Ideal Lattices in Cryptography

Håvard Damm-Johnsen

August 17, 2020

Abstract

Lattices have a long history of use in number theory, and have in recent times found applications in cryptography. Out of the 26 second-round candidates for the NIST post-quantum cryptography competition, 9 base their security on conjecturally computationally hard problems about lattices. For optimisation, several proposed lattices are *ideal lattices*, which have rich number-theoretic structure. In this report, we investigate whether the *Arakelov class group*, which parameterises certain ideal lattices up to isometry, can provide avenues of attack on the aforementioned hard problems. This idea was first introduced in [4].

Contents

1 Lattices

1.1 Introduction to lattices

A *lattice* L of rank n is a discrete subgroup of $\mathbb{R}^n$ isomorphic to $\mathbb{Z}^n$. The requirement that a discrete subgroup L be isomorphic to $\mathbb{Z}^n$ is equivalent to the quotient group $\mathbb{R}^n/L$ being compact; in that case we say that L is *cocompact.* Lattices arise naturally in several classical problems in number theory, for example in the study of quadratic forms, cf. [2, Section 1.4].

For any basis $\mathcal{B} = \{b_1, \dots, b_n\}$ of $\mathbb{R}^n$, the $\mathbb{Z}$-span of $\mathcal{B}$ defines a lattice. Conversely, for any lattice we can find a collection of n linearly independent elements in L, hence a basis for $\mathbb{R}^n$. This shows that there is a correspondence between lattices of dimension n and the collection of invertible $n \times n$-matrices over $\mathbb{R}$, $\mathrm{Gl}_n(\mathbb{R})$. Explicitly, we send a basis $b_1, \dots, b_n$ to the matrix $[b_1, \dots, b_n]^t$, which we recall is invertible by basic linear algebra.

However, not all bases determine different lattices; for example, if $n = 1$, any lattice takes the form $b\mathbb{Z} = \{bn \colon n \in \mathbb{Z}\}$ for some non-zero real number b, and we see that the lattices determined by $b = 1$ and $b = -1$ give the same subgroup of $\mathbb{R}$. This phenomenon extends to higher dimensions, as the following lemma shows.

Lemma 1.1. *Let L and L' be lattices determined by bases $b_1, \dots, b_n$ and $b'_1, \dots, b'_n$, respectively. Then L and L' define the same set if and only if there exists a matrix A with integer coefficients satisfying $|\det A| = 1$ and $A[b_1, \dots, b_n]^t = [b'_1, \dots, b'_n]^t$.*

This is not particularly difficult to prove, see [10, Thm. 7.14]. In other words, the map $\mathrm{Gl}_n(\mathbb{R}) \to \{\text{Lattices in } \mathbb{R}^n\}$ is surjective but not injective. If $n = 1$, then there are only two different bases for a lattice, since the only real 1×1 matrices of determinant 1 are $[\pm 1]$. However, in higher dimensions there are infinitely many: if a, b are coprime integers, then by the Euclidean algorithm we can find integers c, d such that $ac - bd = 1$, so the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

takes one basis to a different one. By an induction argument, it is possible to construct similar examples in higher dimensions.

For any lattice, we define the *volume* (or sometimes *covolume*) of the lattice to be the number $\mathrm{vol}(L) = |\det B|$ where $B = [b_1, \dots, b_n]^t$. By the lemma above, the choice of basis is irrelevant.

The *fundamental domain* of a lattice L is the quotient $\mathbb{R}^n/L$. Given a basis $b_1 \dots, b_n$, we can identify the fundamental domain of L with the set

$$\mathcal{F}(L) = \left\{ \sum_{i=1}^{n} a_i b_i \colon a_i \in [0, 1) \right\}.$$

We can also consider it as an n-fold torus via the isomorphism $L \cong \mathbb{Z}^n$, by

$$\mathbb{R}^n/L \cong \mathbb{R}^n/\mathbb{Z}^n \cong (\mathbb{R}/\mathbb{Z})^n =: \mathbb{T}^n.$$

This point of view will be more prevalent in the later sections.

1.2 Short vectors in lattices

Among the main reasons for the ubiquity of lattices are the following few problems. Fix a norm $\|-\|$ on $\mathbb{R}^n$, and let $L \subset \mathbb{R}^n$ be a lattice of rank n.

- The shortest vector problem (SVP): Find a shortest vector $v \in L$, that is, a non-zero vector which satisfies $\|v\| = \min_{w \in L} \|w\|$.
- The approximate shortest vector problem (apprSVP): Given a function $\phi(n)$, the "approximation factor", find a non-zero vector $w \in L$ satisfying
$$\|w\| \leq \phi(n)\|v\|,$$
where v is the shortest vector in L.
- The closest vector problem (CVP): Given a fixed vector $x \in \mathbb{R}^n$, find the vector $w \in L$ that minimises $\|w - x\|$.

A special case of apprSVP is γ-hermiteSVP, for a positive number γ, which asks to solve apprSVP with $\phi(n) = \gamma \cdot \mathrm{vol}(L)^{1/n}$.

These are all considered to be computationally hard to crack, with both classical and quantum algorithms. While one might think that apprSVP should be significantly easier than the other two, even the best algorithms are often impractical for sufficiently large n. While CVP is considered slightly harder than SVP, one can often reduce CVP to SVP in a slightly higher dimension, cf. [10, Rmk. 7.23]. It is often easy to solve these problems given an almost orthogonal basis for the lattice using Babai's algorithm, cf [10, Section 7.6]. However, with a sufficiently high dimension and a highly non-orthogonal basis, the solving the problems exactly is unfeasible even with a lot computing power.

The choice of a norm is also important: the Euclidean norm is perhaps the most common, but some algorithms take the supremum norm $\|v\|_\infty = \sup_{1 \leq i \leq n} |v_i|$ as a starting point. The hardness of the problems above is conjectured to be influenced by the choice of norm, and some work has been put reducing from one to another, cf. [9, Chap. 13, p.449ff].

To study such vector problems in lattices, it is useful to introduce some notation: the lenght of the shortest vector in a lattice L is usually denoted by $\lambda_1(L)$, and for $k > 1$ we define the *k-th successive minima* of L as

$$\lambda_k(L) := \min_{L_k \subset L} \max_{v \in L_k} \|v\|,$$

where L_k runs over all subsets of L consisting of k linearly independent vectors. If we take $k = 1$, we see that this reduces to the original definition of λ_1. For example, consider the lattice generated by the vectors $(1, 0)$ and $(0, 2)$. For this we have $\lambda_1(L) = \|(1, 0)\| = 1$ but $\lambda_2(L) = \max\{\|(1, 0)\|, \|(0, 2)\|\} = 2$. In general, it is easy to check that

$$\lambda_1(L) \leq \lambda_2(L) \leq \ldots \leq \lambda_n(L),$$

and these numbers are all equal if and only if L is a dilation and/or rotation of $\mathbb{Z}^n$. Minkowski proved (a generalisation of) the following theorem about the successive minima of a lattice:

Theorem 1.2 (Minkowski's second theorem)**.** *Let L be a lattice in $\mathbb{R}^n$. Then*

$$\frac{\mathrm{vol}(L)}{n!} \leq \prod \lambda_i \leq \mathrm{vol}(L).$$

1.3 Cyclic and ideal lattices

Given a polynomial $f(x) \in \mathbb{Z}[x]$ of degree n, we can consider the polynomial quotient ring

$$R = \frac{\mathbb{Z}[x]}{(f(x))}.$$

This becomes a lattice via the *coordinate embedding*: fix a basis $x_0, \dots, x_{n-1}$ for $\mathbb{R}^n$, and consider the linear map ϕ defined by $\phi \colon x^i \mapsto x_i$. Since we can pick any coefficients from $\mathbb{Z}$ to define a polynomial in R, the image of ϕ is the $\mathbb{Z}$-span of a basis of $\mathbb{R}^n$, hence a lattice. If I is an ideal of R, then the image $L = \phi(I) \subset \mathbb{R}^n$ is called an *ideal lattice*. As the name suggests, this is also a lattice, and has rank n.

