = 3$) and d_K is $-d$ or $-4d$ according as $d \equiv 3 \pmod{4}$ or $d \equiv 1, 2 \pmod{4}$.

  Suppose now $K = \mathbb{Q}(\sqrt{-q})$ where $q \equiv 3 \pmod{4}$ is a prime bigger than 3, we get $\dfrac{2h_K}{2q} = L(1, \chi)$ where $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ is the unique character of order 2. So we can find the class number by evaluating the series $\sum \dfrac{1}{n}\left(\dfrac{n}{q}\right)$.

Computing $L(1,\chi)$

Let q be an odd prime and let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ be a non-trivial character. Fix $\zeta = e^{\frac{2\pi i}{q}}$ and define the Gauss sum $\tau(\chi) := \sum_{a=1}^{q-1} \chi(a)\zeta^a$. We then have

$\tau(\chi)\overline{\tau(\chi)} = q$ and $\chi(n) = \frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na}$. Hence

$$L(1,\chi) = \frac{\tau(\chi)}{q} \sum_{n=1}^{\infty} \frac{1}{n} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na} = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{-a})$$

where $\log$ is assumed to be valued on $-\pi < \mathrm{Im} \log z < \pi$. We can then use $L(1,\chi) = -\frac{\chi(-1)\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{a})$ to deduce the following:

Computing $L(1,\chi)$

Let q be an odd prime and let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ be a non-trivial character. Fix $\zeta = e^{\frac{2\pi i}{q}}$ and define the Gauss sum $\tau(\chi) := \sum_{a=1}^{q-1} \chi(a)\zeta^a$. We then have

$\tau(\chi)\overline{\tau(\chi)} = q$ and $\chi(n) = \frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na}$. Hence

$$L(1,\chi) = \frac{\tau(\chi)}{q} \sum_{n=1}^{\infty} \frac{1}{n} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na} = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{-a})$$

where $\log$ is assumed to be valued on $-\pi < \operatorname{Im} \log z < \pi$. We can then use $L(1,\chi) = -\frac{\chi(-1)\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{a})$ to deduce the following:

- If $\chi(-1) = 1$ then $L(1,\chi) = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log \sin \frac{\pi a}{q}$.

Computing $L(1,\chi)$

Let q be an odd prime and let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ be a non-trivial character. Fix $\zeta = e^{\frac{2\pi i}{q}}$ and define the Gauss sum $\tau(\chi) := \sum_{a=1}^{q-1} \chi(a)\zeta^a$. We then have $\tau(\chi)\overline{\tau(\chi)} = q$ and $\chi(n) = \frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na}$. Hence

$$L(1,\chi) = \frac{\tau(\chi)}{q} \sum_{n=1}^{\infty} \frac{1}{n} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na} = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{-a})$$

where $\log$ is assumed to be valued on $-\pi < \operatorname{Im} \log z < \pi$. We can then use $L(1,\chi) = -\frac{\chi(-1)\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^a)$ to deduce the following:

- If $\chi(-1) = 1$ then $L(1,\chi) = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log \sin \frac{\pi a}{q}$.
- If $\chi(-1) = -1$ then $L(1,\chi) = -\frac{i\pi\tau(\chi)}{q^2} \sum_{a=1}^{q-1} \overline{\chi}(a) k$.

Computing $L(1,\chi)$

Let q be an odd prime and let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ be a non-trivial character. Fix $\zeta = e^{\frac{2\pi i}{q}}$ and define the Gauss sum $\tau(\chi) := \sum_{a=1}^{q-1} \chi(a)\zeta^a$. We then have $\tau(\chi)\overline{\tau(\chi)} = q$ and $\chi(n) = \frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na}$. Hence

$$L(1,\chi) = \frac{\tau(\chi)}{q} \sum_{n=1}^{\infty} \frac{1}{n} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na} = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{-a})$$

where $\log$ is assumed to be valued on $-\pi < \operatorname{Im} \log z < \pi$. We can then use $L(1,\chi) = -\frac{\chi(-1)\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^a)$ to deduce the following:

- If $\chi(-1) = 1$ then $L(1,\chi) = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log \sin \frac{\pi a}{q}$.
- If $\chi(-1) = -1$ then $L(1,\chi) = -\frac{i\pi\tau(\chi)}{q^2} \sum_{a=1}^{q-1} \overline{\chi}(a) k$.

Computing $L(1,\chi)$

Let q be an odd prime and let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ be a non-trivial character. Fix $\zeta = e^{\frac{2\pi i}{q}}$ and define the Gauss sum $\tau(\chi) := \sum_{a=1}^{q-1} \chi(a)\zeta^a$. We then have $\tau(\chi)\overline{\tau(\chi)} = q$ and $\chi(n) = \frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na}$. Hence

$$L(1,\chi) = \frac{\tau(\chi)}{q} \sum_{n=1}^{\infty} \frac{1}{n} \sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na} = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{-a})$$

where $\log$ is assumed to be valued on $-\pi < \operatorname{Im} \log z < \pi$. We can then use $L(1,\chi) = -\frac{\chi(-1)\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log(1-\zeta^{a})$ to deduce the following:

- If $\chi(-1) = 1$ then $L(1,\chi) = -\frac{\tau(\chi)}{q} \sum_{a=1}^{q-1} \overline{\chi}(a) \log \sin \frac{\pi a}{q}$.
- If $\chi(-1) = -1$ then $L(1,\chi) = -\frac{i\pi\tau(\chi)}{q^2} \sum_{a=1}^{q-1} \overline{\chi}(a) k$.

