Lecture 3: Lattices from Number Fields

F. Oggier

Journées Algébriques du Gabon, Libreville, Mars 2025

A number field K is a finite extension of $\mathbb{Q}$. We will focus on two families of number fields:

- Quadratic fields
- Cyclotomic fields

For $d > 1$ a squarefree integer, consider the *quadratic* field

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d},\ a, b \in \mathbb{Q}\}$$

which has degree 2, that is dimension 2 as a vector space over $\mathbb{Q}$.

- There are two meaningful ways of embedding $\mathbb{Q}(\sqrt{d})$ into $\mathbb{R}$:

$$\begin{aligned} \sigma_1 : &\quad a + b\sqrt{d} \mapsto a + b\sqrt{d} \\ \sigma_2 : &\quad a + b\sqrt{d} \mapsto a - b\sqrt{d} \end{aligned}$$

- In fact, σ_1, σ_2 are the only two maps that satisfy (1) $\tau(x + y) = \tau(x) + \tau(y)$ and $\tau(xy) = \tau(x)\tau(y)$ for all $x, y \in \mathbb{Q}(\sqrt{d})$, (2) $\tau(a) = a$ for any $a \in \mathbb{Q}$:

$$\tau\left((\sqrt{d})^2\right) = \begin{cases} \tau(d) = d \\ \tau(\sqrt{d})^2 \end{cases}$$

and thus $\tau(\sqrt{d})$ must satisfy

$$\tau(\sqrt{d})^2 - d = 0$$

showing that $\tau(\sqrt{d}) = \pm\sqrt{d}$.

- Let K be a number field, that is a finite extension of degree $[K : \mathbb{Q}] = n < \infty$ over $\mathbb{Q}$. Then K has dimension n as a vector space over $\mathbb{Q}$.
- For a number field K of degree n, there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis.
- For a number field K of degree n, there are n distinct embeddings of K into $\mathbb{C}$, that is $\{\sigma_1, \ldots, \sigma_n\}$ is the set of embeddings of K containing field homomorphisms of the form $\sigma_m : K \to \mathbb{C}$ fixing $\mathbb{Q}$ for all m.
- Let K be a number field of degree n with s real embeddings and t pairs of complex embeddings, then

$$n = [K : \mathbb{Q}] = s + 2t.$$

- A number field K is called totally real if all embeddings are real embeddings.
  - For $d > 1$, $\mathbb{Q}(\sqrt{d})$ is totally real: $\tau(\sqrt{d}) = \pm\sqrt{d}$.
- A number field K is called CM if there exists a totally real number field $F \subseteq K$ where $[K : F] = 2$ and $\sigma_m(K) \not\subseteq \mathbb{R}$ for all $m = 1, \ldots, n$.

Consider

$$\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d}, a, b, \in \mathbb{Z} \right\},$$

which has a $\mathbb{Z}$-basis, given for example by $\{1, \sqrt{d}\}$. Embedding this basis using $\sigma = (\sigma_1, \sigma_2)$ gives

$$B = \begin{bmatrix} 1 & 1 \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{bmatrix}$$

and integer linear combinations of rows of B do define a lattice (since the two rows are linearly independent). Note that

$$\mathbf{u}B = (u_1, u_2) \begin{bmatrix} 1 & 1 \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{bmatrix} = \begin{bmatrix} \sigma_1(x) & \sigma_2(x) \end{bmatrix},$$

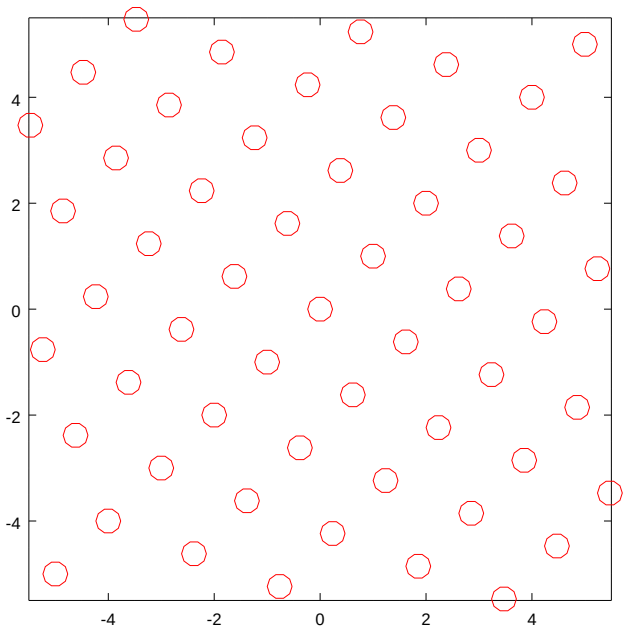
which shows how an element $x = u_1 + u_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is embedded in the lattice $\sigma(\mathbb{Z}[\sqrt{d}])$.

The ring $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{a + b\frac{1+\sqrt{5}}{2},\ a, b \in \mathbb{Z}\}$ is a subset of the field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5},\ a, b \in \mathbb{Q}\}$. The two ways of embedding $\mathbb{Q}(\sqrt{5})$ into $\mathbb{R}$ are:

$$\sigma_1 : \sqrt{5} \mapsto \sqrt{5},\ \sigma_2 : \sqrt{5} \mapsto -\sqrt{5}.$$

We then embed $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ into $\mathbb{R}^2$ using $\sigma = (\sigma_1, \sigma_2)$, to get a generator matrix

$$B = \begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}.$$

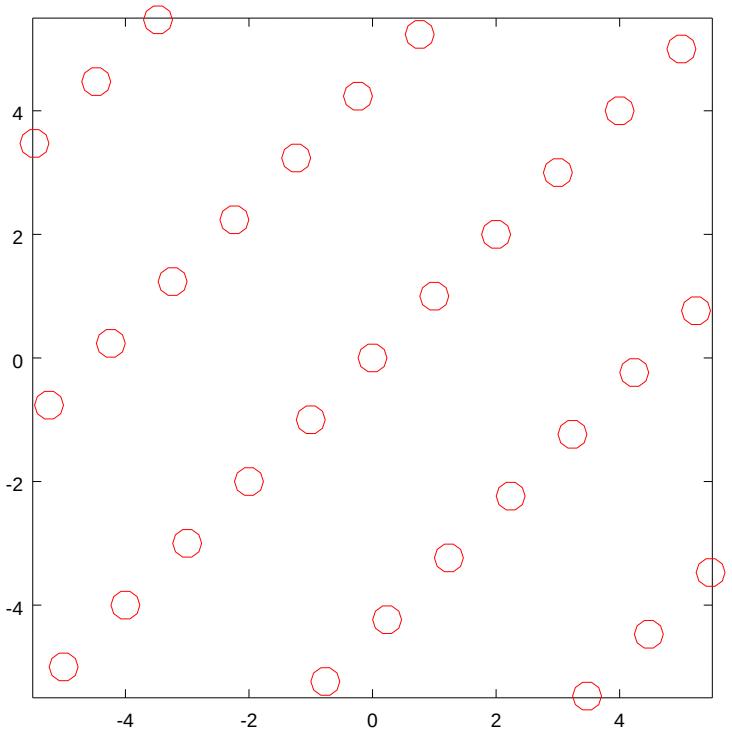


Its corresponding Gram matrix is

$$\begin{aligned} G &= BB^T \\ &= \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}. \end{aligned}$$