The main and perhaps historically most significant examples are the *cyclic lattices*, which arise from taking $f(x) = x^n - 1$, for some positive integer n. This is the basis for the NTRU cryptosystem [10, Section 7.10]. However, f is not irreducible, so we are prone to divide by $x - 1$ to obtain the irreducible polynomial $f(x) = x^{n-1} + x^{n-2} + \ldots + 1$, and use this instead. Geometrically, this can be viewed as a hyperplane in $\mathbb{Z}[x]/(x^n - 1)$. The ring $\mathbb{Z}[x]/(f(x))$ is then a so-called cyclotomic ring, and has several useful properties enabling fast computation.

1.4 Two lattice-based cryptosystems

We now sketch a simple lattice-based public key cipher, called the *GGH cryptosystem*. The exposition follows [10, Section 7.8]. Suppose Bob wants to send a message to a trusted partner Alice securely. Alice fixes her secret key, a reasonably orthogonal collection of vectors $v_1, \dots, v_n \in \mathbb{Z}^n$ which define a lattice $L \subset \mathbb{R}^n$. For convenience, set $V = [v_1, \dots, v_n]^t$. Next Alice chooses an $n \times n$ matrix W with integer coefficients and $\det W = \pm 1$, so that the new basis $\{w_i = v_i U \colon i = 1, \dots, n\}$ is "bad", that is, far from being orthogonal. This new basis $w_1, \dots, w_n$ is Alice's public key.

If Bob wants to transmit a message $m \in \mathbb{Z}^n$ securely, he fixes additionally a small "error term" e. Next he computes the cipher text $c = mW + e$. This is generally not a lattice point, but by choosing e sufficiently small, it will be close to a unique lattice point. Alice can then use her "good" basis for L to solve the closest vector problem, and obtain mW. By multiplying by W^{-1}, Alice then obtains Bob's secret message m.

In practice, most lattice cryptosystems are a lot more involved than this, and considering its simplicity it should come as no surprise that it is insecure, see [6].

Another lattice-based cryptosystem, briefly mentioned earlier, is the NTRU family of algorithms. The NTRU asymmetric public key system described in [10, Section 7.10] goes as follows:

Define

$$R := \frac{\mathbb{Z}[x]}{x^N - 1},$$

where $N > 3$ is a large prime. Fix two other distinct primes p and q, along with an integer $d \approx N/3$, and set

$$R_p := \frac{\mathbb{Z}/p\mathbb{Z}[x]}{x^N - 1} \quad \text{and} \quad R_q := \frac{\mathbb{Z}/q\mathbb{Z}[x]}{x^N - 1}.$$

We define $\mathcal{T}(a, b)$ to be the collection of *ternary polynomials*, that is, polynomials with a coefficients equal to 1, b coeffients equal -1 and the rest 0. The public data for the NTRU Encrypt algorithm is the following: N, p, q and $d \in \mathbb{Z}$, chosen such that $q > (6d + 1)p$.

Alice chooses secret polynomials $f \in \mathcal{T}(d + 1, d)$ and $g \in \mathcal{T}(d, d)$ such that $f \pmod p$ and $f \pmod q$ are invertible in R_p and R_q, respectively, and we call the inverses F_p and F_q. Alice's public key is $h(x) := F_q(x)g(x) \pmod q$.

If Bob wants to send a plaintext $m \in R_p$, he picks a random "noise element" $r \in \mathcal{T}(d, d)$, and computes the ciphertext $e = prh + m \pmod q$, which is passed on to Alice.

Alice then computes $f \cdot e = pgr + fm \pmod q$, and lifts this to an element $a(x) \in R$: the lift used is the one centered at 0, meaning that a has integral coefficients in the interval $(-q/2, q/2)$. The condition on p, q and d ensures that the message is preserved; Alice then reduces modulo p to obtain $a(x) \pmod p = f(x)m(x) \pmod p$, and by multiplying by F_p she recovers Bob's plaintext $m(x)$.

On the surface, this does not look much like a lattice algorithm; however, one can show, cf. [10, Prop. 7.61] that breaking the algorithm is at least as difficult as solving `apprSVP` in a lattice determined by q and the coefficients of the polynomial h, explicitly by

$$M_h^{\text{NTRU}} := \begin{pmatrix} \mathbb{I} & \mathbf{h} \\ 0 & q\mathbb{I} \end{pmatrix}$$

where $\mathbb{I}$ is the $n \times n$-identity matrix where $n = \deg h$, and $\mathbf{h}$ is the matrix defined as follows: if h has coefficients h_i for $i = 0, \ldots, n-1$, then the entry $\mathbf{h}_{ij} = h_{i-j}$ with the subtraction computed modulo n. The key result is then that f and g are short vectors of M_h^{NTRU}.

1.5 Instantiations

An *instantiation* is a choice of parameters for a specific instance of a cryptosystem. For example, a choice of N, p, q and d in NTRU Encrypt in the previous section constitues an instantiation. There are many concerns to be taken when choosing an instantiation; we generally want the parameters to be chosen such that computation is fast, in which case smaller numbers are preferred, but on the other hand this can prove a risk to security. The same goes for choices of lattices; we want lattices with a lot of structure (such as the cyclotomic ring generated by $x^N - 1$), but not so much that the structure can be used to solve the underlying lattice problems more easily than other lattices. This is part of the reason why the NIST post-quantum candidate NTRU Prime, also based on the NTRU setup, uses the ring $x^N - x - 1$ instead of $x^N - 1$; the cyclotomic rings simply have a too large attack surface.

2 Number-theoretic background

2.1 Number fields

Let k be a field containing the rational numbers $\mathbb{Q}$. Then k is naturally a $\mathbb{Q}$-vector space where the scalars act via the multiplication in k. Its dimension is usually called the *index*, denoted by $[k : \mathbb{Q}]$. In algebraic number theory, the main object of study is the *number field*, which is a field of finite index. Suppose α is a root of a (monic, irreducible) polynomial $f \in \mathbb{Z}[x]$ of degree n. Then the ring

$$\mathbb{Q}(\alpha) := \{b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} \colon b_i \in \mathbb{Q}\}$$

is in fact a field, which one shows by establishing an isomorphism $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f(x))$, which is a field by the extended Euclidean algorithm. Clearly it contains a copy of $\mathbb{Q}$, and it has finite index because it is spanned by $1, \alpha, \ldots, \alpha^{n-1}$. It turns out that every number field is of this form, for some suitable α. This result is called *Artin's primitive element theorem.*

In $\mathbb{Q}$ it is easy to show that the only rational numbers that arise from polynomials with integer coefficients are the integers themselves. However, recall that *the golden ratio* is defined as the root of the polynomial $x^2 - x - 1$, and equals $\frac{1}{2} + \frac{1}{2}\sqrt{5}$. This shows that the *integral closure* of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{5})$, that is, the collection of elements of $\mathbb{Q}(\sqrt{5})$ arising as roots of polynomials with coefficients in $\mathbb{Z}$, can be strictly larger than $\mathbb{Z}[\alpha]$. If k is a number field, we call the integral closure of $\mathbb{Z}$ in k the *ring of algebraic integers* of k, usually denoted by $\mathcal{O}_k$. If $\mathcal{O}_k = \mathbb{Z}[\alpha]$, then we say that f is *monogenic.*

Suppose k is a number field with $k \cong \mathbb{Q}[x]/(f(x))$ for some irreducible monic polynomial $f \in \mathbb{Z}[x]$. Without choosing a distinguished element α defining $\mathbb{Q}(\alpha)$, we have $\deg f = [k : \mathbb{Q}]$ distinct roots of f to choose from. Each root α gives an embedding σ of k into $\mathbb{C}$, defined by

$$\begin{aligned} \sigma \colon k \cong \frac{\mathbb{Q}[x]}{(f(x))} &\to \mathbb{C}, \\ P(x) + f(x) &\mapsto P(\alpha) + f(\alpha) = P(\alpha). \end{aligned}$$

We define the *norm* of an element $a \in k$ as $N_{k/\mathbb{Q}}(a) := \prod_\sigma \sigma(a)$, and the *trace* as $\mathrm{tr}_{k/\mathbb{Q}} := \sum_\sigma \sigma(a)$. If there is no room for confusion, we tend to drop the subscripts and write simply $N(a)$ and $\mathrm{tr}(a)$. Their names are related to the fact that they are the determinant and trace, respectively, of multiplication by α regarded as a linear map on the $\mathbb{Q}$-vector space k. Both the norm and the trace are integers whenever α is an algebraic integer; this is easily seen by Vieta's formulae.