Computing $L(1,\chi)$

Let q be an odd prime and let $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ be a non-trivial character. Fix $\zeta = e^{\frac{2\pi i}{q}}$ and define the Gauss sum $\tau(\chi) := \sum_{a=1}^{q-1} \chi(a)\zeta^a$. We then have $\tau(\chi)\overline{\tau(\chi)} = q$ and $\chi(n) = \frac{\tau(\chi)}{q}\sum_{a=1}^{q-1} \overline{\chi}(a)\zeta^{-na}$. Hence

$$L(1,\chi) = \frac{\tau(\chi)}{q}\sum_{n=1}^{\infty}\frac{1}{n}\sum_{a=1}^{q-1}\overline{\chi}(a)\zeta^{-na} = -\frac{\tau(\chi)}{q}\sum_{a=1}^{q-1}\overline{\chi}(a)\log(1-\zeta^{-a})$$

where $\log$ is assumed to be valued on $-\pi < \operatorname{Im}\log z < \pi$. We can then use $L(1,\chi) = -\frac{\chi(-1)\tau(\chi)}{q}\sum_{a=1}^{q-1}\overline{\chi}(a)\log(1-\zeta^a)$ to deduce the following:

- If $\chi(-1) = 1$ then $L(1,\chi) = -\frac{\tau(\chi)}{q}\sum_{a=1}^{q-1}\overline{\chi}(a)\log\sin\dfrac{\pi a}{q}$.
- If $\chi(-1) = -1$ then $L(1,\chi) = -\frac{i\pi\tau(\chi)}{q^2}\sum_{a=1}^{q-1}\overline{\chi}(a)k$.

Let K be a number field of degree $[K:\mathbb{Q}] = n$. We fix the following notation

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.
- d_K is the discriminant of K.
- h, R and w respectively denotes the class number of K, the regulator of K and the number of roots of unity in K.

We shall sketch the main ideas involved in proving the analytic class number formula: we indicate how to prove that $\zeta_K(z) := \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \mathbf{N}I^{-z}$ converges and defines an analytic function for $\mathrm{Re}(z) > 1$ and why

$$\lim_{z \to 1+} (z-1)\zeta_K(z) = \frac{2^{r+s}\pi^s hR}{w\sqrt{|d_K|}}.$$

Let K be a number field of degree $[K:\mathbb{Q}] = n$. We fix the following notation

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.
- d_K is the discriminant of K.
- h, R and w respectively denotes the class number of K, the regulator of K and the number of roots of unity in K.

We shall sketch the main ideas involved in proving the analytic class number formula: we indicate how to prove that $\zeta_K(z) := \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \mathbf{N}I^{-z}$ converges and defines an analytic function for $\mathrm{Re}(z) > 1$ and why

$$\lim_{z \to 1+} (z-1)\zeta_K(z) = \frac{2^{r+s}\pi^s hR}{w\sqrt{|d_K|}}.$$

Let K be a number field of degree $[K:\mathbb{Q}] = n$. We fix the following notation

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.
- d_K is the discriminant of K.
- h, R and w respectively denotes the class number of K, the regulator of K and the number of roots of unity in K.

We shall sketch the main ideas involved in proving the analytic class number formula: we indicate how to prove that $\zeta_K(z) := \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \mathbf{N}I^{-z}$ converges and defines an analytic function for $\mathrm{Re}(z) > 1$ and why

$$\lim_{z \to 1+} (z-1)\zeta_K(z) = \frac{2^{r+s}\pi^s hR}{w\sqrt{|d_K|}}.$$

Let K be a number field of degree $[K:\mathbb{Q}] = n$. We fix the following notation

- r is the number of real embeddings and $2s$ is the number of non-real embeddings. We write

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}, \quad \sigma_1, \ldots, \sigma_s, \overline{\sigma}_1, \ldots, \overline{\sigma}_s : K \to \mathbb{C}$$

  for the real and non-real embeddings.
- d_K is the discriminant of K.
- h, R and w respectively denotes the class number of K, the regulator of K and the number of roots of unity in K.

We shall sketch the main ideas involved in proving the analytic class number formula: we indicate how to prove that $\zeta_K(z) := \sum_{0 \neq I \trianglelefteq \mathcal{O}_K} \mathbf{N}I^{-z}$ converges and defines an analytic function for $\mathrm{Re}(z) > 1$ and why

$$\lim_{z \to 1+} (z-1)\zeta_K(z) = \frac{2^{r+s}\pi^s hR}{w\sqrt{|d_K|}}.$$

Let $\mathcal{C}$ be an equivalence class of ideals in $\mathcal{O}_K$ and consider $\zeta_{\mathcal{C}}(z) := \sum_{I \in \mathcal{C}} \mathbf{N}I^{-z}$.

Now fix an ideal $A \in \mathcal{C}^{-1}$. Then the association $I \to IA$ sets up a one to one correspondence between

$$\text{ideals} \quad I \in \mathcal{C} \longleftrightarrow \text{principal ideals} \quad 0 \neq (a) \subseteq A.$$

This gives $\zeta_{\mathcal{C}}(z) = (\mathbf{N}A)^z \zeta_A(z)$ where

$$\zeta_A(z) := \sum_{0 \neq (a) \subseteq A} \mathbf{N}(a)^{-z}.$$

Our result will follow if we can show that $\zeta_A(z)$ is analytic for $\mathrm{Re}(z) > 1$ and

$$\lim_{z \to 1+} (z-1)\zeta_A(z) = \frac{2^{r+s}\pi^s R}{\mathbf{N}(A) w \sqrt{|d_K|}}.$$

Dealing with principal ideals is almost the same as dealing with their generators except that we need to worry about associates. Clearly if we can find a way of choosing generators systematically then the series above should become easier to deal with.