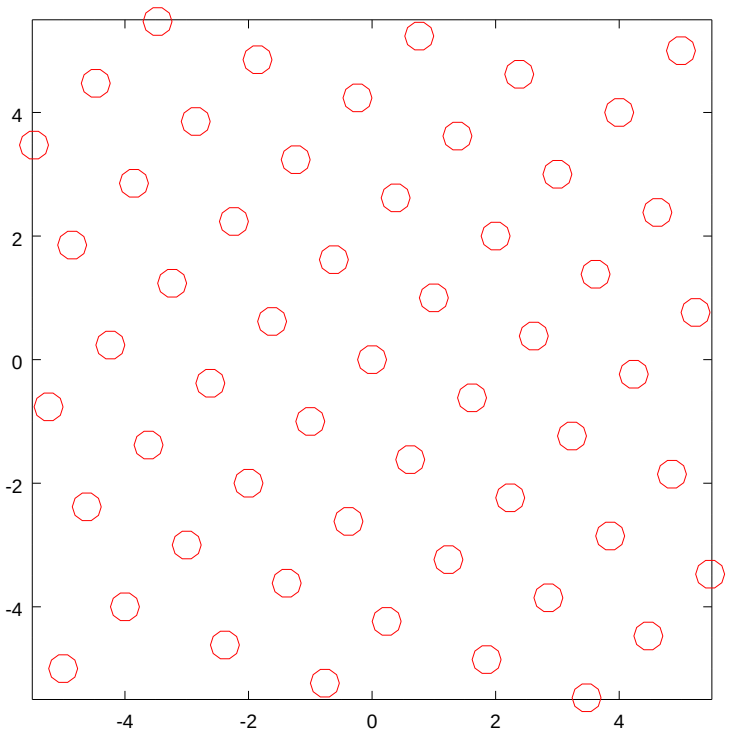
$\sigma(\mathbb{Z}[\sqrt{5}])$:

$$\begin{bmatrix} 2 & 0 \\ 0 & 10 \end{bmatrix}.$$



$\sigma(\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$:

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}.$$



Now for a $\mathbb{Z}$-basis $\{\theta_1, \theta_2\}$ (of respectively $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ depending on the congruence of $d \pmod 4$, or of (an ideal of) an order of these two rings), a Gram matrix is of the form

$$\begin{aligned}
& \begin{bmatrix} \sigma_1(\theta_1) & \sigma_2(\theta_1) \\ \sigma_1(\theta_2) & \sigma_2(\theta_2) \end{bmatrix} \begin{bmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) \end{bmatrix} \\
= & \begin{bmatrix} \sigma_1(\theta_1)^2 + \sigma_2(\theta_1)^2 & \sigma_1(\theta_1)\sigma_1(\theta_2) + \sigma_2(\theta_1)\sigma_2(\theta_2) \\ \sigma_1(\theta_1)\sigma_1(\theta_2) + \sigma_2(\theta_1)\sigma_2(\theta_2) & \sigma_1(\theta_2)^2 + \sigma_2(\theta_2)^2 \end{bmatrix} \\
= & \begin{bmatrix} \sigma_1(\theta_1^2) + \sigma_2(\theta_1^2) & \sigma_1(\theta_1\theta_2) + \sigma_2(\theta_1\theta_2) \\ \sigma_1(\theta_1\theta_2) + \sigma_2(\theta_1\theta_2) & \sigma_1(\theta_2^2) + \sigma_2(\theta_2^2) \end{bmatrix} \\
= & \begin{bmatrix} \mathrm{Tr}(\theta_1^2) & \mathrm{Tr}(\theta_1\theta_2) \\ \mathrm{Tr}(\theta_1\theta_2) & \mathrm{Tr}(\theta_2^2) \end{bmatrix}.
\end{aligned}$$

Coefficients are thus integers.

- Let $\mathcal{O}_K$ be the ring of integers of K, a number field of degree n.
- Then $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank n. A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an integral basis for K.
  - If $K = \mathbb{Q}(\sqrt{5})$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.
- Let $\{\theta_1, \ldots, \theta_n\}$ be an integral basis of K, for K a totally real number field. Then

$$B = \begin{bmatrix} \sigma_1(\theta_1) & \ldots & \sigma_n(\theta_1) \\ \vdots & & \vdots \\ \sigma_1(\theta_n) & \ldots & \sigma_n(\theta_n) \end{bmatrix}$$

is a lattice generator matrix.

For the lattice generator matrix B, we get the Gram matrix

$$BB^T = \begin{bmatrix} \mathrm{Tr}(\theta_1^2) & \dots & \mathrm{Tr}(\theta_1\theta_n) \\ \vdots & & \vdots \\ \mathrm{Tr}(\theta_n\theta_1) & \dots & \mathrm{Tr}(\theta_n^2) \end{bmatrix}$$

This is an integral quadratic form.

We introduce a "twisting" element α such that $\sigma_1(\alpha) > 0$ and $\sigma_2(\alpha) > 0$. Let θ denote $\sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$ depending on $d \pmod 4$.

