University of Zurich[UZH]

University of Zurich
Institute of Mathematics

Master Thesis

Hyperelliptic Function Field Lattices: Determinant, Successive Minima, and Automorphism Groups

Author:
Lilian Menn

Supervisor:
Professor Dr. Alberto Cattaneo
Co-supervisor:
Dr. Elif Saçıkara

February 2024

Abstract

In this thesis, we contribute to previously known results by exploring the *successive minima* and *determinant* of *hyperelliptic function field* lattices and the automorphism group of an arbitrary algebraic function field lattice.

Acknowledgments

First, I thank Prof. Alberto Cattaneo for being my supervisor and for making this thesis possible. I would also like to thank Dr. Elif Saçıkara for going above and beyond for me as my supervisor. Thank you for always believing in me and taking so much time for me, and providing me with such an interesting topic for my master's thesis.

I would also like to thank Renate Scheidler for answering my questions on function fields and Reto Schnyder for the seminar which introduced me to lattices.

A big thank you to Niklas Gassner for being my only true friend (maybe Dave). Just kidding, thank you for being there to answer any question, no matter how silly, for listening to all my rants, and for being a great friend. I would like to thank my other friends as well, specifically David Berger, Monika Molnar, Julia Yao and Simon Grüning. Thank you for supporting me, working with me and laughing with me.

Last but not least, I would like to thank my parents for always loving and supporting me unconditionally. I am grateful to have had such a wonderful family and I would not be who I am today without you.

Contents

1 Introduction **1**

2 Preliminaries **4**
2.1 Lattices 4
2.1.1 Basic Definitions and Properties 4
2.1.2 Dual Lattices 11
2.1.3 Automorphism Groups of Lattices 14
2.2 Algebraic Function Fields 17
2.2.1 Automorphisms of Function Fields 22
2.2.2 Elliptic Function Fields 23
2.2.3 Hyperelliptic Function Fields 25

3 A Lattice Construction from Algebraic Function Fields **28**
3.1 Basic Definitions and Properties 28
3.2 Elliptic Function Field Lattices 34
3.3 Hermitian Function Field Lattices 37
3.4 Hyperelliptic Function Field Lattices 38

4 Successive Minima and Determinant of Hyperelliptic Function Field Lattices **41**
4.1 Successive Minima 41
4.2 Determinant of Hyperelliptic Function Field Lattices 46

5 Automorphism Groups of Function Field Lattices **50**
5.1 General Algebraic Function Field Lattices 50
5.2 Rational Function Field Lattices 53
5.3 Lattices from Finite Abelian Groups 55
5.4 Elliptic Function Field Lattices 55
5.5 Hermitian Function Field Lattices 58
5.6 Hyperelliptic Function Field Lattices 59

6 Open Problems **65**

7 References **66**

1 Introduction

Lattices are well-known algebraic structures with applications ranging from sphere packing [CS13] to geometry of numbers [Gru93] and cryptography [DM20; HMM21]. Formally, a lattice is a torsion-free, finite rank $\mathbb{Z}$-module, hence many of its properties can be studied in terms of its basis. For instance, to understand the density of a lattice in Euclidean space we use what is called the *determinant*, which can be computed with the basis.

In addition to the determinant lattices have several interesting invariants such as the *minimum distance*, the *kissing number*, and the *successive minima*, to name a few. Some of these can be very difficult to compute, in a general lattice. In particular, there are cases where even computing the basis itself is difficult, which can lead to difficulty in computing even simple invariants, like the determinant. Of course, many of these invariants are not completely independent from one another. If we are interested in length-preserving maps, like automorphisms of lattices for example, then it is reasonable that lattices with a high amount of vectors of equal length will have more automorphisms and will be more symmetrical. In this thesis we focus on special types of lattices, specifically those constructed from algebraic function fields, or as we have come to call them, function field lattices.

The theory of algebraic function fields is concerned with answering certain questions about finite-dimensional field extensions, F/K, of the field of rational fractions $K(x)$. Function fields are related to Riemann-Surfaces, Algebraic Number Theory and Algebraic Geometry and it has several applications from coding theory [TVZ82] to cryptography [Cas+09]. In general a function field and its complexity can be described by its genus g, but instead of just this global notion the typical approach of studying them is to understand their underlying, or equivalent, local structures. *Places*, which are also known as points from a geometric point of view, play an important role in the characterization of function fields. In function fields over finite fields, it is known that the set of places of bounded *degree* is always finite. We associate their precise algebraic description with the underlying places in $K(x)$ and analyze their properties such as being *ramified, inert* or *splitting*.

A principal divisor of a function f in a function field F/K can be roughly described as a formal sum of places, that provide information about the poles and zeros of f by counting their multiplicities. It is well known that the sum of multiplicities in these principal divisors is equal to zero. One can then generalize this definition to consider any divisor of degree zero, which gives rise to the group of degree zero divisors $\mathrm{Div}^0(F)$. The set of principal divisors $\mathrm{Princ}(F)$ forms a subgroup of $\mathrm{Div}^0(F)$ and their quotient $\mathrm{Cl}^0(F) = \mathrm{Div}^0(F)/\mathrm{Princ}(F)$ is called the

class zero group or Jacobian of F/K in the literature. In the case, of finite fields, it is known that the cardinality of $\mathrm{Cl}^0(F)$ is finite, and it is called the class number of F/K. In the cases of the rational and elliptic function field, the class group can be easily explicitly described, but this becomes more difficult as the genus grows larger.

Initially lattices from algebraic function fields were constructed by Rosenbloom and Tsfasman [RT90] around 1990, and independently by Quebbemann [Que89] to create families of asymptotically good lattices. These are families of lattices with high densities even as the dimension grows. Function field lattices get their structure from a subgroup of the group of principal divisors of a given function field. In other words, the lattice vectors are equivalent to elements in the given function field with specific zeros and poles.