Let $\mathcal{C}$ be an equivalence class of ideals in $\mathcal{O}_K$ and consider $\zeta_{\mathcal{C}}(z) := \sum_{I \in \mathcal{C}} \mathbf{N} I^{-z}$.

Now fix an ideal $A \in \mathcal{C}^{-1}$. Then the association $I \to IA$ sets up a one to one correspondence between

$$\text{ideals} \quad I \in \mathcal{C} \dashleftarrow\dashrightarrow \text{principal ideals} \quad 0 \neq (a) \subseteq A.$$

This gives $\zeta_{\mathcal{C}}(z) = (\mathbf{N}A)^z \zeta_A(z)$ where

$$\zeta_A(z) := \sum_{0 \neq (a) \subseteq A} \mathbf{N}(a)^{-z}.$$

Our result will follow if we can show that $\zeta_A(z)$ is analytic for $\mathrm{Re}(z) > 1$ and

$$\lim_{z \to 1+} (z-1)\zeta_A(z) = \frac{2^{r+s}\pi^s R}{\mathbf{N}(A) w \sqrt{|d_K|}}.$$

Dealing with principal ideals is almost the same as dealing with their generators except that we need to worry about associates. Clearly if we can find a way of choosing generators systematically then the series above should become easier to deal with.

Let $\mathcal{C}$ be an equivalence class of ideals in $\mathcal{O}_K$ and consider $\zeta_{\mathcal{C}}(z) := \sum_{I \in \mathcal{C}} \mathbf{N} I^{-z}$.

Now fix an ideal $A \in \mathcal{C}^{-1}$. Then the association $I \to IA$ sets up a one to one correspondence between

$$\text{ideals} \quad I \in \mathcal{C} \dashleftarrow\dashrightarrow \text{principal ideals} \quad 0 \neq (a) \subseteq A.$$

This gives $\zeta_{\mathcal{C}}(z) = (\mathbf{N}A)^z \zeta_A(z)$ where

$$\zeta_A(z) := \sum_{0 \neq (a) \subseteq A} \mathbf{N}(a)^{-z}.$$

Our result will follow if we can show that $\zeta_A(z)$ is analytic for $\mathrm{Re}(z) > 1$ and

$$\lim_{z \to 1+} (z-1)\zeta_A(z) = \frac{2^{r+s}\pi^s R}{\mathbf{N}(A) w \sqrt{|d_K|}}.$$

Dealing with principal ideals is almost the same as dealing with their generators except that we need to worry about associates. Clearly if we can find a way of choosing generators systematically then the series above should become easier to deal with.

Let $\mathcal{C}$ be an equivalence class of ideals in $\mathcal{O}_K$ and consider $\zeta_{\mathcal{C}}(z) := \sum_{I \in \mathcal{C}} \mathbf{N}I^{-z}$.
Now fix an ideal $A \in \mathcal{C}^{-1}$. Then the association $I \to IA$ sets up a one to one correspondence between

$$\text{ideals} \quad I \in \mathcal{C} \dashleftarrow\dashrightarrow \text{principal ideals} \quad 0 \neq (a) \subseteq A.$$

This gives $\zeta_{\mathcal{C}}(z) = (\mathbf{N}A)^z \zeta_A(z)$ where

$$\zeta_A(z) := \sum_{0 \neq (a) \subseteq A} \mathbf{N}(a)^{-z}.$$

Our result will follow if we can show that $\zeta_A(z)$ is analytic for $\mathrm{Re}(z) > 1$ and

$$\lim_{z \to 1+} (z-1)\zeta_A(z) = \frac{2^{r+s}\pi^s R}{\mathbf{N}(A) w \sqrt{|d_K|}}.$$

Dealing with principal ideals is almost the same as dealing with their generators except that we need to worry about associates. Clearly if we can find a way of choosing generators systematically then the series above should become easier to deal with.

We write $\begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix}$ for the vector $(t_1, \ldots, z_1, \ldots)^T \in \mathbb{R}^r \times \mathbb{C}^s$. Define a *norm map* $\| - \| : \mathbb{R}^r \times \mathbb{C}^s \to [0, \infty)$ by $\| \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} \| := |t_1| \cdots |t_r||z_1|^2 \cdots |z_s|^2$. The ring homomorphism $j : K \to \mathbb{R}^r \times \mathbb{C}^s$ given by

$$j(a) := \begin{bmatrix} \rho_\bullet(a) \\ \sigma_\bullet(a) \end{bmatrix} = (\rho_1(a), \ldots, \rho_r(a), \sigma_1(a), \ldots, \sigma_s(a))^T$$

is an injection and $j(K^*) \subseteq (\mathbb{R}^r \times \mathbb{C}^s)^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$. Note that $\|j(a)\| = |\mathbf{N}(a)|$.

The first step now is to find a fundamental domain D for the action of $\mathcal{O}^*$ on $(\mathbb{R}^r \times \mathbb{C}^s)^*$. Then the points in $j(A) \cap D$ will correspond to principal ideals in A. We will actually work with something quite close to D instead, namely a fundamental domain for the action of the free part of $\mathcal{O}^*$.