- A generator matrix of a lattice using a twisting element α is given by

$$B = \begin{bmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\theta) & \sqrt{\sigma_2(\alpha)}\sigma_2(\theta) \end{bmatrix}$$

  and a Gram matrix by

$$BB^T = \begin{bmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha\theta) + \sigma_2(\alpha\theta) \\ \sigma_1(\alpha\theta) + \sigma_2(\alpha\theta) & \sigma_1(\alpha\theta^2) + \sigma_2(\alpha\theta^2) \end{bmatrix}.$$

- The volume of the lattice $\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])$ is given by

$$v(\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])) = \sqrt{|\sigma_1(\alpha)\sigma_2(\alpha)|}\left|\det \begin{bmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\theta) & \sigma_2(\theta) \end{bmatrix}\right|.$$

Take ($\theta = \frac{1+\sqrt{5}}{2}$)

$$\alpha = 3 - \tfrac{1+\sqrt{5}}{2},\ \alpha\theta = -1 + 2\tfrac{1+\sqrt{5}}{2},\ \alpha\theta^2 = 2 + \tfrac{1+\sqrt{5}}{2}.$$

Then a generator matrix of $\sigma(\sqrt{\alpha}\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$ is

$$B = \begin{bmatrix} \sqrt{\alpha} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\alpha}\frac{1+\sqrt{5}}{2} & \sqrt{\sigma_2(\alpha)}\frac{1-\sqrt{5}}{2} \end{bmatrix}$$

with corresponding Gram matrix

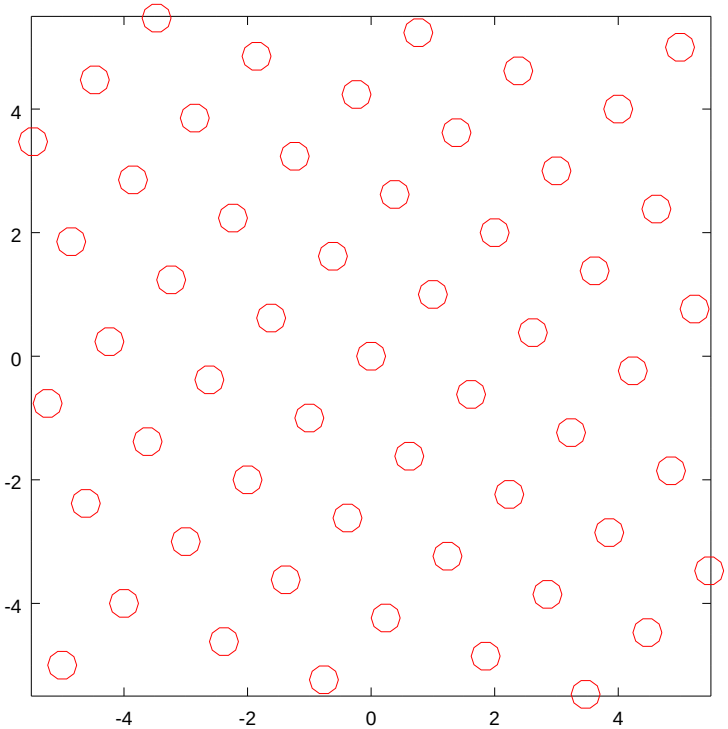
$$\begin{bmatrix} \sigma_1(3 - \frac{1+\sqrt{5}}{2})) + \sigma_2(3 - \frac{1+\sqrt{5}}{2}) & \sigma_1(-1 + 2\frac{1+\sqrt{5}}{2}) + \sigma_2(-1 + 2\frac{1+\sqrt{5}}{2}) \\ \sigma_1(-1 + 2\frac{1+\sqrt{5}}{2}) + \sigma_2(-1 + 2\frac{1+\sqrt{5}}{2}) & \sigma_1(2 + \frac{1+\sqrt{5}}{2}) + \sigma_2(2 + \frac{1+\sqrt{5}}{2}) \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

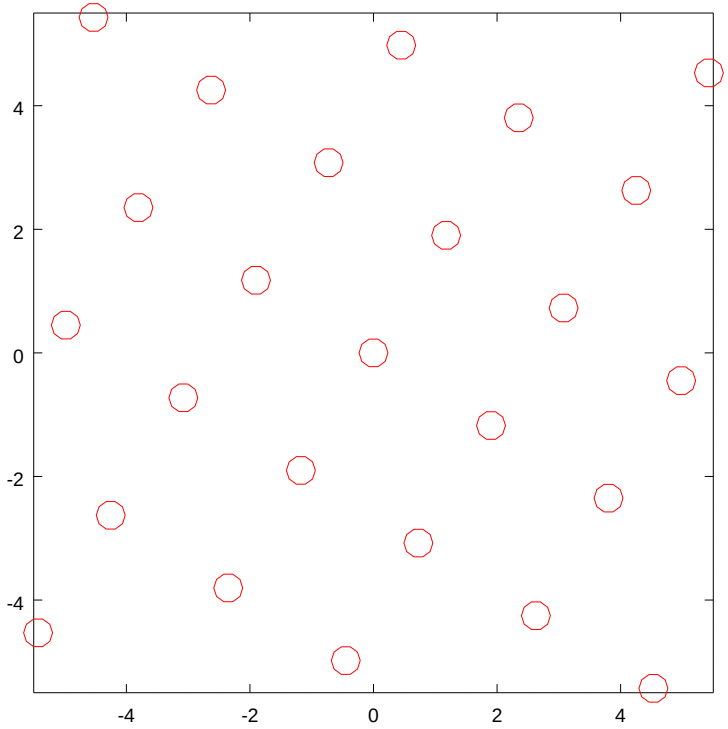
and volume

$$\begin{aligned} v(\sigma(\sqrt{\alpha}\mathbb{Z}[\tfrac{1+\sqrt{5}}{2}])) &= \sqrt{|\sigma_1(\alpha)\sigma_2(\alpha)|}|\sigma_2(\theta) - \sigma_1(\theta)| \\ &= \sqrt{5}|\sqrt{5}| = 5. \end{aligned}$$

This lattice is equivalent to (a scaled version of) $\mathbb{Z}^2$.



The lattice obtained from $\{1, \frac{1+\sqrt{5}}{2}\}$.



The lattice obtained from $\{1, \frac{1+\sqrt{5}}{2}\}$ using a twisting element $\alpha = 3 - \frac{1+\sqrt{5}}{2}$.

An element $\alpha \in K$ is called totally positive if $\sigma_m(\alpha) > 0$ for all embeddings σ_m, $m = 1, \ldots, n$.
The square volume of $\sigma(\sqrt{\alpha}\mathcal{O}_K)$ is

$$N(\alpha)d_K$$

where d_K is the discriminant of K and $N(\alpha)$ is the norm of α.