Over the course of the two decades following their construction almost no research was done on these lattices. Starting in 2014 function field lattices were investigated in [FM14]. In this paper the lattices from elliptic function fields were studied, including properties such as their determinant, kissing number, covering radius and the fact that they are well-rounded. Adding on to this, in [Sha15] these lattices were shown to have a basis made up of minimal vectors. Lattices from Hermitian function fields and many of their properties, including their automorphisms, were studied in [Böt+16]. The question of whether function field lattices are well-rounded, was tackled in [AS16], in particular some hyperelliptic function field lattices are not.

In this thesis, after introducing the necessary definitions on lattices and function fields, we first consider the successive minima of function field lattices which are not well-rounded. More specifically, we analyze hyperelliptic function field lattices of a certain genus and defining polynomial, and certain set of places used in their construction. The difficulty here is in understanding the principal divisors with support on certain sets of places.

Then we analyze the determinant of certain hyperelliptic function field lattices. The determinants of these lattices have not been discussed before, unlike those of elliptic or Hermitian function field lattices. Through computing the determinant we observe that, under some assumptions, some hyperelliptic function field lattices have higher density than others. On a related note, for hyperelliptic function field lattices constructed from the set of rational places, even just finding a basis is difficult. Again, this is, in part due to the difficulty of understanding the principal divisors, or similarly, the zero class group.

In addition to the successive minima and the determinant, much of this thesis is dedicated to the study of the automorphism groups of function field lattices. In particular, we want to understand if there are automorphisms of function fields which induce automorphisms on the lattices constructed from them. We do this, by first understanding which types of automorphisms on function fields can define automorphisms on these lattices. In general, we find that the automorphism groups of function fields and lattices are not equivalent, but are related. As a nice example, we show that the automorphisms of the rational function field induce a subgroup of the automorphism group of the rational function field lattice constructed from rational places. We similarly study lattices from elliptic and hyperelliptic function fields.

Studying these automorphisms was done using two main approaches. On the one hand, as already explained, we study automorphism from the function field and how, or if, these define automorphisms on the lattices. On the other hand, since we also want to find as many automorphisms of these lattices as possible, we attempt to find more maps not particularly related to the function fields. Overall, the automorphisms we find act as permutations of the coordinates of the function field lattice.

The structure of this thesis is the following. In Section 2, we provide the necessary background on lattices and algebraic function fields. In Section 3, we present the definition of function field lattices and go over their basic properties. In Section 4, we present our results on the successive minima followed by the computation of the determinant of hyperelliptic function field lattices. In Section 5, we explore the automorphism groups of the lattices and their connections to the automorphisms of function fields.

2 Preliminaries

This section provides the necessary background on lattices and algebraic function fields for function field lattices. We start by introducing the fundamentals of lattices supported by certain examples.

2.1 Lattices

2.1.1 Basic Definitions and Properties

Throughout this section we mainly follow Schnorr's lecture notes [Fis01], and the textbook written by Conway and Sloane [CS13]. While introducing fundamental notions supported by relevant examples, we also mention some well-known problems and applications in lattice theory. Let us begin with the definition of a lattice and its parameters.

Definition 2.1.1. Let $\mathbb{R}^n$ denote the n-dimensional vector space over $\mathbb{R}$.

(i) A **lattice** $\mathcal{L}$ of rank k is a $\mathbb{Z}$-module of the form $\mathcal{L} = \bigoplus_{i=1}^{k} \mathbb{Z}v_i$ where the vectors $v_1, ..., v_k \in \mathbb{R}^n$ are linearly independent over $\mathbb{R}$.

(ii) A **sublattice** $\mathcal{L}'$ of $\mathcal{L}$ is a lattice contained in $\mathcal{L}$ of the same rank.

Here, we note that the definition of sublattice requires that it has the same rank as the lattice it is contained in. Otherwise, we cannot compare them in a meaningful way, because they would not span the same space in $\mathbb{R}^n$. This will become more clear after we explain the *determinant* and the *density* of a lattice.

Let us immediately introduce two examples which often appear throughout this thesis.

Example 2.1.2. In this example, we consider two important classes of lattices. Both of these lattices lie in $\mathbb{R}^{n+1}$ and have rank n.

(i) First we define the root lattice $\mathcal{A}_n$, which is given by

$$\mathcal{A}_n \coloneqq \{v \in \mathbb{Z}^{n+1} \mid \sum_{i=0}^{n} v_i = 0\}.$$

(ii) Second we define the Barnes lattice $\mathcal{B}_n$. This lattice is defined by

$$\mathcal{B}_n \coloneqq \{v \in \mathcal{A}_n \mid \sum_{i=0}^{n} iv_i \equiv 0 \bmod n+1\}.$$

It is easy to see by their definitions that $\mathcal{B}_n$ is a sublattice of $\mathcal{A}_n$.

Sublattices are more sparse than the lattice they are contained in but still have the same rank. Imagine one removed certain points from a lattice so that it was still an additive group, then it is as if one cut regular holes into a net to create a looser net.

To give a different perspective on the structure of lattices we present the following characterization, together with its proof, given in Schnorr's lecture notes [Fis01]. Though we include it here, this is not the main way we think of lattices throughout our results.

Theorem 2.1.3. *$\mathcal{L}$ is a lattice if and only if $\mathcal{L}$ is a discrete subgroup of $\mathbb{R}^n$.*

Proof. Assume $\mathcal{L}$ is a lattice, i.e. there exist linearly independent vectors $\{v_1, ..., v_k\}$ in $\mathbb{R}^n$ such that $\mathcal{L} = \bigoplus_{i=1}^{k} \mathbb{Z}v_i$. The fact that it is an additive subgroup follows from its $\mathbb{Z}$-module structure. Now, to show that it is discrete, consider the linear map

$$\begin{aligned} \phi : \mathbb{R}^k &\longrightarrow \operatorname{span}_{\mathbb{R}}\{v_1, ..., v_k\}, \\ (t_1, ..., t_k) &\longmapsto \sum_{i=1}^{k} t_i v_i. \end{aligned}$$

