Lattices and Rings

Student: Teh Yu Xuan
Supervisor: Assoc Prof Frederique Elise Oggier
Division of Mathematical Sciences, School of Physical and Mathematical Sciences

Abstract

In abstract algebra, a lattice is a well studied algebraic structure and it has various applications across different discipline of studies. In particular, lattices are actively studied in cryptography due to the computational hardness of some lattice problems. In material science or computational physics, a lattice model is a crystalline structure coinciding in special cases with the atom or molecule positions in a crystal. In this project, we studied lattices as an algebraic structure and how it is connected to algebraic number theory.

Lattice and dual of a lattice

An n-dimensional lattice $\mathcal{L}$ is any subset of $\mathbb{R}^n$ that is both:

- an additive subgroup: $\mathbf{0} \in \mathcal{L}$ and $-\mathbf{x}, \mathbf{x}+\mathbf{y} \in \mathcal{L}, \forall\ \mathbf{x}, \mathbf{y} \in \mathcal{L}$; and
- discrete: every $\mathbf{x} \in \mathcal{L}$ has a neighbourhood in $\mathbb{R}^n$ in which $\mathbf{x}$ is the only lattice point.

The dual of a lattice $\mathcal{L}$, which is denoted by $\mathcal{L}^*$ is the set of vectors in $\mathbb{R}^n$, such that

$$\mathcal{L}^* = \{\mathbf{w} \in \mathbb{R}^n : \langle \mathbf{w}, \mathcal{L} \rangle \subseteq \mathbb{Z}\}$$

Let $\mathbf{B} \in M_n(\mathbb{R})$, where $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n$ are the column vectors of $\mathbf{B}$ representing the n linearly independent basis vectors of $\mathcal{L}$. We say $\mathbf{B}$ is a basis of $\mathcal{L}$. If $\dim \mathbf{B} = n$, $\mathcal{L}$ is a full rank lattice. In fact, the theorem below shows the relation between the basis of a lattice and the basis of its dual lattice.

Theorem 1. *Let $\mathcal{L}$ be a full rank lattice. If $\mathbf{B}$ is a basis of $\mathcal{L}$, then $(\mathbf{B}^{-1})^T$ is a basis of its dual lattice, $\mathcal{L}^*$. [5]*

With this theorem, we derive the following corollaries.

Corollary 1. *Let $\mathcal{L}$ be a lattice, then $(\mathcal{L}^*)^* = \mathcal{L}$.*

Corollary 2. *Given two lattices $\mathcal{L}$ and $\mathcal{M}$, $\mathcal{L} \subseteq \mathcal{M} \iff \mathcal{M}^* \subseteq \mathcal{L}^*$.*

Corollary 3. *Let q be a scalar, then $(q\mathcal{L})^* = \frac{1}{q}\mathcal{L}^*$.*

q-ary finite dimensional lattices

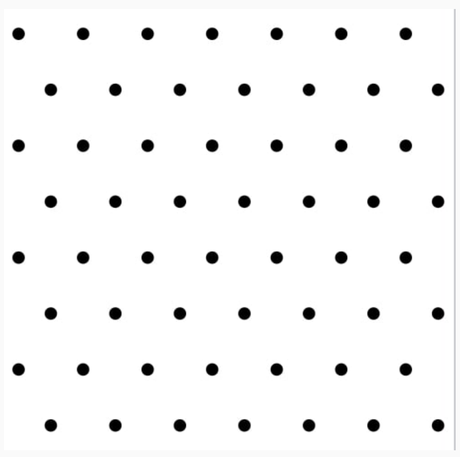
q-ary finite dimensional lattices are being widely studied and applied in cryptography. Here, we will study two common q-ary lattices. A lattice $\mathcal{L} \subset \mathbb{Z}^m$ is a q-ary m-dimensional lattice if $q\mathbb{Z}^m \subseteq \mathcal{L} \subseteq \mathbb{Z}^m$. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we consider the following two lattices [1]

$$\mathcal{L}_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}^T\mathbf{s} \bmod q\ ,\ \mathbf{s} \in \mathbb{Z}^n\},$$
$$\mathcal{L}_q^{\perp}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{A}\mathbf{y} = \mathbf{0} \bmod q\}.$$

It is straightforward to verify that both are indeed q-ary m-dimensional lattices. We have the following theorem which shows the dual relationship between the two lattices above.