- In the previous example

$$\sigma_1(\alpha)\sigma_2(\alpha)\det\begin{bmatrix}\sigma_1(1) & \sigma_2(1)\\ \sigma_1(\theta) & \sigma_2(\theta)\end{bmatrix}^2 = N(\alpha)d_K = 25.$$

Consider two generator matrices

$$B_1 = \begin{bmatrix} \sigma_1(\theta_1) & \sigma_2(\theta_1) \\ \sigma_1(\theta_2) & \sigma_2(\theta_2) \end{bmatrix}, \; B_2 = \begin{bmatrix} \tau_1(\nu_1) & \tau_2(\nu_1) \\ \tau_1(\nu_2) & \tau_2(\nu_2) \end{bmatrix}$$

and their Kronecker (tensor) product

$$B_1 \otimes B_2 = \begin{bmatrix} \sigma_1(\theta_1)B_2 & \sigma_2(\theta_1)B_2 \\ \sigma_1(\theta_2)B_2 & \sigma_2(\theta_2)B_2. \end{bmatrix}$$

- This is the generator matrix of a 4-dimensional lattice, since the columns of this matrix are linearly independent (use the determinant of B_1 and B_2).

Suppose that $\tau_i(\theta_j) = \theta_j$ and $\sigma_i(\nu_j) = \nu_j$, and we place ourself in large field, which contains θ_j, ν_j, and for which τ_i, σ_i are embeddings. Then

$$B_1 \otimes B_2 = \begin{bmatrix} \sigma_1\tau_1(\theta_1\nu_1) & \sigma_1\tau_2(\theta_1\nu_1) & \sigma_2\tau_1(\theta_1\nu_1) & \sigma_2\tau_2(\theta_1\nu_1) \\ \sigma_1\tau_1(\theta_1\nu_2) & \sigma_1\tau_2(\theta_1\nu_2) & \sigma_2\tau_1(\theta_1\nu_2) & \sigma_2\tau_2(\theta_1\nu_2) \\ \sigma_1\tau_1(\theta_2\nu_1) & \sigma_1\tau_2(\theta_2\nu_1) & \sigma_2\tau_1(\theta_2\nu_1) & \sigma_2\tau_2(\theta_2\nu_1) \\ \sigma_1\tau_1(\theta_2\nu_2) & \sigma_1\tau_2(\theta_2\nu_2) & \sigma_2\tau_1(\theta_2\nu_2) & \sigma_2\tau_2(\theta_2\nu_2) \end{bmatrix}$$

Take

$$B_1 = \begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}, \; B_2 = \begin{bmatrix} 1 & 1 \\ \tau_1(\sqrt{2}) & \tau_2(\sqrt{2}) \end{bmatrix}.$$

Placing ourselves in
$\mathbb{Q}(\sqrt{2},\sqrt{5}) = \{a_0 + a_1\sqrt{5} + a_2\sqrt{2} + a_3\sqrt{5}\sqrt{2},\ a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$,
so that $\sigma(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{5}) = \sqrt{5}$. Then $B_1 \otimes B_2$ is a 4-dimensional lattice.

- So far we discussed the totally real case.
- Next we discuss the CM case. Another equivalent characterization of a CM field is that complex conjugation is an automorphism of K that commutes with all embeddings of K.

Set $\zeta = \zeta_n = \exp(2\pi i/n)$ be a primitive nth root of unity. The number field $\mathbb{Q}(\zeta_n)$ is called a cyclotomic field.

- It has degree $\varphi(n)$, where φ is Euler totient function.

Set $\zeta = \zeta_p = \exp(2\pi i/p)$, p an odd prime. Consider the cyclotomic field $\mathbb{Q}(\zeta_p)$, its ring of integers $\mathbb{Z}[\zeta_p]$ given by

$$\begin{aligned} \mathbb{Q}(\zeta_p) &= \{a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},\ a_i \in \mathbb{Q} \text{ for all } i\} \\ \mathbb{Z}[\zeta_p] &= \{a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},\ a_i \in \mathbb{Z} \text{ for all } i\} \end{aligned}$$

and the embeddings

$$\sigma_r : \zeta \mapsto \zeta^r,\ r = 1, \ldots, p-1.$$

Let $\mathrm{Tr}(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha),\ \alpha \in \mathbb{Q}(\zeta_p)$.
Let $\overline{x}$ denote the complex conjugate of x for $x \in \mathbb{Z}[\zeta_p]$. Then $(x, y) \mapsto \mathrm{Tr}(x\overline{y})$ is a positive definite symmetric bilinear form:

$$\mathrm{Tr}(x\overline{x}) = \sum_{i=1}^{p-1} \sigma_i(x)\overline{\sigma_i(x)} > 0,\ x \neq 0.$$

Set $\mathfrak{P} = (1-\zeta)\mathbb{Z}[\zeta_p] = \{(1-\zeta)(a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-2}),\ a_i \in \mathbb{Z} \text{ for all } i\}$.

Claim. $\mathfrak{P}$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice.

- $\mathrm{Tr}(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}[\zeta]$.
- $\mathrm{Tr}(x\overline{y}) \in p\mathbb{Z}$

For $p = 3$, we have $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$, $\mathfrak{P}$ has $\mathbb{Z}$-basis $(1-\zeta_3), (1-\zeta_3)\zeta_3 = 2\zeta_3 + 1$. Then $\sigma(\mathfrak{P}) = \{u_0(1-\zeta_3) + u_1(1+2\zeta_3),\ u_0, u_1 \in \mathbb{Z}\}$ and e.g.
$(1-\zeta_3)\overline{(1-\zeta_3)} = (1-\zeta_3)(1-\zeta_3^2) = 1-\zeta_3^2-\zeta_3+1 = 2+\zeta_3+1-\zeta_3$
and $\mathrm{Tr}((1-\zeta_3)\overline{(1-\zeta_3)}) = 2 \cdot 3 = 6$.

$$\frac{1}{3}\begin{bmatrix} 6 & -3 \\ -3 & 6 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}.$$

This is A_2, the hexagonal lattice.

The hexagonal lattice A_2: .

$$\frac{1}{3}\begin{bmatrix} 6 & -3 \\ -3 & 6 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}.$$

Also

$$\sigma_1 : \quad a + b\zeta_3 \mapsto a + b\zeta_3$$
$$\sigma_2 : \quad a + b\zeta_3 \mapsto a + b\zeta_3^2.$$

Create the lattice $\sigma((1-\zeta_3)\mathbb{Z}[\zeta_3])$

$$\begin{bmatrix} \sigma_1(1-\zeta_3) & \sigma_2(1-\zeta_3) \\ \sigma_1(1+2\zeta_3) & \sigma_2(1+2\zeta_3) \end{bmatrix} \begin{bmatrix} \overline{\sigma_1(1-\zeta_3)} & \overline{\sigma_1(1+2\zeta_3)} \\ \overline{\sigma_2(1-\zeta_3)} & \overline{\sigma_2(1+2\zeta_3)} \end{bmatrix}$$
$$= \begin{bmatrix} 6 & -3 \\ -3 & 6 \end{bmatrix}$$

(e.g. $2(1-\zeta_3)(1-\zeta_3^2) = 2(1-\zeta_3^2-\zeta_3+1) = 2\cdot 3$).