Fix a system of fundamental units $u_1, \ldots, u_{r+s-1} \in \mathcal{O}^*$; thus we can express $\mathcal{O}^*$ as $\mu(K) u_1^{\mathbb{Z}} \cdots u_{r+s-1}^{\mathbb{Z}}$. Now define $u_i^* \in (\mathbb{R}^r \times \mathbb{C}^s)^*$, $i = 1, \ldots, r+s$, via

$$u_i^* = \begin{bmatrix} |\rho_\bullet(u_i)| \\ |\sigma_\bullet(u_i)| \end{bmatrix}, i = 1, \ldots, r+s-1, \quad \text{and} \quad u_{r+s}^* = \begin{bmatrix} e \\ \vdots \\ e \end{bmatrix}.$$

We write $\begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix}$ for the vector $(t_1, \dots, z_1, \dots)^T \in \mathbb{R}^r \times \mathbb{C}^s$. Define a *norm map* $\| - \| : \mathbb{R}^r \times \mathbb{C}^s \to [0, \infty)$ by $\| \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} \| := |t_1| \cdots |t_r||z_1|^2 \cdots |z_s|^2$. The ring homomorphism $j : K \to \mathbb{R}^r \times \mathbb{C}^s$ given by

$$j(a) := \begin{bmatrix} \rho_\bullet(a) \\ \sigma_\bullet(a) \end{bmatrix} = (\rho_1(a), \dots, \rho_r(a), \sigma_1(a), \dots, \sigma_s(a))^T$$

is an injection and $j(K^*) \subseteq (\mathbb{R}^r \times \mathbb{C}^s)^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$. Note that $\|j(a)\| = |\mathbf{N}(a)|$.

The first step now is to find a fundamental domain D for the action of $\mathcal{O}^*$ on $(\mathbb{R}^r \times \mathbb{C}^s)^*$. Then the points in $j(A) \cap D$ will correspond to principal ideals in A. We will actually work with something quite close to D instead, namely a fundamental domain for the action of the free part of $\mathcal{O}^*$.

Fix a system of fundamental units $u_1, \dots, u_{r+s-1} \in \mathcal{O}^*$; thus we can express $\mathcal{O}^*$ as $\mu(K) u_1^{\mathbb{Z}} \cdots u_{r+s-1}^{\mathbb{Z}}$. Now define $u_i^* \in (\mathbb{R}^r \times \mathbb{C}^s)^*$, $i = 1, \dots, r+s$, via

$$u_i^* = \begin{bmatrix} |\rho_\bullet(u_i)| \\ |\sigma_\bullet(u_i)| \end{bmatrix}, i = 1, \dots, r+s-1, \quad \text{and} \quad u_{r+s}^* = \begin{bmatrix} e \\ \vdots \\ e \end{bmatrix}.$$

We write $\begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix}$ for the vector $(t_1, \ldots, z_1, \ldots)^T \in \mathbb{R}^r \times \mathbb{C}^s$. Define a *norm map* $\| - \| : \mathbb{R}^r \times \mathbb{C}^s \to [0, \infty)$ by $\| \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} \| := |t_1| \cdots |t_r| |z_1|^2 \cdots |z_s|^2$. The ring homomorphism $j : K \to \mathbb{R}^r \times \mathbb{C}^s$ given by

$$j(a) := \begin{bmatrix} \rho_\bullet(a) \\ \sigma_\bullet(a) \end{bmatrix} = (\rho_1(a), \ldots, \rho_r(a), \sigma_1(a), \ldots, \sigma_s(a))^T$$

is an injection and $j(K^*) \subseteq (\mathbb{R}^r \times \mathbb{C}^s)^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$. Note that $\|j(a)\| = |\mathbf{N}(a)|$.

The first step now is to find a fundamental domain D for the action of $\mathcal{O}^*$ on $(\mathbb{R}^r \times \mathbb{C}^s)^*$. Then the points in $j(A) \cap D$ will correspond to principal ideals in A. We will actually work with something quite close to D instead, namely a fundamental domain for the action of the free part of $\mathcal{O}^*$.

Fix a system of fundamental units $u_1, \ldots, u_{r+s-1} \in \mathcal{O}^*$; thus we can express $\mathcal{O}^*$ as $\mu(K) u_1^{\mathbb{Z}} \cdots u_{r+s-1}^{\mathbb{Z}}$. Now define $u_i^* \in (\mathbb{R}^r \times \mathbb{C}^s)^*$, $i = 1, \ldots, r+s$, via

$$u_i^* = \begin{bmatrix} |\rho_\bullet(u_i)| \\ |\sigma_\bullet(u_i)| \end{bmatrix}, i = 1, \ldots, r+s-1, \quad \text{and} \quad u_{r+s}^* = \begin{bmatrix} e \\ \vdots \\ e \end{bmatrix}.$$

Next define $\log : (\mathbb{R}^r \times \mathbb{C}^s)^* \to \mathbb{R}^{s+t}$ by $\log \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} = \begin{bmatrix} \log |t_\bullet| \\ 2\log |z_\bullet| \end{bmatrix}$. This is a group homomorphism (from a multiplicative one to an additive group). Vectors in the kernel can be written as

$$(\pm 1, \ldots, \pm 1, e^{i\theta_1}, \ldots, e^{i\theta_s})^T, \quad 0 \le \theta_1, \ldots, \theta_s < 2\pi;$$

they have norm 1. By Dirichlet's unit theorem we see that $\log u_i^*$, $i = 1, \ldots, r+s$ is a basis of $\mathbb{R}^{r+s}$.