2.2 Unique factorisation of prime ideals

The ring $\mathcal{O}_k$ carries many similarities to $\mathbb{Z}$, but also some crucial differences. Most importantly, it fails to have unique factorisation into prime numbers. For example, in $\mathbb{Q}(\sqrt{-5})$, we can factor 6 as both $2 \cdot 3$ and $(1+\sqrt{-5}) \cdot (1-\sqrt{-5})$. This famously lead to an erroneous proof of Fermat's last theorem [5, Lamé, p310 ff.]. In lieu of this, it was observed by Kummer that if we had so-called "ideal numbers" p_i such that

$$\begin{aligned} 2 &= p_1 p_2, & 1+\sqrt{-5} &= p_1 p_3, \\ 3 &= p_3 p_4, & 1-\sqrt{-5} &= p_2 p_4, \end{aligned}$$

then unique factorisation would be preserved. Dedekind translated this into the language of abstract algebra, giving *ideals*, which are subgroups under multiplication by elements of the original ring. The main result is the following:

Theorem 2.1. *Let $\mathcal{O}_k$ be the ring of integers in a number field k. Then any ideal $\mathfrak{a} \subset \mathcal{O}_k$ factors as a finite product of prime ideals*

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdot \ldots \mathfrak{p}_r^{n_r},$$

where $n_i \in \mathbb{N}$ for $i = 1, \ldots r$.

Here the product of two ideals $\mathfrak{a} \cdot \mathfrak{b}$ is by definition the ideal consisting of finite sums of elements $a \cdot b$ for $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. We also define a *fractional ideal* I as an additive subgroup of k for which there exists some $x \in \mathcal{O}_k$ such that $x \cdot I \subset \mathcal{O}_k$. For example, in $\mathbb{Q}$ the subgroup $\frac{1}{2}\mathbb{Z}$ is a fractional ideal, and indeed here every fractional ideal is of the form $\frac{a}{b}\mathbb{Z}$ for some coprime $a, b \in \mathbb{Z}$. It is important to note that **a fractional ideal is not an ideal**: it is not even a subset of $\mathcal{O}_k$.[1] Fields, on the other hand, have only the trivial ideal. In very formal terms, fractional ideals are precisely the projective rank 1 $\mathcal{O}_k$-modules, cf. [8, Exercise I.3.10]. Then Theorem 2.1 generalises to negative exponents in a natural way, see

Under the multiplication defined above, the set of fractional ideals $\mathcal{I}_k$ forms an abelian group, with $\mathcal{O}_k$ as the identity element. For example, the inverse of $\frac{1}{2}\mathbb{Z}$ in $\mathbb{Q}$ is $2\mathbb{Z}$. We call a *principal fractional ideal* any fractional ideal which can be written as $x \cdot \mathcal{O}_k$ for some $x \in k$. The principal fractional ideals form a subgroup Prin_k of $\mathcal{I}_k$. In $\mathbb{Q}$, and more generally in any number field whose ring of integers is a principal ideal domain, one shows that every fractional ideal is principal. As is usual in modern mathematics, we are then inspired to form an object which measures the failure of being a principal ideal domain. Namely, define

$$\mathrm{Cl}_k := \frac{\mathcal{I}_k}{\mathrm{Prin}_k}.$$

[1] Unlike much of the literature, in the following we make a conscious effort to separate between the two.

This is called the *ideal class group* of the number field k, and an important result in algebraic number theory is that Cl_k is always a finite group, cf. [8, Theorem I 6.3]. We call its size $\#\,\mathrm{Cl}_k$ the *class number of* k. Evidently, k has class number 1 if and only if $\mathcal{O}_k$ is a principal ideal domain.

2.3 The Minkowski embedding

Recall that we have $n = \dim_{\mathbb{Q}} k$ embeddings of k into $\mathbb{C}$, as described in the end of section Section 2.1. Minkowski's brilliant idea was that instead of choosing one, we can combine all of them to obtain an embedding which carries more arithmetic information. For example, returning to our quadratic extension $\mathbb{Q}(\sqrt{5})$, the roots of the minimal polynomial $x^2 - 5$ are $\pm\sqrt{5}$, and so we have two distinct embeddings $\sigma\colon \sqrt{5} \mapsto \sqrt{5}$ and $\tau\colon \sqrt{5} \mapsto -\sqrt{5}$. These are in a sense indistinguishable, since $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(-\sqrt{5})$ define the same field.

Let $\{\sigma_i\colon i = 1, \dots, n\}$ be the collection of embeddings $k \hookrightarrow \mathbb{C}$. We can assemble these into a map $k \hookrightarrow k_{\mathbb{C}} := \prod_i \mathbb{C}$ by $a \mapsto (\sigma_1(a), \dots, \sigma_n(a))$. By convention, we tend to drop the subscripts and write the tuple as $(\sigma(a))_\sigma$. If σ is an embedding, then it is easy to see that $\bar{\sigma}$ which sends a to $\overline{\sigma(a)}$, is also such an embedding, although σ and $\bar{\sigma}$ need not be different. Therefore we have a natural conjugation action on $k_{\mathbb{C}}$, not simply by conjugating each element, but by conjugating each element *and* switching the σ-coordinate with the $\bar{\sigma}$-coordinate. By definition, this action leaves fixed the elements of $k_{\mathbb{C}}$ that come from k. Therefore we can identify the elements of $k_{\mathbb{C}}$ related by the conjugation action to yield a new vector space $k_{\mathbb{R}}$ formally defined as

$$k_{\mathbb{R}} := \{(x_\sigma)_\sigma \in k_{\mathbb{C}}\colon \bar{x}_\sigma = x_{\bar{\sigma}}\}.$$

Since the conjugation action does nothing to the image of k, there is a natural embedding of k into $k_{\mathbb{R}}$. This is called the *Minkowski embedding*, or sometimes the *canonical embedding*.

If we again consider $k = \mathbb{Q}(\sqrt{5})$, then we see that $k_{\mathbb{C}}$ consists of pairs (x_σ, x_τ) where $x_\sigma, x_\tau \in \mathbb{C}$. Since the images of both σ and τ lie in $\mathbb{R}$, the conjugation action does nothing to these. Therefore

$$k_{\mathbb{R}} = \{(x_\sigma, x_\tau) \in k_{\mathbb{C}}\colon \bar{x}_\sigma = x_\sigma,\ \bar{x}_\tau = \bar{x}_\tau\} \cong \mathbb{R}^2,$$

as a complex number equals its conjugate if and only if it lies along the real line. The embedding of $\mathbb{Q}(\sqrt{5})$ into $k_{\mathbb{R}}$ then looks like

$$(a + b\sqrt{5}) \mapsto (a + b\sqrt{5}, a - b\sqrt{5}),$$

in other words the copy of $\mathbb{Q}$ lies along the diagonal $x_\sigma = x_\tau$, while $\sqrt{5} \cdot \mathbb{Q}$ lies on the anti-diagonal, $x_\sigma = -x_\tau$. The situation is described in Fig. 1.