Theorem 2. $\mathcal{L}_q^{\perp}(\mathbf{A}) = q\left(\mathcal{L}_q(\mathbf{A})\right)^*$

Diagrams



(a) Lattice points in $\mathbb{R}^2$

(b) Lattice points in $\mathbb{R}^3$

Embeddings of a number field

There is a notion of embedding of an algebraic extension of $\mathbb{Q}$ into $\mathbb{C}$ [4]. Let K be a number field of degree n. An embedding is a map that maps K to $\mathbb{C}$. By the Primitive Element Theorem, $K/\mathbb{Q}$ is a simple extension and let $K = \mathbb{Q}(\alpha)$. There exists $f(X) \in \mathbb{Q}[X]$ with degree n, such that $f(X)$ is the minimal polynomial of α. Every element of K can be written as

$$c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}, \text{ for } c_i \in \mathbb{Q}.$$

$f(X)$ is irreducible over $\mathbb{Q}$. By the Fundamental Theorem of Algebra, $f(X)$ has n distinct roots in $\mathbb{C}$.
Let $\rho_1, \rho_2, ..., \rho_n$ be the n distinct roots of $f(X)$. We have

$$f(X) = \prod_{i=1}^{n}(X - \rho_i), \text{ for } \rho_i \in \mathbb{C}.$$

We have n embeddings in total. For $j = 1, 2, \ldots, n$, we define σ_j to be an embedding that maps K to $\mathbb{C}$ by the following way:

$$\sigma_j(c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}) = c_0 + c_1\rho_j + ... + c_{n-1}\rho_j^{n-1}.$$

Suppose there are $2s$ complex roots and r real roots, i.e. $n = r+2s$, we relabel the n embeddings as $\sigma_1, \sigma_2, ..., \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, ..., \sigma_{r+s}, \overline{\sigma_{r+s}}$.

Embeddings of an ideal in $\mathcal{O}_K$

In this section, $\mathcal{O}_K$ is the ring of integers of a number field K. Let K be a number field of degree n, $\mathcal{O}_K$ has a $\mathbb{Z}$-basis, say $\{x_1, x_2, \ldots, x_n\}$. Also, let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the n distinct embeddings that maps K to $\mathbb{C}$. We have the discriminant [2]

$$\triangle_K = D(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2$$

By Dedekind's theorem of linear independence of characters, we can show that $\triangle_K \neq 0$.

Proposition 1. *[3] Let K be a number field of degree n. Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$, then $\sigma_i(\mathfrak{a})$ for $i = 1, 2, \ldots, n$ is a full lattice, where σ_i's are the embeddings that map K to $\mathbb{C}$.*

The steps leading to prove this proposition are as follows:

- Prove that $\mathfrak{a}$ has a $\mathbb{Z}$-basis of n elements, say $\{x_1, x_2, \ldots, x_n\}$.
- Let $\mathbf{A} \in M_n(\mathbb{R})$ with its ith row being the n embeddings of x_i, namely $\sigma_1, \sigma_2, ..., \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, ..., \sigma_{r+s}, \overline{\sigma_{r+s}}$, where $n = r + 2s$.
- We know $\det \mathbf{A} \neq 0$, by performing elementary column operations, we can successively prove the proposition.

References

[1] *Dual lattice*, Dec 2020. https://en.wikipedia.org/wiki/Dual_lattice.

[2] *Discriminant of an algebraic number field*, Jan 2021. https://en.wikipedia.org/wiki/Discriminant_of_an_algebraic_number_field.

[3] J. S. Milne, *Algebraic number theory (v3.08)*, 2020. Available at www.jmilne.org/math/.

[4] J. Neukirch, *Algebraic number theory*, vol. 322, Springer Science & Business Media, 2013.

[5] C. Peikert, *A decade of lattice cryptography*, Foundations and Trends® in Theoretical Computer Science, 10 (2016), pp. 283–424.

Acknowledgements

This project was conducted as part of the Odyssey Research Programme at the School of Physical and Mathematical Sciences, Nanyang Technological University.