We can easily see that ϕ is an isomorphism of vector spaces with the property $\phi(\mathbb{Z}^k) = \mathcal{L}$. Further, ϕ^{-1} is continuous, that is, the image of every closed set with respect to the Euclidean norm in $\mathbb{R}^k$ under ϕ, is a closed set in $\operatorname{span}_{\mathbb{R}}\{v_1, ..., v_k\}$ with respect to the norm induced by the Euclidean topology in $\mathbb{R}^k$. Indeed, we can verify this by representing ϕ by a full rank matrix B, i.e. $\phi(t_1, ..., t_k) = B(t_1, ..., t_k)^\top$. Then, we see that for a positive real number r, we have

$$||Bx|| \leq \sup_{\substack{x \in \mathbb{R}^k \\ ||x|| \leq r}} ||Bx|| \leq r\sqrt{\lambda_1},$$

where λ_1 is the largest positive eigenvalue of the positive definite symmetric matrix $BB^\top$. Thus, since $\mathbb{Z}^k$ is discrete it follows that $\mathcal{L}$ is discrete.
For the other implication, assume $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$. Let k be the maximum number of linearly independent vectors in $\mathcal{L}$. We show by induction on k that $\mathcal{L}$ is a lattice.

- $k = 1$
  Let v_1, or also $-v_1$, be the shortest vector in $\mathcal{L}$. This vector exists, since otherwise $\mathcal{L}$ would have an accumulation point. Then necessarily, $\mathbb{Z}v_1 = \mathcal{L}$.

- $k > 1$
  Choose $v_1 \in \mathcal{L} \backslash \{0\}$ such that $\frac{1}{m} v_1 \notin \mathcal{L}$ for all $m \geq 2$. Then we have that

$$\mathbb{Z}v_1 = \mathcal{L} \cap \operatorname{span}_{\mathbb{R}}(v_1).$$

The orthogonal projection $\pi : \mathbb{R}^k \to \mathrm{span}_{\mathbb{R}}(v_1)^{\perp}$ is given by

$$\pi(u) = u - \frac{\langle v_1, u\rangle}{\langle v_1, v_1\rangle} v_1.$$

One can show that $\pi(\mathcal{L})$ is discrete and therefore by induction hypothesis is a lattice of rank $k-1$. Then there exist $k-1$ vectors $v_2, v_3, ...v_k \in \mathcal{L}$ such that $\pi(v_2), ...\pi(v_k)$ form a lattice basis of $\pi(\mathcal{L})$. Since $v_1, v_2, v_3, ...v_k$ are all contained in $\mathcal{L}$ it follows that $\bigoplus_{i=1}^{k} \mathbb{Z}v_i \supseteq \mathcal{L}$. Left to show is the other inclusion.
Let $u \in \mathcal{L}$. Then we have that $\pi(u) \in \pi(\mathcal{L}) = \bigoplus_{i=2}^{k} \mathbb{Z}\pi(v_i)$ and so there exists a vector $\tilde{u} \in \bigoplus_{i=2}^{k} \mathbb{Z}v_i$ with $\pi(\tilde{u}) = \pi(u)$. It follows that $u - \tilde{u} \in \mathrm{span}_{\mathbb{R}}(v_1)$. Since the vectors u and $\tilde{u}$ are both contained in $\mathcal{L}$ we have that $u - \tilde{u} \in \mathcal{L} \cap \mathrm{span}_{\mathbb{R}}(v_1) = \mathbb{Z}v_1$. Therefore $u \in \bigoplus_{i=1}^{k} \mathbb{Z}v_i$ and so $\mathcal{L} = \bigoplus_{i=1}^{k} \mathbb{Z}v_i$.

□

The following definition gives us one of the simplest description of a lattice, namely its basis matrix.

Definition 2.1.4. Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$. Then a set of vectors $\{v_1, ..., v_k\}$ such that $\mathcal{L} = \bigoplus_{i=1}^{k} \mathbb{Z}v_i$, is called a **basis** of the lattice. Moreover, the $k \times n$ matrix B whose ith row is v_i is called the **basis matrix** of $\mathcal{L}$.

By this definition, every lattice can be completely described by a basis matrix. Every point in the lattice is given by $u \cdot B$ for some $u \in \mathbb{Z}^k$. These matrices are not unique however. The following lemma details when two matrices generate the same lattice.

Lemma 2.1.5. *Two basis matrices B, B' of a lattice $\mathcal{L}$ of rank k are equivalent if and only if there exists a unimodular matrix $U \in \mathrm{GL}_k(\mathbb{Z})$ such that*

$$B' = UB.$$

Example 2.1.6. One possible basis matrix of the root lattice $\mathcal{A}_n$ is given by the $n \times (n+1)$ matrix

$$B_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & -1 \\ 0 & 1 & 0 & \cdots & -1 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -1 \end{pmatrix}.$$

Another commonly seen example for this lattice is the following $n \times (n+1)$ matrix

$$B_2 = \begin{pmatrix} 1 & -1 & 0 & & \cdots & 0 \\ 0 & 1 & -1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ & & & & & \\ 0 & & \cdots & 0 & 1 & -1 \end{pmatrix}.$$

For $n \geq 4$, a basis matrix of $\mathcal{B}_n$ of size $n \times (n+1)$ can be given by

$$B = \begin{pmatrix} 1 & 1 & -1 & 0 & 0 & \cdots & 0 & 0 & -1 \\ 1 & 0 & 1 & -1 & 0 & \cdots & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 & -1 & \cdots & 0 & 0 & -1 \\ \vdots & & & & \ddots & \ddots & \vdots & & \\ 1 & 0 & 0 & 0 & 0 & \cdots & 1 & -1 & -1 \\ -1 & 1 & 0 & 0 & 0 & \cdots & 1 & -1 & 0 \\ -1 & 1 & 0 & 0 & 0 & \cdots & 0 & 1 & -1 \end{pmatrix}.$$

Next, we define our first lattice invariant, the determinant. The points in a lattice can be viewed as the corners of equally sized parallelotopes, which cover the space spanned by the lattice. Then the determinant is the volume of one of these parallelotopes. The determinant is used to compute the density of a lattice, for example.