Now define X to be the vectors $v \in (\mathbb{R}^r \times \mathbb{C}^s)^*$ such that

$$\log v = l_1 \log u_1^* + \ldots + l_{r+s-1} \log u_{r+s-1}^* + l_{r+s} \log u_{r+s}^*$$

with $0 \le l_1, \ldots, l_{r+s-1} < 1$. It is then easy to check that

- X is a cone i.e. $v \in X$, $r > 0$, implies $rv \in X$;
- X is a set of coset representatives for $(\mathbb{R}^r \times \mathbb{C}^s)^* / u_1^{*\mathbb{Z}} \ldots u_{r+s-1}^{*\mathbb{Z}}$;

Next define $\log : (\mathbb{R}^r \times \mathbb{C}^s)^* \to \mathbb{R}^{s+t}$ by $\log \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} = \begin{bmatrix} \log |t_\bullet| \\ 2\log |z_\bullet| \end{bmatrix}$. This is a group homomorphism (from a multiplicative one to an additive group). Vectors in the kernel can be written as

$$(\pm 1, \ldots, \pm 1, e^{i\theta_1}, \ldots, e^{i\theta_s})^T, \quad 0 \le \theta_1, \ldots, \theta_s < 2\pi;$$

they have norm 1. By Dirichlet's unit theorem we see that $\log u_i^*$, $i = 1, \ldots, r+s$ is a basis of $\mathbb{R}^{r+s}$.
Now define X to be the vectors $v \in (\mathbb{R}^r \times \mathbb{C}^s)^*$ such that

$$\log v = l_1 \log u_1^* + \ldots + l_{r+s-1} \log u_{r+s-1}^* + l_{r+s} \log u_{r+s}^*$$

with $0 \le l_1, \ldots, l_{r+s-1} < 1$. It is then easy to check that

- X is a cone i.e. $v \in X$, $r > 0$, implies $rv \in X$;
- X is a set of coset representatives for $(\mathbb{R}^r \times \mathbb{C}^s)^* / {u_1^*}^{\mathbb{Z}} \ldots {u_{r+s-1}^*}^{\mathbb{Z}}$;
- Let $v \in X$. If $u \in \mathcal{O}^*$ is such that $j(u)v \in X$ then $u \in \mu(K)$. Consequently the number of principal ideals $(a) \subseteq A$ with $\mathbf{N}(a) = N$ is $|\{x \in j(A) \cap X \ : \ \|x\| = N\}|/w$.

Next define $\log : (\mathbb{R}^r \times \mathbb{C}^s)^* \to \mathbb{R}^{s+t}$ by $\log \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} = \begin{bmatrix} \log |t_\bullet| \\ 2\log |z_\bullet| \end{bmatrix}$. This is a group homomorphism (from a multiplicative one to an additive group). Vectors in the kernel can be written as

$$(\pm 1, \ldots, \pm 1, e^{i\theta_1}, \ldots, e^{i\theta_s})^T, \quad 0 \le \theta_1, \ldots, \theta_s < 2\pi;$$

they have norm 1. By Dirichlet's unit theorem we see that $\log u_i^*$, $i = 1, \ldots, r+s$ is a basis of $\mathbb{R}^{r+s}$.
Now define X to be the vectors $v \in (\mathbb{R}^r \times \mathbb{C}^s)^*$ such that

$$\log v = l_1 \log u_1^* + \ldots + l_{r+s-1} \log u_{r+s-1}^* + l_{r+s} \log u_{r+s}^*$$

with $0 \le l_1, \ldots, l_{r+s-1} < 1$. It is then easy to check that

- X is a cone i.e. $v \in X$, $r > 0$, implies $rv \in X$;
- X is a set of coset representatives for $(\mathbb{R}^r \times \mathbb{C}^s)^* / {u_1^*}^{\mathbb{Z}} \ldots {u_{r+s-1}^*}^{\mathbb{Z}}$;
- Let $v \in X$. If $u \in \mathcal{O}^*$ is such that $j(u)v \in X$ then $u \in \mu(K)$. Consequently the number of principal ideals $(a) \subseteq A$ with $\mathbf{N}(a) = N$ is $|\{x \in j(A) \cap X \ : \ \|x\| = N\}|/w$.

Next define $\log : (\mathbb{R}^r \times \mathbb{C}^s)^* \to \mathbb{R}^{s+t}$ by $\log \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} = \begin{bmatrix} \log |t_\bullet| \\ 2\log |z_\bullet| \end{bmatrix}$. This is a group homomorphism (from a multiplicative one to an additive group). Vectors in the kernel can be written as

$$(\pm 1, \ldots, \pm 1, e^{i\theta_1}, \ldots, e^{i\theta_s})^T, \quad 0 \leq \theta_1, \ldots, \theta_s < 2\pi;$$

they have norm 1. By Dirichlet's unit theorem we see that $\log u_i^*$, $i = 1, \ldots, r+s$ is a basis of $\mathbb{R}^{r+s}$.
Now define X to be the vectors $v \in (\mathbb{R}^r \times \mathbb{C}^s)^*$ such that

$$\log v = l_1 \log u_1^* + \ldots + l_{r+s-1} \log u_{r+s-1}^* + l_{r+s} \log u_{r+s}^*$$

with $0 \leq l_1, \ldots, l_{r+s-1} < 1$. It is then easy to check that

- X is a cone i.e. $v \in X$, $r > 0$, implies $rv \in X$;
- X is a set of coset representatives for $(\mathbb{R}^r \times \mathbb{C}^s)^* / {u_1^*}^{\mathbb{Z}} \ldots {u_{r+s-1}^*}^{\mathbb{Z}}$;
- Let $v \in X$. If $u \in \mathcal{O}^*$ is such that $j(u)v \in X$ then $u \in \mu(K)$. Consequently the number of principal ideals $(a) \subseteq A$ with $\mathbf{N}(a) = N$ is $|\{x \in j(A) \cap X \ : \ \|x\| = N\}|/w$.