- A generator matrix of a lattice using a twisting element $\alpha = (1-\zeta_3)^2$ is given by

$$B = \begin{bmatrix} \sigma_1(1-\zeta_3) & \sigma_2(1-\zeta_3) \\ \sigma_1(1-\zeta_3)\sigma_1(\zeta) & \sigma_2(1-\zeta_3)\sigma_2(\zeta) \end{bmatrix}.$$

- The volume of the lattice $\sigma((1-\zeta_3)\mathbb{Z}[\zeta])$ is given by

$$\begin{aligned} v(\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])) &= |\sigma_1(1-\zeta_3)\sigma_2(1-\zeta_3)| \left| \det \begin{bmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\zeta) & \sigma_2(\zeta) \end{bmatrix} \right| \\ &= 3 \cdot \sqrt{3}. \end{aligned}$$

The discriminant of $K = \mathbb{Q}(\zeta_p)$ is defined as $d_K = \det[\sigma_j(\zeta^{i-1})]^2$, $i, j = 1, \ldots, p-1$, which is

$$(-1)^{(p-1)/2} p^{p-2}.$$

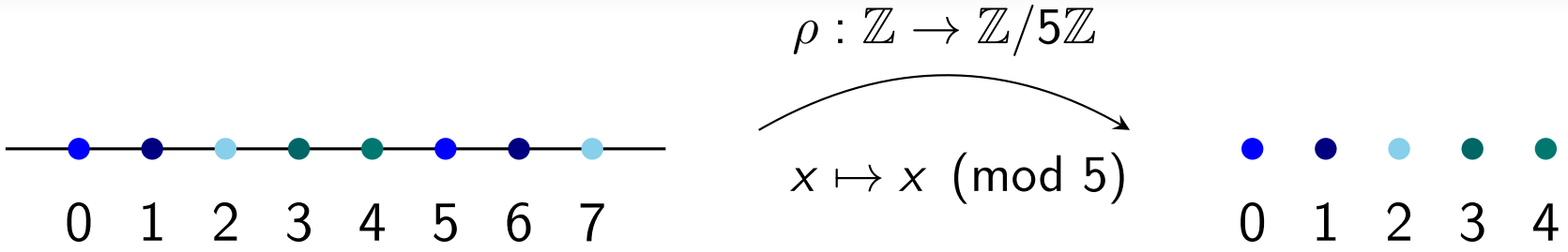
- In our example

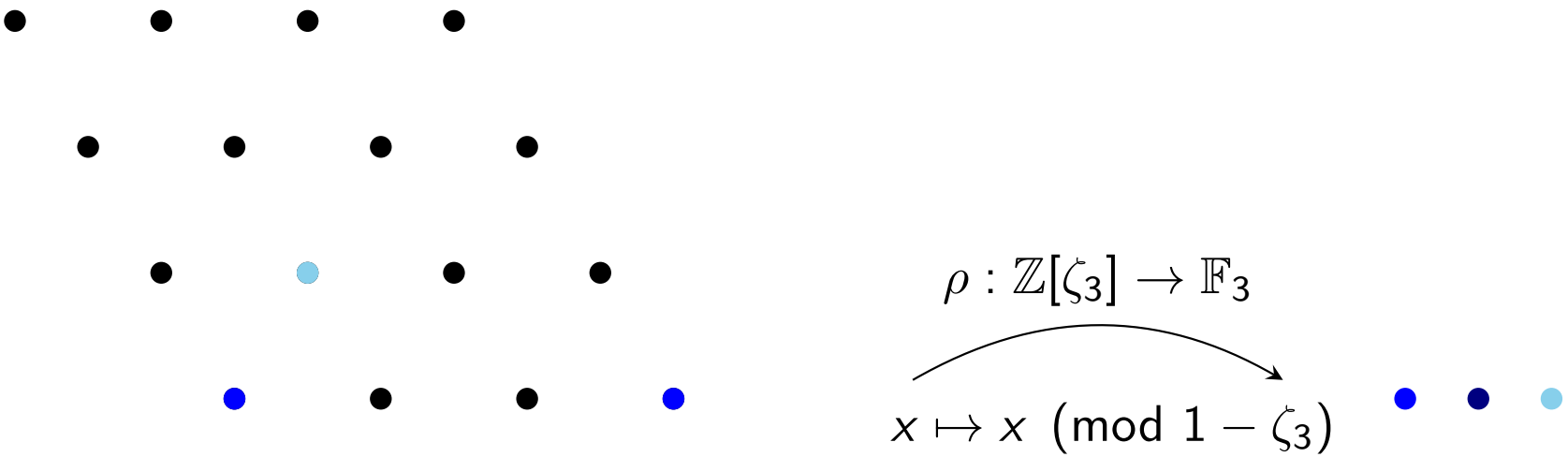
$$\begin{aligned} v(\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])) &= |\sigma_1(1-\zeta_3)\sigma_2(1-\zeta_3)| \left|\det \begin{bmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\zeta) & \sigma_2(\zeta) \end{bmatrix}\right| \\ &= |N(1-\zeta_3)|\sqrt{d_K} \\ &= 3 \cdot \sqrt{3} \\ &= \left(\det \begin{bmatrix} 6 & -3 \\ -3 & 6 \end{bmatrix}\right)^{1/2} \end{aligned}$$

and $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

The construction holds for an arbitrary prime p.

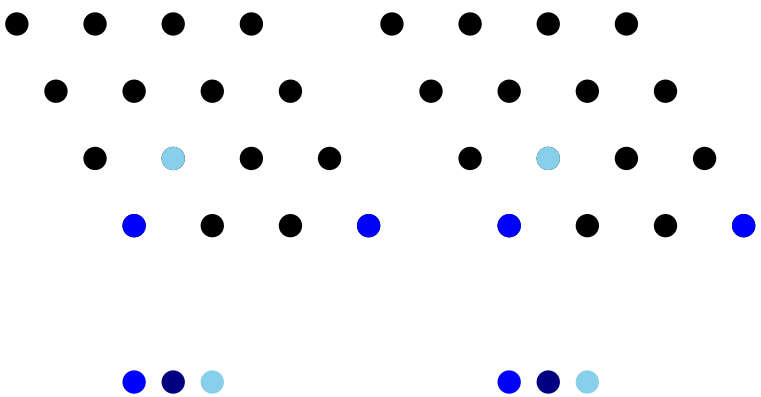
- This provides a parameterized family of lattices.