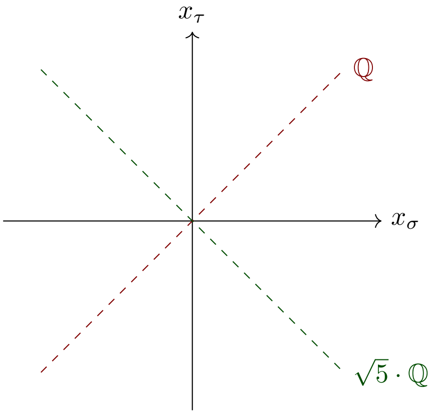

Figure 1: The image of $\mathbb{Q}(\sqrt{5})$ under the Minkowski embedding.

We can transfer the multiplicative structure on k to $k_\mathbb{R}$, simply by requiring that $(x_\sigma)_\sigma \cdot (y_\sigma)_\sigma = (x_\sigma y_\sigma)_\sigma$. In technical language, this makes $k_\mathbb{R}$ into an $\mathbb{R}$-*algebra*, and we have an isomorphism $k_\mathbb{R} \to \mathbb{R}^n$ given by

$$\begin{aligned} x_\tau &\mapsto x_\tau \\ x_\sigma &\mapsto \mathrm{Re}(x_\sigma) \\ x_{\bar\sigma} &\mapsto \mathrm{Im}(x_\sigma), \end{aligned}$$

where τ runs over the real embeddings $k \hookrightarrow \mathbb{R} \subset \mathbb{C}$, and σ the complex embeddings modulo conjugation.

This allows us to define a natural Hermitian inner product inherited from $k_\mathbb{C}$, namely by

$$\langle x_\sigma, y_\sigma \rangle = \sum_\sigma x_\sigma \bar{y}_\sigma.$$

This is frequently also called the *trace product on* $k_\mathbb{R}$, since for elements $x, y \in k$,

$$\langle (\sigma(x))_\sigma, (\sigma(y))_\sigma \rangle = \mathrm{tr}(x\bar{y}),$$

where tr is the usual trace from algebraic number theory, and $\bar{y}$ the complex conjugate of y, inherited from $\mathbb{C}$ in the canonical inclusion $k \subset \mathbb{C}$. Tron: I'm still somewhat confused about the trace; isn't the trace defined this way? (Neukirch's book, page 29-30), i.e., $\mathrm{tr}(x) = \sum \sigma(x)$, so $\mathrm{tr}(x\bar{y}) = \sum \sigma(x)\overline{\sigma(y)}$ by definition? Håvard: Yes, that is correct, but there is more in $k_\mathbb{R}$ than just the image of k. So in formal terms the trace factors as

$$\begin{tikzcd} k \arrow[r, "\text{Minkw}"] \arrow[dr, "\mathrm{tr}(x\bar{y})"'] & k_\mathbb{R} \arrow[d, "\langle x,y\rangle"] \\ & \mathbb{R} \end{tikzcd}$$

Håvard: However, it is not obvious that the trace extends to a map on all of $k_\mathbb{R}$.

The image of a given fractional ideal $\mathfrak{a} \subset k$ under the Minkowski embedding is a lattice. If $\mathfrak{a} \subset \mathcal{O}_k$ is *integral*, that is, wholly contained in $\mathcal{O}_k$, then its volume (that is, the Lebesgue measure of the quotient $k_{\mathbb{R}}/\mathfrak{a}$) is given by

$$\operatorname{vol}(\mathfrak{a}) = \sqrt{|\Delta_k|}[\mathcal{O}_k : \mathfrak{a}], \tag{1}$$

where $\Delta_k = \det\bigl(\operatorname{tr}\bigl(b_i \bar{b}_j\bigr)\bigr)$ for any basis $\{b_i\}$ of $\mathcal{O}_k$ is the *discriminant of* k, and $[\mathcal{O}_k : \mathfrak{a}]$ is the (additive) group-theoretic index of $\mathfrak{a}$ in $\mathcal{O}_k$. From this we can determine the volume of a fractional ideal $\mathfrak{a}^{-1}$ by computing the index (as abelian groups) of the sublattice $\mathfrak{a}$. The (absolute) *norm* of a fractional ideal $\mathfrak{a}$ is defined for integral ideals as $[\mathcal{O}_k : \mathfrak{a}]$, and extended multiplicatively. Explicitly, if a fractional ideal $\mathfrak{a}$ decomposes as $\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$, then $N(\mathfrak{a}) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{n_{\mathfrak{p}}}$. In light of Lagrange's theorem we therefore have for arbitrary fractional ideals that

$$\operatorname{vol}(\mathfrak{a}) = \sqrt{|\Delta_k|}N(\mathfrak{a}) \tag{2}$$

which in the special case of integral ideals reduces to Eq. (1).

The main result of Minkowski theory is the following bound:

Theorem 2.2 (The Minkowski bound)**.** *Let $\mathfrak{a} \subset \mathcal{O}_k$ be an integral ideal, let r and $2s$ be the number of real and complex embeddings of k, respectively, and let $n = [k : \mathbb{Q}]$. Then $\mathfrak{a}$ contains a non-zero element a such that*

$$|N_{k/\mathbb{Q}}(a)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta_k|}.$$

This is used to prove the finiteness of Cl_k, and by taking $n \geq 2$ it is not difficult to show that $|\Delta_k| = 1$ if and only if $k = \mathbb{Q}$.

Consider for instance the integral ideal $\mathfrak{a} = (1 + \sqrt{5})$ in $\mathbb{Q}(\sqrt{5})$. Explicitly, this is the collection of points in $\mathcal{O}_k$ of the form

$$\frac{a + b\sqrt{5}}{2}(1 + \sqrt{5}) = \frac{a + 5b + (a + b)\sqrt{5}}{2},$$

and these are mapped to the points

$$\left(\frac{a + 5b + (a + b)\sqrt{5}}{2}, \frac{a + 5b - (a + b)\sqrt{5}}{2}\right) \in k_{\mathbb{R}}.$$

From the example computation of the Minkowski embedding above, we deduce that the image $\mathfrak{a}$ is given by

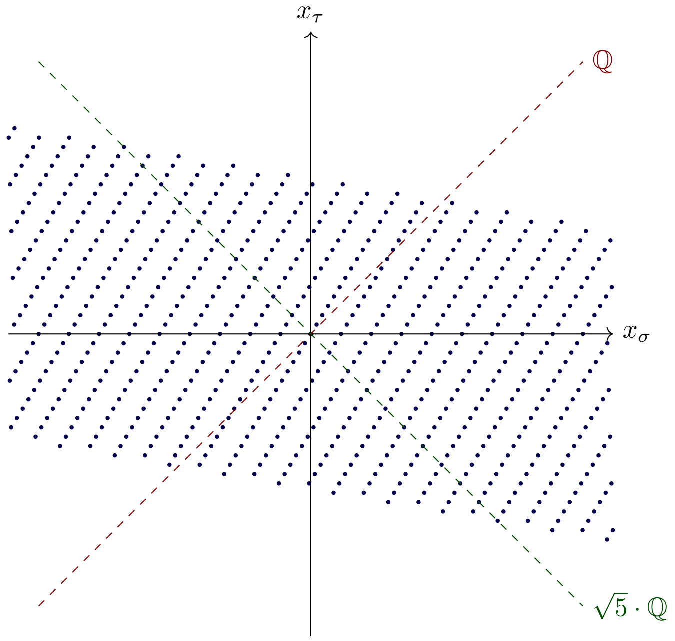

Figure 2: The ideal lattice $(1 + \sqrt{5})$ in $\mathbb{Q}(\sqrt{5})$ under the Minkowski embedding.