Definition 2.1.7. Let $\mathcal{L}$ be a lattice of rank k in $\mathbb{R}^n$.

(i) For a basis matrix B of $\mathcal{L}$, the **fundamental parallelotope** of $\mathcal{L}$ is defined as

$$P(B) = \Big\{ \sum_{i=1}^{k} t_i v_i \mid t_i \in \mathbb{R} \text{ and } 0 \leq t_i < 1 \Big\}.$$

(ii) The **determinant** $\det(\mathcal{L})$ of a lattice is defined as the volume of its fundamental parallelotope.

Remark 2.1.8. Before we give one or two examples, we note that, the determinant can equivalently be calculated by $\det(\mathcal{L}) \coloneqq \sqrt{\det(BB^T)}$. This equivalence follows from the fact that the volume of a paralletope can be computed using the *Gram* matrix. This expression for computing the determinant is a lot more practical in most cases.

Example 2.1.9. Let us find the determinants of the root lattice and Barnes lattice.

(i) The determinant of the root lattice $\mathcal{A}_n$ is given by

$$\det(\mathcal{A}_n) = \sqrt{\det(BB^T)} = \det \begin{pmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & 2 \end{pmatrix}^{\frac{1}{2}} = \sqrt{n+1}.$$

(ii) To compute the determinant of $\mathcal{B}_n$ we use that it is a sublattice of $\mathcal{A}_n$. In general for a lattice $\mathcal{L}$ and a sublattice $\mathcal{L}' \subset \mathcal{L}$ we have that

$$\det(\mathcal{L}') = \det(\mathcal{L}) \cdot [\mathcal{L} : \mathcal{L}']$$

where $[\mathcal{L} : \mathcal{L}']$ is the index of the lattice and its sublattice as groups. This index is finite since they have the same rank.

Then by the definition of the Barnes lattice $\mathcal{B}_n$ we see that

$$\det(\mathcal{B}_n) = \det(\mathcal{A}_n) \cdot [\mathcal{A}_n : \mathcal{B}_n] = \sqrt{n+1} \cdot (n+1) = (n+1)^{\frac{3}{2}}.$$

Notice that the determinant of a lattice does not change depending on the basis. One can check that using either B_1 or B_2 from example 2.1.6 yields the same result, namely $\det(\mathcal{A}_n) = n + 1$. So as long as we have any basis of a lattice we can easily compute its determinant. For some lattices, determining a basis is not trivial and so we use other methods to compute the determinant, as done in example 2.1.9 for $\mathcal{B}_n$. In Subsection 4.2 we do this in the case of some hyperelliptic function field lattices.

The next set of definitions leads us into some well known problems in lattice theory such as the *shortest vector problem* or the *sphere packing problem.*

Definition 2.1.10. The standard Euclidean norm is used to determine length and distance since lattices in general are embedded in $\mathbb{R}^n$.

(i) For a nonzero vector $v \in \mathcal{L} \subset \mathbb{R}^n$, its **length** is defined as

$$||v|| \coloneqq \left(\sum_{i=1}^{n} v_i^2 \right)^{\frac{1}{2}}.$$

(ii) The **minimum distance** of a lattice $\mathcal{L}$ is defined as

$$d(\mathcal{L}) \coloneqq \min\{||v|| : v \in \mathcal{L} \backslash \{0\}\}.$$

Computing the minimum distance, or equivalently, determining the shortest vector of a given lattice is a well-known problem in lattice theory. The shortest vector problem (SVP), as the name suggests, is the problem of finding the shortest non-zero vector in a lattice given a random basis. In [Ajt98] the SVP was shown to be NP-hard for randomized reductions. On the other hand, there are some well-known algorithms for approximating the shortest vector, for instance Lenstra-Lenstra-Lovász, or LLL for short, and more recently *sieve algorithms*. Though LLL runs in polynomial time, it approximates the shortest vector within a factor which is exponential in the dimension of the lattice.
Closely related to this, pun intended, is the closest vector problem (CVP). This is the problem of finding the closest vector in a lattice to any given point in $\mathbb{R}^n$. Though this seems to be the same problem as the SVP at first glance, there are slight differences and unlike the SVP, the CVP was proven to be NP-hard in [Emd81].

Definition 2.1.11. Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$.

(i) The **set of minimal vectors** is defined as

$$S(\mathcal{L}) \coloneqq \{v \in \mathcal{L} : ||v|| = d(\mathcal{L})\}.$$

(ii) The number of minimal vectors $|S(\mathcal{L})|$ is called the **kissing number** of $\mathcal{L}$, denoted by $\kappa(\mathcal{L})$.

Example 2.1.12. (i) We once again use $\mathcal{A}_n$ as our example, as defined in example 2.1.2. The minimum distance of $\mathcal{A}_n$ is $\sqrt{2}$ and the minimal vectors are those of the form

$$\pm\begin{pmatrix}0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -1 & 0 \cdots & 0\end{pmatrix}$$

From this we deduce that $\mathcal{A}_n$ has kissing number $\kappa = 2\binom{n}{2} = n(n-1)$.

(ii) Famously, the leech lattice Λ_{24} has the highest possible kissing number in dimension 24, namely 196560.

The kissing number is related to the sphere packing problem. Imagine a number of equally sized spheres, all of which touch, or "kiss", a sphere in the center of the same size. One may ask, what is the largest possible number of spheres that can be arranged in this way? Or more specifically related to lattices, if we take these spheres to be centered around the shortest vectors and the origin with radius $d(\mathcal{L})/2$, then the question becomes, what is the largest possible kissing number that a lattice can have? In some dimensions the answer is known. In [CS13] it is stated that for $n \leq 9$ it was shown that the highest possible kissing numbers are attained by the laminated lattices Λ_n. But in most other dimensions there is only an estimated range for the maximum kissing number.