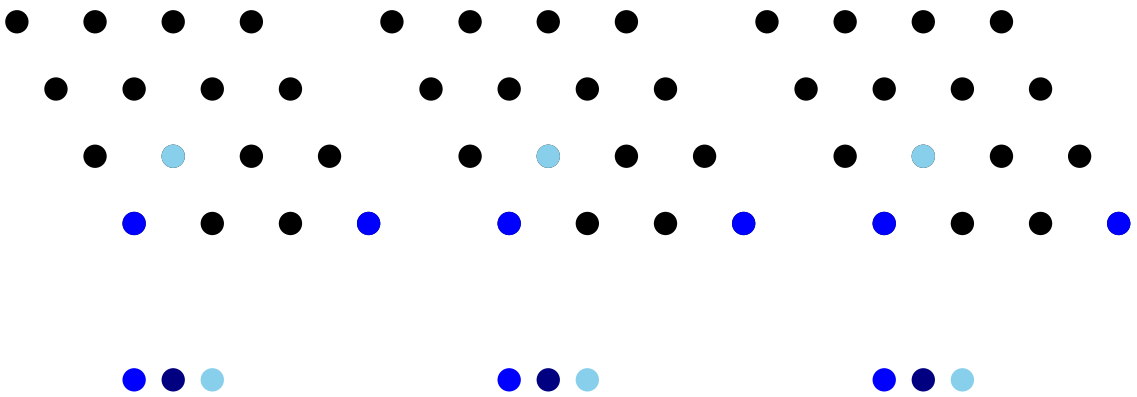


$(a + b\zeta_3 = a + b\frac{-1+i\sqrt{3}}{2} = a - \frac{1}{2}b + i\frac{\sqrt{3}}{2}b \mapsto a + b$ so $0 \mapsto 0$,
$1 + \zeta_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2} \mapsto 2)$

Given a linear code $C \subset \mathbb{F}_p^n$ and ρ the componentwise reduction modulo $1-\zeta$ on $\mathbb{Z}[\zeta]^n$, $\Lambda_C = \rho^{-1}(C) \subset \mathbb{R}^n$ equipped with $(x, y) \mapsto \mathrm{Tr}(x\overline{y}/p)$ is an integral lattice obtained by Construction A.



$$\rho : \mathbb{Z}[\zeta_3] \to \mathbb{F}_3,\ a + b\zeta_3 \mapsto a + b\zeta_3 \pmod{1 - \zeta_3} = a + b.$$



Consider the repetition code of length 3 over $\mathbb{F}_3$:
$C = \{a(1,1,1),\ a \in \mathbb{F}_3\}$. Then $\rho^{-1}(C) = \{x = (a_0 + b_0\zeta_3, a_1 + b_1\zeta_3, a_2 + b_2\zeta_3) \in \mathbb{Z}[\zeta_3]^3,\ \rho(x) \in C\}$.

$$\rho^{-1}(C) = \{x = (a_0 + b_0\zeta_3, a_1 + b_1\zeta_3, a_2 + b_2\zeta_3) \in \mathbb{Z}[\zeta_3]^3,\ \rho(x) \in C\}$$

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \zeta_3 & \zeta_3^2 & \zeta_3 & \zeta_3^2 & \zeta_3 & \zeta_3^2 \\ 0 & 0 & 1-\zeta_3 & 1-\zeta_3^2 & 0 & 0 \\ 0 & 0 & (1-\zeta_3)\zeta_3 & (1-\zeta_3^2)\zeta_3^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1-\zeta_3 & 1-\zeta_3^2 \\ 0 & 0 & 0 & 0 & (1-\zeta_3)\zeta_3 & (1-\zeta_3^2)\zeta_3^2 \end{bmatrix}$$

columns 1,2: $a_0 + b_0\zeta_3 \mapsto a_0 + b_0 \pmod{1-\zeta_3}$
columns 3,4: $a_0 + b_0\zeta_3 + (1-\zeta_3)(a_1 + b_1\zeta_3) \mapsto a_0 + b_0 \pmod{1-\zeta_3}$
columns 5,6: $a_0 + b_0\zeta_3 + (1-\zeta_3)(a_2 + b_2\zeta_3) \mapsto a_0 + b_0 \pmod{1-\zeta_3}$

- $\rho(\mathbf{u}M) = \{a(1,1,1),\ a \in \mathbb{F}_3\}$

Given a linear code $C \subset \mathbb{F}_p^n$ of dimension m and ρ the componentwise reduction modulo $1-\zeta$ on $\mathbb{Z}[\zeta]^n$, $\Lambda_C = \rho^{-1}(C) \subset \mathbb{R}^n$ equipped with $(x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)) \mapsto \sum_{i=1}^n \mathrm{Tr}(x_i \overline{y_i}/p)$ is an integral lattice obtained by Construction A. It has rank $n(p-1)$, volume $\sqrt{p^{n-2m}}$. If C is self-dual, then Λ_C is unimodular.
This construction combines

- the basic Construction A,
- the construction of lattices from number fields.

- A fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is principal if it is of the form $c^{-1}\mathfrak{b}$ where $\mathfrak{b}$ is a principal ideal of $\mathcal{O}_K$.
  - Recall that an $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K is a fractional ideal of $\mathcal{O}_K$ if there exists some non-zero $c \in \mathcal{O}_K$ such that $c\mathfrak{a} \subseteq \mathcal{O}_K$.
  - The non-zero fractional ideals of $\mathcal{O}_K$ form an abelian group under multiplication.
  - The identity is $\mathcal{O}_K$ and we have $\mathfrak{a}^{-1} = \{x \in K,\ x\mathfrak{a} \subseteq \mathcal{O}_K\}$.
- Let $\mathcal{F}$ be the group of fractional ideals under multiplication.
- Let $\mathcal{P}$ be the subgroup of principal fractional ideals.
- The class group of $\mathcal{O}_K$ is the quotient group

$$\mathcal{F}/\mathcal{P}.$$

- Embed again K into $\mathbb{C}$ using each of the embeddings

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}.$$

- Consider again the map $\sigma : K \to \mathbb{R}^s \times \mathbb{C}^t$ given by

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)).$$

- If $\alpha_1, \ldots, \alpha_n$ is a basis for K, then $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are linearly independent over $\mathbb{R}$ (it is worth looking at this claim into more details).