2.4 The logarithmic embedding

The idea of modfying the Minkowski embedding to study the units of a number field is commonly attributed to Dirichlet. Instead of embedding k into some real vector space, we will instead take $k^\times = k \setminus \{0\}$ as our starting point. Since every element then has non-zero norm, we can define a mapping by $\alpha \mapsto (\log|\sigma(\alpha)|)_\sigma$, which transforms the multiplication in k to addition inside $\prod_\sigma \mathbb{R}\sigma$. Even though this is a real vector space, we have a canonical involution as in the additive case, given by $(x_\sigma)_\sigma \mapsto (x_{\bar{\sigma}})_\sigma$.

What do we get by modding out by this action? Well, enumerate the embeddings σ into $\sigma_1, \ldots, \sigma_r$, the real embeddings, and let $\sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s}$ be the remaining complex embeddings. By definition of our labelling, we have $n = r + 2s$ where r is the number of real embeddings, and $2s$ is the number of complex embeddings. The involution leaves fixed the components corresponding to real embeddings, and identifies the coordinate associated to a complex embedding σ with the coordinate of its conjugate $\bar{\sigma}$. Letting $[\prod_\sigma \mathbb{R}]^+$ denote the quotient space following the convention in [8], we therefore find that $\dim\,[\prod_\sigma \mathbb{R}]^+ = r + s$. Note that $\log|\bar{\sigma}(x)| = \log|\overline{\sigma(x)}| = \log|\sigma(x)|$, so the image of k is preserved under the action, and as a consequence we have an embedding of k into $[\prod_\sigma \mathbb{R}]^+$. This is called the *logarithmic embedding* of k, and we denote the map by $\ell\colon k^\times \to [\prod_\sigma \mathbb{R}]^+$.

It is easy to see that if $x \in k^\times$ is a unit of $\mathcal{O}_k$, then it has norm ± 1. On the other hand, by defining the *trace* of an element $(x_\sigma)_\sigma$ in $[\prod_\sigma \mathbb{R}]^+$ as the sum of the components, $\sum_\sigma x_\sigma$, then for a given element $x \in k^\times$ we find that

$$\operatorname{tr} \ell(x) = \sum_\sigma \log |\sigma(x)| = \log \prod_\sigma |\sigma(x)| = \log |N(x)|.$$

In particular, if $x \in \mathcal{O}_k$ is a unit, then its image in the logarithmic embedding lies in the hyperplane H consisting of elements of trace zero, as $\log 1 = 0$. Since the units of $\mathcal{O}_k$ form a multiplicative subgroup of $k^\times$, the image of this subgroup is an additive subgroup of H, seeing as the logarithm turns multiplication into addition. However, it is not just any subgroup: it is a lattice, as the following theorem tells us.

Theorem 2.3 (Dirichlet's unit theorem)**.** *Let k be a number field with ring of integers $\mathcal{O}_k$. Then the group of units in $\mathcal{O}_k$ is finitely generated, and forms a lattice of rank $r + s - 1$ in the logarithmic embedding. In general, the group of units has the form $\mathbb{Z}^{r+s-1} \times \mu_k$, where μ_k is the subgroup consisting of roots of unity in k.*

3 Arakelov theory of number fields

In this section, we aim to explain the setup for the paper [4]. Since the theory in question was heavily based on an analogy between number fields and function fields of algebraic curves, we will first recall the notion of divisors in the algebro-geometric setting. This is included primarily for motivation, and readers unfamiliar with algebraic curves can safely go directly to Section 3.2.

3.1 The function field case

Let C be a curve over $\mathbb{C}$, formally a non-singular projective algebraic variety with function field of transcendence degree 1 over $\mathbb{C}$. We can then form the *divisor group of C*, $\operatorname{Div}(C)$ formally the free abelian group generated by the points on C. A *divisor* is an element $D \in \operatorname{Div}(C)$, and can be written as

$$D = \sum_P n_P \cdot P, \qquad n_P \in \mathbb{Z},$$

with all but finitely many $n_P = 0$. While this is an uncountably infinite group, every element looks like a finite formal sum of points on C, counted with finite multiplicity. An *effective divisor* is one for which $n_P \geq 0$ for all P, and if D is such a divisor we write $D \geq 0$. The *degree map* is the function $\operatorname{Div}(C) \to \mathbb{Z}$ defined by

$$\deg\left(\sum_P n_P \cdot P\right) = \sum_P n_P.$$

As complex curves are also Riemann surfaces, we can consider a rational function $f\colon C \to \mathbb{C}$, to which we associate a *principal divisor*

$$(f) \mapsto \sum_{n_P} n_P(f) \cdot P,$$

where $n_P(f) = 0$ unless f has a pole or a zero at P. If f has a pole at P, then $n_P(f) = -\operatorname{ord}_P(f)$, and if P is a zero, then $n_P(f)$ is its order, both in the usual complex-analytic sense. (cf. [7]). Using the Cauchy integral formula one shows that f necessarily has the same number of poles as zeros. In other words, all principal divisors have degree 0. We say that two divisors D and D' are *equivalent* if $D = D + (f)$ for some rational function f. Clearly, then, equivalent divisors necessarily have the same degree.

Given a meromorphic form

$$fdz$$

on C, we can similarly form a *canonical divisor* $\kappa = (f)$ by counting the poles and zeros of f. One can show that any two canonical divisors are equivalent. For a fixed divisor D, we define the vector space $\mathscr{L}(D)$ to be the set of rational functions with $(f) + D \geq 0$. This can be shown to be finite-dimensional, and denote its dimension by $\ell(D)$. We are now able to state one of the main theorems in the theory of divisors:

Theorem 3.1 (Riemann-Roch for curves)**.** *Let D be a divisor on a non-singular projective algebraic curve C of genus g, and κ a canonical divisor on C. Then*

$$\ell(D) - \ell(\kappa - D) = \deg D + 1 - g.$$

To tie this to number fields, recall that if C is defined as the vanishing locus of $F(t) \in \mathbb{C}[t]$, then every prime ideal of the *coordinate ring*

$$R = \frac{\mathbb{C}[t]}{(F(t))}$$

corresponds to a point on C.[2] Then a function on C can be regarded as a function on $\operatorname{Spec} R$, the collection of prime ideals of R. Now, if we pass to a number field k, the "coordinate ring" will be the ring of integers in k. An element of k can then be regarded as a "function on $\operatorname{Spec} \mathcal{O}_k$" in the same manner as a rational expression in the function field of a curve is a function on the prime ideals on the coordinate ring of the same curve.

This is not sufficient, however; we would like to make $\mathcal{O}_k$ "compact" in some sense. To do this, we add in the "primes at infinity", just like $\mathbb{C}$ is compactified by adding the point at infinity. These are the embeddings of k into $\mathbb{C}$, and arise naturally in the theory of valuations. For an in-depth explanation of this, see [8, Chapters II & III].

3.2 Divisors on number fields

Let $\mathcal{I}_k$ be the ideal group of a number field k with ring of integers $\mathcal{O}_k$, and let $\{\sigma\}$ be the collection of embeddings $k \hookrightarrow \mathbb{C}$. We then form the *Arakelov divisor group*, Div_k, as a slight modification of the free abelian group on the prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$ and embeddings ν, defined up to conjugation:

$$\operatorname{Div}_k = \left(\bigoplus_{\mathfrak{p}} \mathbb{Z}\mathfrak{p} \right) \oplus \left(\bigoplus_{\nu} \mathbb{R}\nu \right).$$

[2] There are also the *generic points*, which we tacitly ignore.

It is not quite free abelian because the infinite places have coefficients in $\mathbb{R}$, not $\mathbb{Z}$. For brevity we frequently omit "Arakelov" and simply write "divisors".

The reason for identifying conjugates is that conjugate embeddings σ and $\bar{\sigma}$ induce the same valuation on k, see [8, Chap. II]. In other words, an Arakelov divisor is a formal $\mathbb{Z}$-linear combination of the primes of $\mathcal{O}_k$, "the finite part", along with an $\mathbb{R}$-linear combination of the embeddings modulo conjugation, "the infinite part". For easier bookkeeping, we will denote embeddings up to conjugation by ν, while σ is used when σ and $\bar{\sigma}$ need to be distinguished.