Next define $\log : (\mathbb{R}^r \times \mathbb{C}^s)^* \to \mathbb{R}^{s+t}$ by $\log \begin{bmatrix} t_\bullet \\ z_\bullet \end{bmatrix} = \begin{bmatrix} \log |t_\bullet| \\ 2\log |z_\bullet| \end{bmatrix}$. This is a group homomorphism (from a multiplicative one to an additive group). Vectors in the kernel can be written as

$$(\pm 1, \dots, \pm 1, e^{i\theta_1}, \dots, e^{i\theta_s})^T, \quad 0 \le \theta_1, \dots, \theta_s < 2\pi;$$

they have norm 1. By Dirichlet's unit theorem we see that $\log u_i^*$, $i = 1, \dots, r+s$ is a basis of $\mathbb{R}^{r+s}$.
Now define X to be the vectors $v \in (\mathbb{R}^r \times \mathbb{C}^s)^*$ such that

$$\log v = l_1 \log u_1^* + \ldots + l_{r+s-1} \log u_{r+s-1}^* + l_{r+s} \log u_{r+s}^*$$

with $0 \le l_1, \dots, l_{r+s-1} < 1$. It is then easy to check that

- X is a cone i.e. $v \in X$, $r > 0$, implies $rv \in X$;
- X is a set of coset representatives for $(\mathbb{R}^r \times \mathbb{C}^s)^* / {u_1^*}^{\mathbb{Z}} \ldots {u_{r+s-1}^*}^{\mathbb{Z}}$;
- Let $v \in X$. If $u \in \mathcal{O}^*$ is such that $j(u)v \in X$ then $u \in \mu(K)$. Consequently the number of principal ideals $(a) \subseteq A$ with $\mathbf{N}(a) = N$ is $|\{x \in j(A) \cap X \ : \ \|x\| = N\}|/w$.

Now let $X(1) := \{x \in X : \|x\| < 1\}$. We can write a vector in X as

$$\alpha {u_1^*}^{l_1} \ldots {u_{r+s}^*}^{l_{r+s}}, \quad 0 \le l_1, \ldots, l_{r+s-1} < 1;$$

the condition that it has norm less than 1 just means $l_{r+s} < 0$. It follows that $X(1)$ is a bounded measurable subset of $\mathbb{R}^r \times \mathbb{C}^s$. Note that $\zeta_A(s) = \frac{1}{w} \sum_{x \in j(A) \cap X} \|x\|^{-z}$. The key assertion is then this series is convergent for $\mathrm{Re}(z) > 1$ and

$$\lim_{z \to 1+} (z-1) \sum_{x \in j(A) \cap X} \|x\|^{-z} = \frac{\mathrm{vol}(X(1))}{\mathrm{vol}(j(A))}.$$

Infact this holds more generally.

Theorem (10.1)

Let Λ be a full lattice in a real Euclidean space $\mathbb{R}^N$, let $0 \notin X$ be a cone in $\mathbb{R}^N$ and let F be a continuous positive real valued function on X homogeneous of degree N i.e. $F(\lambda x) = \lambda^N F(x)$ for all $x \in X, \lambda > 0$. Assume that $X_1 = \{x \in X : F(x) < 1\}$ is bounded and measurable. Then $\sum_{x \in X \cap \Lambda} F(x)^{-z}$ converges and analytic on $Re(z) > 1$. Moreover

$$\lim_{z \to 1+} (z-1) \sum_{x \in X \cap \Lambda} F(x)^{-z} = \frac{vol(X_1)}{vol(\Lambda)}.$$

Now let $X(1) := \{x \in X : \|x\| < 1\}$. We can write a vector in X as

$$\alpha {u_1^*}^{l_1} \dots {u_{r+s}^*}^{l_{r+s}}, \quad 0 \le l_1, \dots, l_{r+s-1} < 1;$$

the condition that it has norm less than 1 just means $l_{r+s} < 0$. It follows that $X(1)$ is a bounded measurable subset of $\mathbb{R}^r \times \mathbb{C}^s$. Note that $\zeta_A(s) = \frac{1}{w} \sum_{x \in j(A) \cap X} \|x\|^{-z}$. The key assertion is then this series is convergent for $\mathrm{Re}(z) > 1$ and

$$\lim_{z \to 1+} (z-1) \sum_{x \in j(A) \cap X} \|x\|^{-z} = \frac{\mathrm{vol}(X(1))}{\mathrm{vol}(j(A))}.$$

Infact this holds more generally.

Theorem (10.1)

Let Λ be a full lattice in a real Euclidean space $\mathbb{R}^N$, let $0 \notin X$ be a cone in $\mathbb{R}^N$ and let F be a continuous positive real valued function on X homogeneous of degree N i.e. $F(\lambda x) = \lambda^N F(x)$ for all $x \in X, \lambda > 0$. Assume that $X_1 = \{x \in X : F(x) < 1\}$ is bounded and measurable. Then $\sum_{x \in X \cap \Lambda} F(x)^{-z}$ converges and analytic on $Re(z) > 1$. Moreover

$$\lim_{z \to 1+} (z-1) \sum_{x \in X \cap \Lambda} F(x)^{-z} = \frac{vol(X_1)}{vol(\Lambda)}.$$

Now the volume of the lattice $j(A)$ is $\mathbf{N}(A)\sqrt{|d_K|}/2^s$. To compute the volume of $X(1)$ use polar co-ordinates to write $z_\bullet$ as $e^{i\theta_\bullet} r_\bullet$. We then need to calculate the integral

$$\int_{X(1)} r_1 \dots r_s dt_1 \dots dt_r dr_1 \dots dr_s d\theta_1 \dots d\theta_s.$$