- Write $\sigma_k(\alpha_l) = x_k^{(l)}$, $\sigma_{s+j}(\alpha_l) = y_j^{(l)} + iz_j^{(l)}$.
- We have

$$E = \begin{bmatrix} x_1^{(1)} & \dots & x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & y_1^{(1)} - iz_1^{(1)} & \dots \\ & \vdots & & & & \\ x_1^{(n)} & \dots & x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & y_1^{(n)} - iz_1^{(n)} & \dots \end{bmatrix}$$

  which is the usual embedding of a basis, so its determinant is not 0 ($\det(E)^2$ is the discriminant of this basis).
- Also

$$D = \begin{bmatrix} x_1^{(1)} & \dots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \dots & y_t^{(1)} & z_1^{(1)} \\ & \vdots & & & & & & \\ x_1^{(n)} & \dots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \dots & y_1^{(n)} & z_1^{(n)} \end{bmatrix}$$

  and $\det(E) = (-2i)^t \det(D)$ so $\det(D) \neq 0$ as required.

Lemma. If L is a lattice in $\mathbb{R}^s \times \mathbb{C}^t$ of volume V, and if $c_1, \ldots, c_{s+t}$ are positive reals such that

$$c_1 \cdots c_{s+t} > \left(\frac{4}{\pi}\right)^t V,$$

then there exists $(x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+t}) \neq \mathbf{0}$ in L such

$$|x_1| < c_1, \ldots, |x_s| < c_s, |x_{s+1}| < c_{s+1}, \ldots, |x_{s+t}| < c_{s+t}.$$

Proof.

- Pick a set X which is a cartesian product of line segments and circular discs satisfying the required constraints and compute $v(X)$, using $\int_{-c_j}^{c_j} dx_j$ and $\int_{y_j^2+z_j^2<c_{s+j}} dy_j dz_j$ to find $v(X) = 2^s \pi^t c_1 \cdots c_{s+t}$.
- Since X is bounded, symmetric and convex, apply Minkowski's theorem. $\square$

Theorem. Let K be a number field of degree $n = s + 2t$ and let $0 \neq \mathfrak{b}$ be an ideal of $\mathcal{O}_K$. Then

$$v(\sigma(\mathfrak{b})) = 2^{-t} N(\mathfrak{b}) \sqrt{|d_K|}.$$

Proof. The term 2^{-t} comes from separating the real and imaginary parts. Then since $\mathfrak{b}$ has a $\mathbb{Z}$-basis, it may be expressed in terms of an integral basis, which gives both $N(\mathfrak{b})$ and $\sqrt{|d_K|}$. $\square$

Theorem. If $\mathfrak{b} \neq 0$ is an ideal of $\mathcal{O}_K$, then contains an integer α with

$$|N(\alpha)| \leq (2/\pi)^t N(\mathfrak{b}) \sqrt{|d_K|}.$$

Proof.

- For $\epsilon > 0$, choose positive reals $c_1, \ldots, c_{s+t}$ such that

$$c_1 \cdots c_{s+t} = (2/\pi)^t N(\mathfrak{b}) \sqrt{|d_K|} + \epsilon.$$

- Thus there exists $0 \neq \alpha \in \mathfrak{b}$ such that

$$|\sigma_1(\alpha)| < c_1, \ldots, |\sigma_s(\alpha)| < c_s, |\sigma_{s+1}(\alpha)|^2 < c_{s+1}, \ldots, |\sigma_{s+1}(\alpha)|^2 < c_{s+t}.$$

- Since a lattice is discrete, the set A_ϵ of α such that $|N(\alpha)| < (2/\pi)^t N(\mathfrak{b}) \sqrt{|d_K|} + \epsilon$ is finite and we pick an $\alpha \in A = \cap A_\epsilon$. This α satisfies the claim. $\square$

Recall that the class group of $\mathcal{O}_K$ is the quotient group

$$\mathcal{F}/\mathcal{P}.$$

- Two fractional ideals are equivalent if they belong to the same coset of $\mathcal{P}$ in $\mathcal{F}$.
- Then $[\mathfrak{a}]$ denotes the equivalence class of $\mathfrak{a}$, that is it contains all fractional ideals that are equivalent to $\mathfrak{a}$.
- If $\mathfrak{a}$ is a fractional ideal, then $\mathfrak{a} = c^{-1}\mathfrak{b}$, $c \in \mathcal{O}_K$ and $\mathfrak{b}$ an ideal, so

  $$\mathfrak{b} = c\mathfrak{a} = \langle c \rangle \mathfrak{a}$$

  for $\langle c \rangle \in \mathcal{P}$. So $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent.
- Also every equivalence class contains an ideal ($\mathfrak{b} \in [\mathfrak{a}]$).

Corollary. Every non-zero ideal $\mathfrak{b}$ of $\mathcal{O}_K$ is equivalent to an ideal $\mathfrak{c}'$ such that $N(\mathfrak{c}') \leq (2/\pi)^t \sqrt{|\Delta|}$.

Proof.

- The class $[\mathfrak{b}^{-1}]$ of fractional ideals equivalent to $\mathfrak{b}^{-1}$ contains an ideal $\mathfrak{c}$.
- We find an integer $\gamma \in \mathfrak{c}$ such that

$$|N(\gamma)| \leq (2/\pi)^t N(\mathfrak{c}) \sqrt{|d_K|}.$$

- Since $\mathfrak{c} | \langle \gamma \rangle$, we have $\langle \gamma \rangle = \mathfrak{c}\mathfrak{c}'$ for some ideal $\mathfrak{c}'$.
- Since $N(\mathfrak{c}')N(\mathfrak{c}) = |N(\gamma)|$, we have

$$N(\mathfrak{c}') \leq (2/\pi)^t \sqrt{|d_K|}.$$

- Since $\mathfrak{c}$ is equivalent to $\mathfrak{b}^{-1}$ and $\mathfrak{c}'$ is equivalent to $\mathfrak{c}^{-1}$ (recall $\langle \gamma \rangle = \mathfrak{c}\mathfrak{c}'$), we have that $\mathfrak{c}'$ is equivalent to $\mathfrak{b}$. $\square$

If $K = \mathbb{Q}(\sqrt{-5})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $d_K = -20$. So

$$(2/\pi)^t \sqrt{|d_K|} = \frac{2\sqrt{20}}{\pi} < 2.85.$$

Thus every ideal of $\mathcal{O}_K$ is equivalent to either an ideal of norm 1 (thus $\mathcal{O}_K$) or to an ideal of norm 2, which must divide $\langle 2 \rangle = \langle 2, 1 + \sqrt{-5} \rangle^2$. In fact $\langle 2, 1 + \sqrt{-5} \rangle$ is the only ideal of norm 2, so every ideal is either equivalent to $\mathcal{O}_K$ or to $\langle 2, 1 + \sqrt{-5} \rangle$.