For example, for the quadratic extension $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$, we have a priori two complex embeddings (sending i to a choice of $\pm i$), but in the divisor sum we identify these, so that a divisor D takes the form

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + x_\nu \nu.$$

Then $7 \cdot (1+i) + \pi\nu$ is a divisor since $(1+i)$ is a prime in $\mathbb{Q}(i)$, but $\sum_{p \equiv 3 \pmod 4} p \cdot (p)$, where the sum is taken of primes of $\mathbb{Z}$ which do not split in $\mathbb{Q}(i)$, is not, since there are infinitely many non-zero coefficients.

Since the finite part $\sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$ is determined uniquely by the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ and vice versa, it is natural to define a map $\mathrm{Div}_k \to \mathcal{I}_k$ by "forgetting the infinite part",

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\nu} x_\nu \nu \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}.$$

Since the kernel of this map is precisely $\prod_\nu \mathbb{R}$, we have an exact sequence[3]

$$0 \to \prod_{\nu} \mathbb{R} \to \mathrm{Div}_k \to \mathcal{I}_k \to 0. \tag{3}$$

With the notation from Section 2.4, we recognise $\prod_\nu \mathbb{R}$ as being exactly the space $[\prod_\sigma \mathbb{R}]^+$.

Next, as in the function field case, we define the *degree map* $\deg\colon \mathrm{Div}_k \to \mathbb{R}$ by the rules

$$\deg \mathfrak{p} = \log N(\mathfrak{p}) \quad \text{and} \quad \deg \nu = \begin{cases} 1 \text{ if } \nu \text{ is real,} \\ 2 \text{ if } \nu \text{ is complex.} \end{cases}$$

Note that $N(\mathfrak{p})$ is always finite: by Lagrange's theorem, it equals $\#(\mathcal{O}_k/\mathfrak{p})$. This is a finite number since $\mathcal{O}_k/\mathfrak{p}$ is a quotient of a free $\mathbb{Z}$-module by a free submodule of the same rank, which follows from an easy induction on the rank. The fact that $\mathfrak{p}$ is a free $\mathbb{Z}$-module is deduced from the fact that any submodule of a free $\mathbb{Z}$-module is also free, proved using a similar induction argument.

It is easily checked that deg is a surjective group homomorphism onto the additive group $\mathbb{R}$. We next consider the kernel of deg, which we denote by Div_k^0, which by definition is the subgroup of divisors with degree 0. This fits into a natural exact sequence derived from Eq. (3), namely

$$0 \to H \to \mathrm{Div}_k^0 \to \mathcal{I}_k \to 0.$$

[3] Recall that a sequence is exact if at any object in the sequence, the image of the map *in* equals the kernel of the map *out*.

Here H is the trace 0 hyperplane of $[\prod_\sigma \mathbb{R}]^+$ defined in Section 2.4.

For an arbitrary non-zero element $f \in k$, we have a unique prime ideal factorisation $f\mathcal{O}_k = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(f)}$ and form the corresponding *principal divisor*

$$(f) = \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(f) \cdot \mathfrak{p} + \sum_\nu - \log(|\nu(f)|) \cdot \nu.$$

Formally, the correspondence $f \mapsto (f)$ defines a group homomorphism $\mathrm{div} : k^\times \to \mathrm{Div}_k$. As a corollary of [8, Prop. III 1.3], we then have following:

Theorem 3.2. *For any $f \in k^\times$, we have $\deg(f) = 0$. In other words,*

$$\deg \circ \, \mathrm{div} = 0.$$

Since div is a group homomorphism, its image is a subgroup of Div_k. By analogy with the ideal class group, we quotient Div_k by the subgroup of principal divisors, and denote the resulting group by Pic_k, the *Picard group* of k.[4]

By the theorem above, the degree map factors through the quotient, and so we can consider the "degree zero part" of Pic_k, that is, the subgroup of divisor classes $[D]$ for which we have $\deg[D] = 0$. This is what is called the *Arakelov class group* in [4], denoted by Pic_k^0.[5]

Throughout our discussion, we have encountered several exact sequences which we can assemble into a diagram with exact rows and columns,

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{O}_k^\times/\mu_k \arrow[r, hook] \arrow[d, "\ell"] & k^\times/\mu_k \arrow[r] \arrow[d, "\mathrm{div}"] & \mathrm{Prin}_k \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & {[\prod_\sigma \mathbb{R}]^+} \arrow[r] & \mathrm{Div}_k \arrow[r] \arrow[d] & \mathcal{I}_k \arrow[r] \arrow[d] & 0 \\
 & & \mathrm{Pic}_k \arrow[d] & \mathrm{Cl}_k \arrow[d] & \\
 & & 0 & 0 &
\end{tikzcd}$$

Now, remembering the dictum from high school maths to always complete the square, we observe that the missing corner of our diagram can be filled either with $[\prod_\sigma \mathbb{R}]^+/\ell(\mathcal{O}_k^\times)$ or the kernel of some map $\mathrm{Pic}_k \to \mathrm{Cl}_k$. It turns out that this map is in fact well-defined, since the notions of principal fractional ideals and principal divisors are naturally compatible. More interestingly, with some homological algebra magic (also known as the snake lemma), the square

[4] This is technically the first Chow group, as explained in [8, Chap. III], which is however isomorphic to the Picard group, according to Prop. III.1.13.

[5] In [8], Pic_k is the Arakelov class group, not Pic_k^0.

completes to

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{O}_k^\times/\mu_k \arrow[r, hook] \arrow[d, "\ell"] & k^\times/\mu_k \arrow[r] \arrow[d, "\mathrm{div}"] & \mathrm{Prin}_k \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & {[\prod_\sigma \mathbb{R}]^+} \arrow[r] \arrow[d] & \mathrm{Div}_k \arrow[r] \arrow[d] & \mathcal{I}_k \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & T \arrow[r] \arrow[d] & \mathrm{Pic}_k \arrow[r] \arrow[d] & \mathrm{Cl}_k \arrow[r] \arrow[d] & 0 \\
& 0 & 0 & 0 &
\end{tikzcd}$$

However, as stated earlier (without much justification), we are more interested in Pic_k^0, it does in fact fit into an analogous diagram with exact rows and columns:

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{O}_k^\times/\mu_k \arrow[r, hook] \arrow[d, "\ell"] & k^\times/\mu_k \arrow[r] \arrow[d, "\mathrm{div}"] & \mathrm{Prin}_k \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H \arrow[r] \arrow[d] & \mathrm{Div}_k^0 \arrow[r] \arrow[d] & \mathcal{I}_k \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & T^0 \arrow[r] \arrow[d] & \mathrm{Pic}_k^0 \arrow[r] \arrow[d] & \mathrm{Cl}_k \arrow[r] \arrow[d] & 0 \\
& 0 & 0 & 0 &
\end{tikzcd}$$

where H is the trace 0 hyperplane as above. It is a non-trivial fact that Pic_k^0 is a compact topological group. To see this, observe that $T^0 = H/\ell(\mathcal{O}_k^\times)$ is isomorphic to a torus by Dirichlet's unit theorem, and Cl_k is a finite group by Minkowski theory, which can be made into a topological group by equipping it with the discrete topology. As a topological space, we then have that Pic_k^0 is the product of T^0 and Cl_k, and is therefore compact. This identification does not respect the group law, so Pic_k^0 is not isomorphic to an $\#\,\mathrm{Cl}_k$-fold torus as topological groups, but the argument above still proves that it is a compact topological group. It turns out that the compactness of Pic_k^0 conversely implies the Dirichlet unit theorem and the finiteness of the ideal class group, cf. [8, III 1.11].