Let T be the region given by

$$\begin{bmatrix} |\rho_\bullet(u_1)|^{l_1} \dots |\rho_\bullet(u_{r+s-1})|^{l_{r+s-1}} e^{l_{r+s}} \\ e^{i\theta_\bullet} |\sigma_\bullet(u_1)|^{l_1} \dots |\sigma_\bullet(u_{r+s-1})|^{l_{r+s-1}} e^{l_{r+s}} \end{bmatrix}$$

where $0 \le l_1, \dots, l_{r+s-1} < 1$, $l_{r+s} < 0$ and $0 \le \theta_1, \dots \theta_s < 2\pi$. Then $\mathrm{vol}(X(1)) = 2^r \mathrm{vol}(T)$. Change co-rordinates to get

$$\mathrm{vol}(T) = (2\pi)^s \left| \int_{l_1=0}^{1} \cdots \int_{l_{r+s-1}=0}^{1} \int_{l_{r+s}=0}^{-\infty} \frac{\partial(t_\bullet, r_\bullet)}{\partial(l_1, \cdots, l_{r+s})} r_1 \dots r_s dl_1 \dots dl_{r+s} \right|.$$

Now

$$\left| \frac{\partial(t_\bullet, r_\bullet)}{\partial(l_1, \cdots, l_{r+s})} \right| = \frac{1}{2^s} \left| \det \left(\log u_1^* | \cdots \log u_{r+s}^* \right) \right| = \frac{nR}{2^s}$$

and so $\mathrm{vol}(T) = \pi^s R$.

Sketch proof of Theorem 5.1. Let $\mathbb{R}^N, \Lambda, X, F$ be as in the statement of the theorem. For $r > 0$ we set $X(r) := \{x \in X : F(x) \leq r\}$, $a(r) := |\Lambda \cap X(r)|$, $\alpha := \mathrm{vol}(X(1))$, and $\beta := \mathrm{vol}(\Lambda)$.

- The volume of $X(1)$ can be approximated by considering $\frac{1}{r}\Lambda \cap X(1)$, and we can deduce that $\alpha/\beta = \lim_{r\to\infty} a(r)/r$.
- Now order $X \cap \Lambda$ as $x_1, x_2, \ldots$ so that $F(x_1) \leq F(x_2) \leq \ldots$. If $\varepsilon > 0$ then $a(F(x_k) - \varepsilon) < k \leq a(F(x_k))$ for sufficiently large k. It follows that $\alpha/\beta = \lim_{k\to\infty} \dfrac{k}{F(x_k)}$.
- Fix $\varepsilon > 0$. Then $\left(\dfrac{\alpha}{\beta} - \varepsilon\right)\dfrac{1}{k} < \dfrac{1}{F(x_k)} < \left(\dfrac{\alpha}{\beta} + \varepsilon\right)\dfrac{1}{k}$ for sufficiently large k and comparision with $\zeta(z)$ shows that $\sum F(x_k)^{-z}$ converges and is analytic for $\mathrm{Re}(z) > 1$.

Sketch proof of Theorem 5.1. Let $\mathbb{R}^N, \Lambda, X, F$ be as in the statement of the theorem. For $r > 0$ we set $X(r) := \{x \in X : F(x) \leq r\}$, $a(r) := |\Lambda \cap X(r)|$, $\alpha := \mathrm{vol}(X(1))$, and $\beta := \mathrm{vol}(\Lambda)$.

- The volume of $X(1)$ can be approximated by considering $\frac{1}{r}\Lambda \cap X(1)$, and we can deduce that $\alpha/\beta = \lim_{r\to\infty} a(r)/r$.
- Now order $X \cap \Lambda$ as $x_1, x_2, \dots$ so that $F(x_1) \leq F(x_2) \leq \dots$. If $\varepsilon > 0$ then $a(F(x_k) - \varepsilon) < k \leq a(F(x_k))$ for sufficiently large k. It follows that $\alpha/\beta = \lim\limits_{k\to\infty} \dfrac{k}{F(x_k)}$.
- Fix $\varepsilon > 0$. Then $\left(\dfrac{\alpha}{\beta} - \varepsilon\right)\dfrac{1}{k} < \dfrac{1}{F(x_k)} < \left(\dfrac{\alpha}{\beta} + \varepsilon\right)\dfrac{1}{k}$ for sufficiently large k and comparision with $\zeta(z)$ shows that $\sum F(x_k)^{-z}$ converges and is analytic for $\mathrm{Re}(z) > 1$.
- Set $\widehat{\zeta}(z) := \sum_{x \in X\cap\Lambda} F(x)^{-z}$. Using $\lim_{z\to 1+}(z-1)\zeta(z) = 1$ one then deduces that

$$\left(\frac{\alpha}{\beta} - \varepsilon\right) \leq \liminf_{z\to 1+}(z-1)\widehat{\zeta}(z) \leq \limsup_{z\to 1+}(z-1)\widehat{\zeta}(z) \leq \left(\frac{\alpha}{\beta} + \varepsilon\right).$$

As $\varepsilon > 0$ was arbitrary the desired formula for the limit follows.

Sketch proof of Theorem 5.1. Let $\mathbb{R}^N, \Lambda, X, F$ be as in the statement of the theorem. For $r > 0$ we set $X(r) := \{x \in X : F(x) \leq r\}$, $a(r) := |\Lambda \cap X(r)|$, $\alpha := \mathrm{vol}(X(1))$, and $\beta := \mathrm{vol}(\Lambda)$.