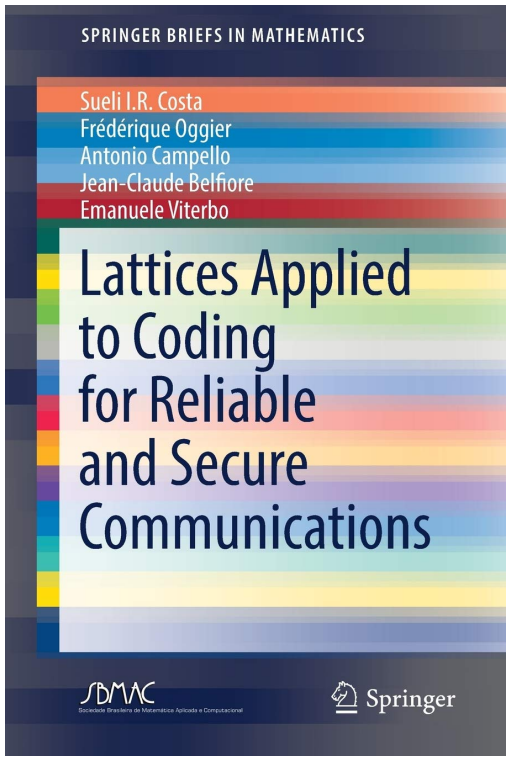
Theorem. The class number h_K is finite for K a number field of discriminant d_K and degree $n = s + 2t$.

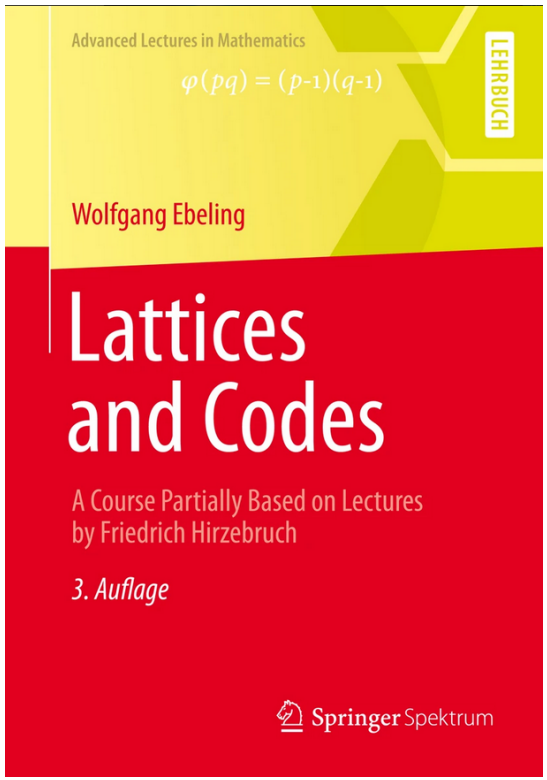
Proof.

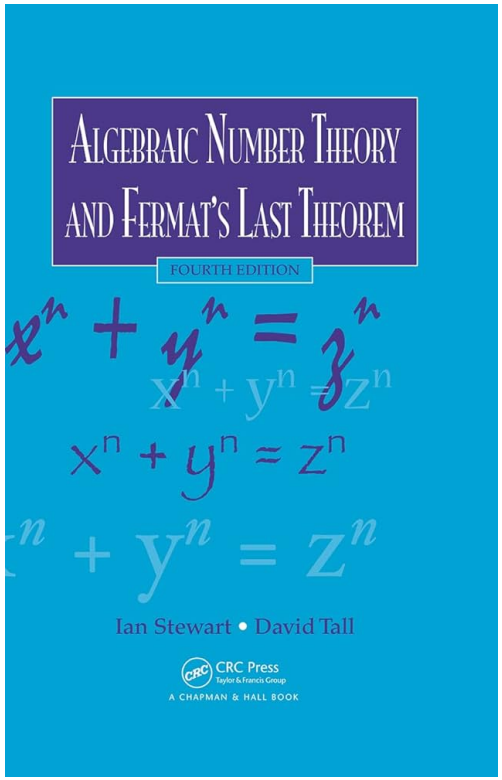
- That $h_K = |\mathcal{F}/\mathcal{P}|$ is finite is equivalent to say that the number of distinct equivalence classes of fractional ideals is finite.
- Let $[\mathfrak{c}]$ be such an equivalence class. Then $[\mathfrak{c}]$ contains an ideal $\mathfrak{a}$ which is equivalent to an ideal $\mathfrak{b}$ with $N(\mathfrak{b}) \leq (2/\pi)^t \sqrt{|d_K|}$.
- Since only finitely many ideals have a given norm (use ideal factorization and compute the norms appearing in this factorization), there are only finitely many possible choices for $\mathfrak{b}$.
- Since $[\mathfrak{c}] = [\mathfrak{a}] = [\mathfrak{b}]$, there are only finitely many equivalence classes $[\mathfrak{c}]$. $\square$

Lattices from number fields are of interest:

- to mathematicians working on quadratic forms and algebraic number theory,
- to cryptographers ('ideal' lattices),
- to coding theorists (fading channels).


SPRINGER BRIEFS IN MATHEMATICS
Sueli I.R. Costa
Frédérique Oggier
Antonio Campello
Jean-Claude Belfiore
Emanuele Viterbo
Lattices Applied to Coding for Reliable and Secure Communications
SBMAC
Springer


Advanced Lectures in Mathematics
$\varphi(pq) = (p-1)(q-1)$
LEHRBUCH
Wolfgang Ebeling
Lattices and Codes
A Course Partially Based on Lectures by Friedrich Hirzebruch
3. Auflage
Springer Spektrum


Algebraic Number Theory and Fermat's Last Theorem
FOURTH EDITION
$x^n + y^n = z^n$
Ian Stewart • David Tall
CRC Press
A CHAPMAN & HALL BOOK