3.3 Ideal lattices of number fields

Recall from Section 2.3 that the image of any fractional ideal forms a lattice in the Minkowski embedding. In this section we want to extend this definition to associate lattices to Arakelov divisors as well.[6] This prompts the following definition:

An *ideal lattice* is a fractional $\mathcal{O}_k$-ideal $\mathfrak{a}$ equipped with a non-degenerate bilinear form $\langle -, - \rangle$ which is "Hermitian" in the sense that

$$\langle \lambda a, b \rangle = \langle a, \bar{\lambda} b \rangle$$

for all $a, b \in \mathfrak{a}$ and $\lambda \in \mathcal{O}_k$, where $\bar{\lambda}$ is the complex conjugate of λ, inherited from the complex embedding $k \subset \mathbb{C}$.

While we already defined an ideal lattice as something else in Section 1.3, the definition in the current section predates the previous one. Since making up a new name for these will only be a source of confusion, we henceforth adopt the convention that an unspecified ideal lattice is one arising from a fractional ideal, and an ideal lattice in the quotient ring sense is specified as such.

Recall that any Hermitian form on $\mathfrak{a}$ induces a norm by $\|a\|_{\mathfrak{a}}^2 = \langle a, a \rangle$. One shows, cf. [1, Prop. 1], that there exists some invertible element $u \in k \otimes_{\mathbb{Q}} \mathbb{R}$ with $u = \bar{u}$ such that $\langle a, b \rangle = \mathrm{tr}\big(ua\bar{b}\big)$, where we identify $\mathfrak{a}$ with $\mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{R} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$. Thus specifying the bilinear form is equivalent to specfying a unit u, and an ideal lattice can be determined by a pair $(\mathfrak{a}, u)$. This is also called a *Hermitian line bundle*.

To connect this with our previous setup, observe that $k_{\mathbb{R}}$ is naturally an $\mathbb{R}$-algebra under pointwise multiplication. There is an isomorphism of $\mathbb{R}$-algebras, $k \otimes_{\mathbb{Q}} \mathbb{R} \cong k_{\mathbb{R}}$ via the map $\eta \colon a \otimes x \mapsto (\sigma(a))_\sigma \cdot x$ cf. [8, Rmk. on p. 30]. We can therefore define a map $\phi \colon k \otimes_{\mathbb{Q}} \mathbb{R} \to k_{\mathbb{R}}$ by $a \otimes x \mapsto \eta(u \cdot a \otimes x)$, where u is the unit in the trace above, and ϕ maps the fractional ideal $\mathfrak{a}$ to $u\mathfrak{a} \subset k_{\mathbb{R}}$. Then the Hermitian form on $\mathfrak{a}$ is compatible with the inner product on $k_{\mathbb{R}}$, as for any $f \in \mathfrak{a}$ we have that

$$\|f\|_{\mathfrak{a}}^2 = \mathrm{tr}\big(uf\bar{f}\big) = \mathrm{tr}\big(\phi(f\bar{f})\big) = \|\phi(f)\|_{k_{\mathbb{R}}}$$

so this way of embedding the ideal is quite natural. In this way, we arrive at the definition of an ideal lattice given in [4]: namely a lattice in $k_{\mathbb{R}}$ which takes the form $x\mathcal{L}(\mathfrak{a})$, where $x \in k_{\mathbb{R}}$ is invertible, $\mathfrak{a} \subset k$ is a fractional ideal, and $\mathcal{L}$ denotes the Minkowski embedding as usual. Note that u has changed name to x.

There is a natural group structure on the set of fractional ideal lattices, which we denote by IdLat_k, given by $x\mathcal{L}(\mathfrak{a}) \cdot y\mathcal{L}(\mathfrak{b}) = xy\mathcal{L}(\mathfrak{ab})$. The identity element is $\mathcal{L}(\mathcal{O}_k)$, and inverses are defined in the natural way. We can compute the volume of a ideal lattice by using Eq. (2) from Section 2.3:

$$\mathrm{vol}\, x\mathcal{L}(\mathfrak{a}) = \sqrt{|\Delta_k|} \cdot N(\mathfrak{a}) \cdot \prod_{\sigma} |x_\sigma|.$$

Now, let us relate this to Arakelov theory: let

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\nu} n_\nu \nu,$$

[6] This definition of an ideal lattice, as far as I can tell, precedes the context of the Arakelov class group, and is taken from [1].

be an Arakelov divisor. Note well that the number of infinite places is $r + s$ (the number of real + the number of complex pairs) while the space containing ideal lattices is $k_{\mathbb{R}}$ with dimension $n = r + 2s$. Thus we need to make use of the canonical map $[\prod_\sigma \mathbb{R}]^+ \to k_{\mathbb{R}}$, essentially sending the coordinates corresponding to real embeddings to themselves, while for $\nu \neq \bar{\nu}$ the coordinate x_ν is mapped to both the x_ν-coordinate and the $x_{\bar{\nu}}$-coordinate. Following [4], we will denote this assignment by $(x_\nu)_\nu \mapsto (x_{\nu_\sigma})_\sigma$. A quick example to fix ideas: in $\mathbb{Q}(i)$, we have the complex embeddings determined by $\sigma\colon i \mapsto i$ and $\bar{\sigma}\colon i \mapsto -i$, and the map sends $x_\nu \mapsto (x_{\nu_\sigma}, x_{\nu_{\bar{\sigma}}}) = (x_\nu, x_\nu) \in k_{\mathbb{R}}$. In very concrete terms, $\ell(1+i) = \log|1+i| = \log 2$ is mapped to $(\log 2, \log 2) \in k_{\mathbb{R}}$.

With this in mind, we can form a ideal lattice associated to D by setting

$$\mathcal{L}(D) := (e^{n_{\nu_\sigma}})_\sigma \mathcal{L}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}\right).$$

The exponential ensures that $(\exp n_{\nu_\sigma})_\sigma$ is always invertible. We then easily compute that

$$\begin{aligned} \operatorname{vol} \mathcal{L}(D) &= \sqrt{|\Delta_k|} \cdot N\left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}\right) \cdot \prod_\sigma e^{n_{\nu_\sigma}} \\ &= \sqrt{|\Delta_k|} \cdot \exp\left(\sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \log N(\mathfrak{p}) + \sum_\sigma n_{\nu_\sigma}\right) \\ &= \sqrt{|\Delta_k|} \cdot \exp\left(\sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \deg \mathfrak{p} + \sum_\nu n_\nu \cdot \deg \nu\right) \\ &= \sqrt{|\Delta_k|} \cdot e^{\deg D}, \end{aligned}$$

in light of the definition of the degree in Section 3.2. In particular, we see that divisors of same degree produce lattice of the same volume, indicating that we are on the right track. In light of this, we define IdLat_k^0 as the subgroup of ideal lattices coming from degree 0 divisors.

It is natural to ask what the right notion of equivalence of ideal lattices is. Since each lattice is equipped with a metric, we certainly wish distances to be preserved between equivalent lattices. This leads to the notion of an *isometry*, namely a distance-preserving morphism. In this case, we want it to be a linear map, and for our purposes it is useful to respect the embeddings σ. Thus we arrive at the conclusion that an isometry of $\mathcal{O}_k$-ideal lattices is a map acting as multiplication by an element $(z_\sigma)_\sigma$ and which preserves the norm, forcing $|z_\sigma| = 1$ for each σ.

To summarise, we say that two ideal lattices $x\mathcal{L}(\mathfrak{a})$ and $y\mathcal{L}(\mathfrak{b})$ are $\mathcal{O}_k$-*isometric* if there exists an element $(z_\sigma)_\sigma \in k_{\mathbb{R}}$ with $|z_\sigma| = 1$ such that $x\mathcal{L}(\mathfrak{a}) = (z_\sigma)_\sigma y\mathcal{L}(\mathfrak{b})$.