Definition 2.1.13. The **i-th successive minimum** $\lambda_i(\mathcal{L})$ of a lattice $\mathcal{L}$ is the smallest real number $r \in \mathbb{R}$ such that there exist i linearly independent vectors in $\mathcal{L}$, of length at most r.

Remark 2.1.14. From definition 2.1.13 it is easy to see that $\lambda_1(\mathcal{L}) = d(\mathcal{L})$. We also note that for any lattice we have

$$\lambda_1(\mathcal{L}) \leq \lambda_2(\mathcal{L}) \leq \ldots \leq \lambda_k(\mathcal{L}).$$

There are some interesting applications of the successive minima, as detailed in [Wen18], for example. However, finding the successive minima of a given lattice is a difficult problem, in general.

Definition 2.1.15. The **sphere packing density** of a lattice describes the proportion of space which is taken up by open spheres with radius $d(\mathcal{L})/2$, which are centered at points in the lattice. This is given by $\Delta(\mathcal{L}) \coloneqq \frac{d(\mathcal{L})^k V_K}{2^k det(\mathcal{L})}$ where V_k is the volume of the k-dimensional unit sphere.

Naturally this leads to the question, what are the lattices which attain the highest density? In dimensions $n \leq 8$ we have the answer, but similarly to the kissing number problem we only have an estimated range in most dimensions.

It seems intuitive for these two notions, kissing number and density, to be related. A lattice with a high kissing number will likely be more dense. However, as well-put in [CS13], achieving the highest kissing number is more of a local problem and achieving the highest density more of a global problem. In dimension 11, for example, the best currently known solutions to these problems are two distinct lattices.

Another lattice property that we often discuss in the following sections is well-roundness. We introduce this and two related properties in the next definition.

Definition 2.1.16. Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$.

(i) A lattice of rank k is called **well-rounded** if $S(\mathcal{L})$ contains k linearly independent vectors.

(ii) A lattice $\mathcal{L}$ is called **strongly well-rounded** if it is generated by its minimal vectors, i.e. $\mathcal{L} = \text{span}_{\mathbb{Z}} S(\mathcal{L})$.

(iii) A lattice $\mathcal{L}$ has a **basis of minimal vectors** if $S(\mathcal{L})$ contains a basis of $\mathcal{L}$.

Remark 2.1.17. By the above definition, a lattice is well-rounded if and only if all its successive minima are equal, i.e.

$$\lambda_1(\mathcal{L}) = \lambda_2(\mathcal{L}) = ... = \lambda_k(\mathcal{L}).$$

It follows that the successive minima problem is really only interesting when a lattice is not well-rounded. We study one such case in Section 4.1.

It is known that the densest lattices typically have large kissing numbers and that well-rounded lattices are often studied when these two problems are discussed [HMM21].

For $n \leq 4$ the three notions in Definition 2.1.16 are equivalent. In higher dimensions, it is clear that having a basis of minimal vectors implies that the lattice is strongly well-rounded, i.e. is generated by its minimal vectors. Though it might not seem intuitive at first, there is a famous example by Conway and Sloane [CS95] which shows that the other implication does not hold.

Similarly, a strongly well-rounded lattice is always well-rounded, but again, the converse is not true. An example of this is shown in [DM20] and we present it here in more detail.

Example 2.1.18. Take the lattice $\mathcal{L}$ in $\mathbb{R}^n$ generated by the standard basis vectors $e_1, ..., e_{n-1}$ and the vector $v = (\frac{1}{k}, ..., \frac{1}{k})$ with $k^2 < n$.
This lattice has rank n since $e_1, .., e_{n-1}$ and v are linearly independent and its determinant is

$$\det\left(\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ & & \ddots & & \\ 0 & \dots & 0 & 1 & 0 \\ \frac{1}{k} & \frac{1}{k} & \dots & \frac{1}{k} & \frac{1}{k} \end{pmatrix}\right) = \frac{1}{k}.$$

The minimum distance is 1 and so the set of shortest vectors in this case is

$$S(\mathcal{L}) = \{\pm e_1, \dots, \pm e_n\}.$$

Note that v is not in $S(\mathcal{L})$ since its length is $||v|| = \sqrt{\frac{n}{k^2}} > 1$. $S(\mathcal{L})$ contains n linearly independent vectors, so $\mathcal{L}$ is well-rounded. However, the shortest vectors do not generate the vector v and therefore do not generate the whole lattice.

The lattices we focus on throughout this thesis are often, but not always, well-rounded.

Example 2.1.19. Both lattices $\mathcal{A}_n$ and $\mathcal{B}_n$ have a basis of minimal vectors and hence are well-rounded. Indeed, the basis matrices of these lattices shown in example 2.1.6 both consist of minimal vectors of length $\sqrt{2}$ and 2 respectively.

2.1.2 Dual Lattices

In this subsection we introduce dual lattices. The idea of their construction shares similarities to those of dual spaces or dual codes in coding theory. We first define the dual lattice and then go over some of its properties. The structure and geometry of the lattice and its dual are connected in some ways. This leads to the dual often being useful in understanding the lattice itself better, such as with the successive minima or automorphisms for example.

Definition 2.1.20. The **dual** $\mathcal{L}^*$ of a lattice $\mathcal{L}$ is given by the set of all vectors $u \in \mathrm{span}_{\mathbb{R}}(\mathcal{L})$ such that $\langle u, v\rangle \in \mathbb{Z}$ for all v in $\mathcal{L}$, where $\langle \cdot, \cdot \rangle$ denotes the standard scalar product in $\mathbb{R}^n$.

Remark 2.1.21. If the basis matrix of a lattice $\mathcal{L}$ is B, then the basis matrix of the dual lattice is given by $D = (BB^\top)^{-1}B$. This is in part because we then have $BD^\top = I_n$, where I_n denotes the identity matrix of size n. By this observation, the dual lattice can be easily constructed when the basis matrix of $\mathcal{L}$ is given. We illustrate this with the root lattice in the following example.