- The volume of $X(1)$ can be approximated by considering $\frac{1}{r}\Lambda \cap X(1)$, and we can deduce that $\alpha/\beta = \lim_{r\to\infty} a(r)/r$.
- Now order $X \cap \Lambda$ as $x_1, x_2, \ldots$ so that $F(x_1) \leq F(x_2) \leq \ldots$. If $\varepsilon > 0$ then $a(F(x_k) - \varepsilon) < k \leq a(F(x_k))$ for sufficiently large k. It follows that $\alpha/\beta = \lim\limits_{k\to\infty} \dfrac{k}{F(x_k)}$.
- Fix $\varepsilon > 0$. Then $\left(\dfrac{\alpha}{\beta} - \varepsilon\right)\dfrac{1}{k} < \dfrac{1}{F(x_k)} < \left(\dfrac{\alpha}{\beta} + \varepsilon\right)\dfrac{1}{k}$ for sufficiently large k and comparision with $\zeta(z)$ shows that $\sum F(x_k)^{-z}$ converges and is analytic for $\mathrm{Re}(z) > 1$.
- Set $\widehat{\zeta}(z) := \sum_{x\in X\cap\Lambda} F(x)^{-z}$. Using $\lim_{z\to 1+}(z-1)\zeta(z) = 1$ one then deduces that

$$\left(\frac{\alpha}{\beta} - \varepsilon\right) \leq \liminf_{z\to 1+}(z-1)\widehat{\zeta}(z) \leq \limsup_{z\to 1+}(z-1)\widehat{\zeta}(z) \leq \left(\frac{\alpha}{\beta} + \varepsilon\right).$$

As $\varepsilon > 0$ was arbitrary the desired formula for the limit follows.

Sketch proof of Theorem 5.1. Let $\mathbb{R}^N, \Lambda, X, F$ be as in the statement of the theorem. For $r > 0$ we set $X(r) := \{x \in X : F(x) \leq r\}$, $a(r) := |\Lambda \cap X(r)|$, $\alpha := \mathrm{vol}(X(1))$, and $\beta := \mathrm{vol}(\Lambda)$.

- The volume of $X(1)$ can be approximated by considering $\frac{1}{r}\Lambda \cap X(1)$, and we can deduce that $\alpha/\beta = \lim_{r\to\infty} a(r)/r$.
- Now order $X \cap \Lambda$ as $x_1, x_2, \ldots$ so that $F(x_1) \leq F(x_2) \leq \ldots$. If $\varepsilon > 0$ then $a(F(x_k) - \varepsilon) < k \leq a(F(x_k))$ for sufficiently large k. It follows that $\alpha/\beta = \lim\limits_{k\to\infty} \dfrac{k}{F(x_k)}$.
- Fix $\varepsilon > 0$. Then $\left(\dfrac{\alpha}{\beta} - \varepsilon\right)\dfrac{1}{k} < \dfrac{1}{F(x_k)} < \left(\dfrac{\alpha}{\beta} + \varepsilon\right)\dfrac{1}{k}$ for sufficiently large k and comparision with $\zeta(z)$ shows that $\sum F(x_k)^{-z}$ converges and is analytic for $\mathrm{Re}(z) > 1$.
- Set $\widehat{\zeta}(z) := \sum_{x\in X\cap\Lambda} F(x)^{-z}$. Using $\lim_{z\to1+}(z-1)\zeta(z) = 1$ one then deduces that

$$\left(\frac{\alpha}{\beta} - \varepsilon\right) \leq \liminf_{z\to1+}(z-1)\widehat{\zeta}(z) \leq \limsup_{z\to1+}(z-1)\widehat{\zeta}(z) \leq \left(\frac{\alpha}{\beta} + \varepsilon\right).$$

As $\varepsilon > 0$ was arbitrary the desired formula for the limit follows.

Sketch proof of Theorem 5.1. Let $\mathbb{R}^N, \Lambda, X, F$ be as in the statement of the theorem. For $r > 0$ we set $X(r) := \{x \in X : F(x) \leq r\}$, $a(r) := |\Lambda \cap X(r)|$, $\alpha := \mathrm{vol}(X(1))$, and $\beta := \mathrm{vol}(\Lambda)$.

- The volume of $X(1)$ can be approximated by considering $\frac{1}{r}\Lambda \cap X(1)$, and we can deduce that $\alpha/\beta = \lim_{r\to\infty} a(r)/r$.
- Now order $X \cap \Lambda$ as $x_1, x_2, \ldots$ so that $F(x_1) \leq F(x_2) \leq \ldots$. If $\varepsilon > 0$ then $a(F(x_k) - \varepsilon) < k \leq a(F(x_k))$ for sufficiently large k. It follows that $\alpha/\beta = \lim\limits_{k\to\infty} \dfrac{k}{F(x_k)}$.
- Fix $\varepsilon > 0$. Then $\left(\dfrac{\alpha}{\beta} - \varepsilon\right)\dfrac{1}{k} < \dfrac{1}{F(x_k)} < \left(\dfrac{\alpha}{\beta} + \varepsilon\right)\dfrac{1}{k}$ for sufficiently large k and comparision with $\zeta(z)$ shows that $\sum F(x_k)^{-z}$ converges and is analytic for $\mathrm{Re}(z) > 1$.
- Set $\widehat{\zeta}(z) := \sum_{x\in X\cap\Lambda} F(x)^{-z}$. Using $\lim_{z\to 1+}(z-1)\zeta(z) = 1$ one then deduces that

$$\left(\frac{\alpha}{\beta} - \varepsilon\right) \leq \liminf_{z\to 1+}(z-1)\widehat{\zeta}(z) \leq \limsup_{z\to 1+}(z-1)\widehat{\zeta}(z) \leq \left(\frac{\alpha}{\beta} + \varepsilon\right).$$

  As $\varepsilon > 0$ was arbitrary the desired formula for the limit follows.