We can now consider the subgroup $\mathrm{Iso}_{\mathcal{O}_k}$ of ideal lattices which are isometric to $\mathcal{L}(\mathcal{O}_k)$ – it is straightforward yet useful to verify that this indeed forms a subgroup – and obtain the following perhaps surprising result:

Theorem 3.3. *The Arakelov class group parameterises ideal lattices up to*

$\mathcal{O}_k$-isometry. In other words, we have a short exact sequence

$$0 \to \mathrm{Iso}_{\mathcal{O}_k} \to \mathrm{Pic}_k^0 \to \mathrm{IdLat}_k^0 \to 0.$$

3.4 A metric on the Arakelov class group

Recall from Section 3.2 that we could regard the Arakelov class group Pic_k^0 topologically as the $\#\,\mathrm{Cl}_k$-fold product of T^0, where T^0 was defined as $H/\ell(\mathcal{O}_k^\times)$, where H is the trace 0 hyperplane of $[\prod_\sigma \mathbb{R}]^+$, and ℓ the logarithmic embedding. Since T^0 is a dimension $r+s-1$ vector space modulo the log-lattice of dimension $r+s-1$, it is a compact real torus.

Given any lattice $L \subset \mathbb{R}^n$ with a norm $\|-\|_{\mathbb{R}^n}$ on $\mathbb{R}^n$, we can define a metric on the fundamental domain $\mathcal{F} := \mathbb{R}^n/L$ by

$$d_{\mathcal{F}}(x+L, y+L) := \min_{v \in L} \|x-y+v\|_{\mathbb{R}^n}$$

For metric spaces in general, we can define a quotient pseudometric in this way, and it is easy to verify that $d_{\mathcal{F}}(x+L, y+L) = 0$ if and only if $x+L = y+L$. The equivalence relation defining $\mathcal{F}$ is given by $x \sim y$ whenever $x - y \in L$.

Alternatively, we can define $d_{\mathcal{F}}$ as the induced Riemannian metric by identifying the tangent space at every point of $\mathcal{F}$ with $\mathbb{R}^n$.

Applying this to our current situation, we obtain a metric on the fundamental domain $T^0 = H/\ell(\mathcal{O}_k^\times)$ which we denote by $\|-\|_{T^0}$, following [4], explicitly given by

$$\|x\|_{T^0} = \min_{\epsilon \in \mathcal{O}_k^\times} \|x + (\log|\sigma(\epsilon)|)_\sigma\|_H.$$

Note that this is **not a norm**, contrary to appearances.

We now return to the last diagram in Section 3.2, more specifically to the exact bottom row,

$$0 \to T^0 \xrightarrow{\phi} \mathrm{Pic}_k^0 \xrightarrow{\psi} \mathrm{Cl}_k \to 0.$$

Recall that topologically, but not group-theoretically, Pic_k^0 can be considered as a $h(k) := \#\,\mathrm{Cl}_k$-fold product of the torus T^0. In these terms, two divisor classes $[D]$ and $[D']$ lie in the same connected component if $\psi([D]-[D']) = [\mathcal{O}_k]$ in Cl_k, $[D]-[D']$ lies in the kernel of ψ. Since the sequence is exact, $\ker\psi = \mathrm{Im}\,\phi$ so $[D]-[D'] \in \mathrm{Im}\,\phi$, and since ϕ is injective, there exists a unique element $u \in T^0$ such that $\phi(u) = [D]-[D']$. Therefore, we can define a metric on the Arakelov class group by $\|[D]-[D']\|_{\mathrm{Pic}_k^0} := \|u\|_{T^0}$.

How do we determine this $u \in T^0$ explicitly? Choose a lift $D - D' + (f)$ of $[D]-[D']$, where f is some element of $k^\times \setminus \mu_k$ and (f) the divisor associated to f, as described in Section 3.2. By exactness of the part of the middle row

$$0 \to H \to \mathrm{Div}_k,$$

there exists a unique element in H being mapped to $D - D' + (f)$. Explicitly, since $[D-D'] \mapsto [\mathcal{O}_k]$ we can assume that $D - D'$ has only the infinite places, $D - D' = \sum_\nu n_\nu \cdot \nu + (f)$. Then the preimage in H of $D - D' + (f)$ is the same as the preimage of, by disregarding the finite places, $\sum_\nu n_\nu \cdot \nu + \sum_\nu -\log|\nu(f)| \cdot \nu$, and this equals the vector $(n_\nu - \log|\nu(f)|)_\nu \in H$. Up to addition by a lattice point, this is exactly the value of u we are looking for.

3.5 Random walks on the Arakelov class group

The main result of [4] is a reduction of a variant of `apprSVP` called `HermiteSVP`, from a worst-case ideal lattice to an "average"-case, in a probabilistic sense. In other words, they show that if we can solve `HermiteSVP` in an average ideal lattice, then up to a slight increase in the approximation factor we can solve it in any ideal lattice.

The method in [4] is based on random walks on Pic_k^0, which are defined by making discrete jumps corresponding to multiplication by a sampled selection prime ideals, combined with a "blurring technique", which is continuous. The first step as achieved by defining so-called Hecke operators, applied to a probability distribution on Pic_k^0 to yield a new probability distribution by a kind of averaging. This enables to use of powerful techniques from analytic number theory. Still, the results obtained are conditional on the generalised Riemann hypothesis, which is highly non-trivial.

Further questions

At this point in time, there are several questions I would look into given more time:

- Is there a way to relate solutions of `apprSVP` in "close" (in the Arakelov class group metric) ideal lattices? In other words, if v is the shortest vector in $x\mathcal{L}(\mathfrak{a})$ with associated Arakelov divisor D, can we find a function $f_D \colon \mathbb{R}_+ \to \mathbb{R}_+$ such that $\|D - D'\|_{\mathrm{Pic}_k^0} < \epsilon$ implies that there is a vector w in the lattice associated with D' with $||v| - |w|| \leq f_D(\epsilon)$?
- More generally, if we define functions $\lambda_i \colon \mathrm{IdLat}_k^0 \to (0, \infty)$ sending an ideal lattice to its i-th successive minimum, is this function continuous? Lipschitz?
- Is it possible to prove weaker versions of the results in [4] without conditioning on the generalised Riemann hypothesis?
- Does the theory developed extend if we replace $\mathcal{O}_k$ by an order (i.e. subring) in $\mathcal{O}_k$, as in [3]? If so, we would be able to reconcile the different definitions of cyclic lattices. If not, what fails, and why?
- Can we use the action of the Galois group on Cl_k to modify the random walk argument? Are there any qualitative differences if we choose k with large contra small Galois group?

References

[1] Eva Bayer-Fluckiger. Ideal lattices. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 168–184. Cambridge Univ. Press, Cambridge, 2002.

[2] J. Buchmann and U. Vollmer. *Binary Quadratic Forms: An Algorithmic Approach*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2007.

[3] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An Efficient Post-Quantum Commutative Group Action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, volume 11274, pages 395–427. Springer International Publishing, Cham, 2018.

[4] Koen de Boer, Léo Ducas, Alice Pellet-Mary, and Benjamin Wesolowski. Random self-reducibility of ideal-svp via arakelov random walks. Cryptology ePrint Archive, Report 2020/297, 2020. https://eprint.iacr.org/2020/297.

[5] Académie des sciences (France). Comptes rendus hebdomadaires des séances de l'académie des sciences / publiés... par mm. les secrétaires perpétuels. Gauthier-Villars , Paris, 1847.

[6] Gerhard Goos, Juris Hartmanis, Jan van Leeuwen, and Phong Nguyen. Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, volume 1666, pages 288–304. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[7] F.C. Kirwan. *Complex Algebraic Curves*. London Mathematical Society Student Texts. Cambridge University Press, 1992.

[8] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[9] P.Q. Nguyen and B. Vallée. *The LLL Algorithm: Survey and Applications*. Information Security and Cryptography. Springer Berlin Heidelberg, 2009.

[10] J.H. Silverman, J. Hoffstein, and J. Pipher. *An Introduction to Mathematical Cryptography*. Undergraduate Texts in Mathematics. Springer New York, 2008.