Example 2.1.22. Let $\mathcal{A}_n$ denote the root lattice introduced in Example 2.1.2. One particular basis matrix that we have already seen in Example 2.1.6 is given by

$$B = \begin{pmatrix} 1 & 0 & 0 & \cdots & -1 \\ 0 & 1 & 0 & \cdots & -1 \\ \vdots & & \ddots & & \vdots \\ 0 & \cdots & 0 & 1 & -1 \end{pmatrix}.$$

Then by Remark 2.1.21, a basis of the dual lattice is given by the following $n \times (n+1)$ matrix

$$D = \frac{1}{n+1} \begin{pmatrix} -n & 1 & 1 & \cdots & 1 \\ 1 & -n & 1 & \cdots & 1 \\ \vdots & & \ddots & & \vdots \\ 1 & 1 & \cdots & -n & 1 \end{pmatrix}.$$

We can check that indeed $BD^\top = I_n$.

The following are some simple and well-known properties of the dual lattice. Most of these and their proofs can be found in [Reg04] for example.

Proposition 2.1.23. *Let $\mathcal{L}^*$ be the dual lattice of $\mathcal{L}$.*

(i) The dual of $\mathcal{L}^*$ is $(\mathcal{L}^*)^* = \mathcal{L}$.

(ii) The determinant of the dual is $\det(\mathcal{L}^*) = \frac{1}{\det(\mathcal{L})}$

(iii) If $\mathcal{L}$ is integral i.e. its Gram-matrix only has integer entries, then

$$\mathcal{L} \subseteq \mathcal{L}^* \subseteq \frac{1}{\det(\mathcal{L})^2} \cdot \mathcal{L}.$$

Next are two results which link the successive minima of a lattice and its dual, the first of which follows from Minkowski's bound.

Proposition 2.1.24. *Let $\mathcal{L}$ be a lattice of rank n and $\mathcal{L}^*$ be its dual, then the following hold.*

(i) $\lambda_1(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \leq n$,

(ii) $\lambda_1(\mathcal{L}) \cdot \lambda_n(\mathcal{L}^*) \geq 1$,

where λ_1 denote the first and n-th successive minima respectively.

Remark 2.1.25. Though a lattice and its dual can share some characteristics, duality does not preserve properties like well-roundness. Recall from Example 2.1.19 that the Barnes lattice $\mathcal{B}_n$ is well-rounded. In [Mar13] it is described that when its rank is $n = 8$, for example, then the dual of the Barnes lattice $\mathcal{B}_8^*$ only has three minimal vectors and therefore cannot be well-rounded.

Remark 2.1.26. Note that for lattices, inclusion is reversed when taking the dual, i.e. $\mathcal{L}' \subseteq \mathcal{L}$ implies that $\mathcal{L}^* \subseteq (\mathcal{L}')^*$.

The next proposition explains how one can construct the dual of a sublattice by constructing a set of vectors which, together with $\mathcal{L}^*$, generate $(\mathcal{L}')^*$.

Proposition 2.1.27. *[Mar13, Proposition 1.3.8.] Let $\mathcal{L}$ be a lattice and $\mathcal{L}' \subseteq \mathcal{L}$ be a sublattice. Let $u_1, \ldots, u_r$ be a finite set of vectors in $\mathcal{L}$ and m_i, for $1 \leq i \leq r$, be integers such that $\mathcal{L}'$ is equal to the intersection of the kernels of the homomorphisms*

$$\begin{aligned} \mathcal{L} &\to \mathbb{Z}/m_i\mathbb{Z} \\ v &\mapsto \langle v, u_i \rangle \bmod m_i. \end{aligned}$$

Then $(\mathcal{L}')^*$ is generated by $\mathcal{L}^*$ and the vectors $\frac{1}{m_i}u_i$ for $1 \leq i \leq r$.

In the following example we directly apply Proposition 2.1.27 to compute the dual of the Barnes lattice $\mathcal{B}_n$.

Example 2.1.28. Recall the definition of the Barnes lattice $\mathcal{B}_n$ in Example 2.1.2. The vectors in $\mathcal{B}_n$ are those x in $\mathcal{A}_n$ which fulfill the relation

$$\sum_{i=0}^{n} i \cdot x_i \equiv 0 \bmod (n+1).$$

We want to find vectors such that $\mathcal{B}_n$ is the kernel of the homomorphism described in the previous proposition. To this end, take u to be the vector $(0, 1, 2, \ldots, n)$. However, u is not in the lattice $\mathcal{A}_n$, so we take $v = u - \frac{n}{2}\mathbf{1}$ instead, where $\mathbf{1}$ denotes the vector whose entries are all equal to 1. Notice that we then still fulfill

$$\langle x, v \rangle = \langle x, (u - \frac{n}{2}\mathbf{1}) \rangle = \sum_{i=0}^{n} i \cdot x_i - \frac{n}{2} \sum_{i=0}^{n} x_i \equiv 0 \bmod (n+1)$$

for any x in the Barnes lattice and that

$$\sum_{i=0}^{n} v_i = \sum_{i=0}^{n} (i - \frac{n}{2}) = 0,$$

which means v is in $\mathcal{A}_n$. By Proposition 2.1.27 the dual of the Barnes lattice is generated by $\mathcal{A}_n^*$ and the vector v^* given by

$$v^* = \frac{1}{n+1} \left[\begin{pmatrix} 0 \\ 1 \\ \vdots \\ n \end{pmatrix} - \frac{n}{2} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \right].$$

A basis of the dual consists of $\{b_1, b_2, \ldots, b_{n-1}, v^*\}$, where the vectors b_i are the rows of the basis matrix of $\mathcal{A}_n^*$ from Example 2.1.22. This is because b_n can be generated be the other n vectors as follows

$$n \cdot b_1 + (n-1) \cdot b_2 + \ldots + 2 \cdot b_{n-1} - (n+1) \cdot v^* = -b_n.$$

2.1.3 Automorphism Groups of Lattices

The automorphisms of a lattice are essential in understanding the symmetries of a lattice. The question is, how one can spin or mirror the points of a lattice to still obtain the same lattice after. This means that what we want are isometries, which are still bijections when restricted to the lattice. These maps form the automorphism group of a lattice. The following definition and theorem are taken from [Mar13].

Definition 2.1.29. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two lattices in $\mathbb{R}^n$ of the same rank. Then an **isometry** of $\mathcal{L}_1$ onto $\mathcal{L}_2$ is an isometry of $\mathbb{R}^n$ which sends $\mathcal{L}_1$ to $\mathcal{L}_2$. An **automorphism** of a lattice $\mathcal{L}$ is an isometry of the lattice onto itself. Then the set of all automorphisms of the lattice is the automorphism group of $\mathcal{L}$ denoted $\mathrm{Aut}(\mathcal{L})$.

From this definition we see that an orthogonal matrix $O \in \mathrm{O}(\mathbb{R}^n)$ is an automorphism of a lattice given by $B \in \mathbb{R}^{k \times n}$, if there exists a matrix $U \in \mathrm{GL}_k(\mathbb{Z})$ such that

$$BO = UB.$$

This is because BO generates the image of the lattice under the isometry O and is equal to another basis matrix which generates our original lattice.
Since $\mathrm{GL}_k(\mathbb{Z})$ is discrete and $\mathrm{O}(\mathbb{R}^n)$ is compact this gives us our first important fact about the automorphism groups of lattices.

Theorem 2.1.30. *The automorphism group of a lattice is finite.*

Isometry preserves many of the defining characteristics of a lattice. The determinant, kissing number and well-roundedness are all preserved under isometry. For most lattices the automorphism group has only two elements, those being $\{\pm \mathrm{Id}\}$. But there are lattices with far more interesting automorphism groups.

Example 2.1.31. The following examples are two very well-known lattices.

(i) The integer lattice $\mathbb{Z}^n$ has $2^n n!$ automorphisms, namely the signed permutations. In higher dimensions this is known to be the largest possible automorphism group of a lattice in $\mathbb{R}^n$.

(ii) The *Leech Lattice* L_{24} in $\mathbb{R}^{24}$, has the automorphism group $\mathrm{Aut}(L_{24}) = \{\pm \mathrm{Id}\} \times \mathrm{Co}_1$, with Co_1 being Conway's sporadic simple group of order $2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$.

When discussing well-rounded lattices it is more common to use similarity, a weaker relation than isometry. Two lattices given by B_1 and B_2 are said to be similar if there exist an $\alpha \in \mathbb{R}_+$ and an orthogonal matrix $O \in \mathcal{O}(\mathbb{R}^n)$ such that $B_1 = \alpha B_2 O$. Instead of just spinning and reflecting the lattice we also scale it. Now the question is, whether similarity also preserves the automorphism group of a lattice. In the following lemma we prove that it does. This is needed in Subsection 5.6 to determine the automorphism group of specific hyperelliptic function field lattices.

Lemma 2.1.32. *If two lattices are similar then their automorphism groups are isomorphic.*

Proof. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two similar lattices in $\mathbb{R}^n$. Let their basis matrices be denoted by B_1 and B_2. Then there exist an $\alpha \in \mathbb{R}_+$ and $O \in \mathcal{O}(\mathbb{R}^n)$ such that

$$B_1 = \alpha B_2 O.$$

Let $V \in \mathrm{Aut}(\mathcal{L}_1)$ be an automorphism. Then V is an orthogonal matrix and there exists a unimodular matrix $U \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$B_1 V = U B_1.$$

Now using the similarity of $\mathcal{L}_1$ and $\mathcal{L}_2$ we get

$$\alpha B_2 O V = U \alpha B_2 O.$$

Since α is a positive real number we can simply divide by it on both sides and then multiply from the right hand side by O^{-1} which gives us

$$B_2 O V O^{-1} = U B_2.$$

This proves that OVO^{-1} is an automorphism of $\mathcal{L}_2$. Now define the map given by

$$\begin{aligned} \mathrm{Aut}(\mathcal{L}_1) &\to \mathrm{Aut}(\mathcal{L}_2) \\ V &\mapsto OVO^{-1}. \end{aligned}$$

We just showed that this map is well-defined and it is easy to show that it is an injective group homomorphism.
Finally, since we can symmetrically argue that there is an injective group homomorphism from $\mathrm{Aut}(\mathcal{L}_2)$ to $\mathrm{Aut}(\mathcal{L}_1)$, we can conclude that the two groups are isomorphic.

□

Interestingly, even though a lattice and its dual are not necessarily isometric or even similar, their automorphism groups are always isomorphic. This can sometimes be useful when trying to find all automorphisms of a lattice. Since automorphisms preserve the length of vectors, we can sometimes use the number of vectors of a certain length in the lattice or its dual to understand the number automorphisms. We will illustrate an example of this when discussing the automorphisms of elliptic function field lattices in Remark 5.4.5.

Lemma 2.1.33. *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ then* $\mathrm{Aut}(\mathcal{L}) \cong \mathrm{Aut}(\mathcal{L}^*)$.

Proof. Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ and let $V \in \mathrm{Aut}(\mathcal{L})$ be the matrix representation of the lattice automorphism. Then by definition V is an isometry of $\mathbb{R}^n$ and the only thing left to show is that it defines a bijection on $\mathcal{L}^*$. Let $y \in \mathcal{L}^*$. By definition of the dual we have

$$\langle x, y \rangle \in \mathbb{Z} \text{ for all } x \in \mathcal{L}.$$

Since V is an isometry we have

$$\langle xV, yV \rangle \in \mathbb{Z} \text{ for all } x \in \mathcal{L}.$$

V is a bijection on $\mathcal{L}$ so therefore

$$\langle x, yV \rangle \in \mathbb{Z} \text{ for all } x \in \mathcal{L},$$

which implies that yV is an element of $\mathcal{L}^*$. The map $\mathcal{L}^* \to \mathcal{L}^*$ given by $y \mapsto yV$ is injective because V is an invertible matrix. Therefore V is an automorphism of the dual $\mathcal{L}^*$ and $\mathrm{Aut}(\mathcal{L}) \subseteq \mathrm{Aut}(\mathcal{L}^*)$. The other direction follows from the fact that $(\mathcal{L}^*)^* = \mathcal{L}$ and we conclude that $\mathrm{Aut}(\mathcal{L}) \cong \mathrm{Aut}(\mathcal{L}^*)$. □

We show in Lemma 2.1.32 that similar lattices have the same automorphism group. However, two lattices having isomorphic automorphism groups does not imply that they are similar. We can now demonstrate this with an example using the dual.

Example 2.1.34. In this example we construct a lattice in Magma [BCP97] with determinant 1. Then we construct a new lattice by taking the dual of the first. By Lemma 2.1.33 these lattices have isomorphic automorphism groups, which we can also check.
Now since they both have determinant 1 we can check, without having to worry about rescaling, whether they are isometric. Indeed they are not.

```
>L1 := LatticeWithBasis(3, [1/3,0,0, 0,1/3,0, 0,0,9]);
>L2 := Dual(L1 : Rescale := false);
>G1 := AutomorphismGroup(3*L1);
>G2 := AutomorphismGroup(9*L2);
>IsIsomorphic(G1, G2);
true Mapping from: GrpMat: G1 to GrpMat: G2
Composition of Mapping from: GrpMat: G1 to GrpPC and
Mapping from: GrpPC to GrpPC and
Mapping from: GrpPC to GrpMat: G2
>IsIsometric(L1, L2);
false
```

Remark 2.1.35. We close this section with the following observation on a lattice $\mathcal{L}$ and sublattice $\mathcal{L}' \subseteq \mathcal{L}$. The automorphism groups of the lattice and that of the sublattice are, in general, not subgroups of one another. This may not seem intuitive at first. On the one hand, a sublattice might not have all the automorphisms that the lattice has, which makes sense when considering that $\mathcal{L}'$ is a subgroup of $\mathcal{L}$. On the other hand, being less dense opens up the possibility for more automorphisms which the lattice $\mathcal{L}$ does not have. Their automorphism groups are therefore related, in the sense that they share many elements, but in general are not subgroups of one another.

Take as an example, once again, the Barnes lattice $\mathcal{B}_n$ which is a sublattice of the root lattice $\mathcal{A}_n$. There are some dimensions in which their automorphism groups are not contained in one another. We detail this in Remark 5.4.5.

2.2 Algebraic Function Fields

Throughout this section we mainly follow [Sti09] and [Sal06]. First we list the fundamental definitions supported by well-known examples. Let us begin with the definition of an algebraic function field.

Definition 2.2.1. An **algebraic function field of one variable** over K is a field extension F over K, denoted by F/K, such that there exists a transcendental element $x \in F$ and $[F : K(x)] < \infty$.

Example 2.2.2. (i) The simplest example is known as the rational function field, which is the field of fractions $K(x)$, because x is transcendental over K, and the extension degree of $K(x)$ over itself is one.

(ii) As another example consider $F := K(x, y)$ where x and y are variables satisfying the algebraic equation $y^2 = f(x)$, with the degree three square-free polynomial $f(x) \in K[x]$.

The following definitions describe core structures inside of function fields.

Definition 2.2.3. Let F/K be a function field.

(i) A **valuation ring** $\mathcal{O}$ of F/K is a subring such that $K \subsetneq \mathcal{O} \subsetneq F$, and for all $z \in F$, one has $z \in \mathcal{O}$, $z^{-1} \in \mathcal{O}$ or both.

(ii) Such a ring $\mathcal{O}$ is a local ring and its maximal ideal $P := \mathcal{O} \setminus \mathcal{O}^*$ is called a **place** of F/K.

We denote the set of places of a function field F by $\mathbb{P}(F)$.

Example 2.2.4. All places in $K(x)$ are either of the form $P_{p(x)}$, meaning the irreducible polynomial $p(x) \in K[x]$ is a prime element of P, or P_∞ denoting the pole of x.

In the above example we mention prime elements. The valuation rings $\mathcal{O}$ are PIDs, which in particular means their maximal ideals P are generated by a prime element. In the following remark we use this to elaborate on why places are important to understanding algebraic function fields.

Remark 2.2.5. Let P be a place of F/K and let t be its prime element. Any element $z \in F$ can then be uniquely expressed as $z = t^n u$, for an integer $n \in \mathbb{Z}$ and a unit $u \in \mathcal{O}_P^*$. This allows us to define a discrete valuation map v_P for a given place P, which satisfies

$$v_P(z) = n.$$

For the purposes of this thesis, we define the valuation maps v_P through their places. In general, one can also first define discrete valuation maps on the function field and then derive the places from those. In this sense, the valuation rings, their places, and the valuation maps are interchangeable notions describing the structure of a function field.

Definition 2.2.6. Let F/K be a function field and P be a place in it.

(i) The quotient $F_P := \mathcal{O}/P$ is called the **residue class field** of F/K at P.

(ii) The **degree of a place** P is defined as the extension degree $\deg(P) := [F_P : K]$. If the degree of a place is one, then we call it a **rational place**.

Example 2.2.7. Let us consider the rational function field $K(x)$ again. As stated in Example 2.2.4, the places in $K(x)$ are usually of the form $P_{p(x)}$. In this case the degree of $P_{p(x)}$ is equal to the degree of the polynomial $p(x)$.

It is known that the degrees of all places are finite. Furthermore, we can now consider the the places as the zeros and poles of a given function z counting their multiplicities.

Definition 2.2.8. Let $P \in \mathbb{P}(F)$ and $z \in F$.

(i) P is called a **zero** of z of multiplicity n if $v_P(z) = n > 0$.

(ii) P is called a **pole** of z of multiplicity n if $v_P(z) = -n < 0$.

As we create extension of function fields, their elements become more difficult to picture or describe intuitively. Instead of relying on explicit descriptions of function field elements we can instead describe each one as a sum of its zeros and poles with multiplicities. For this we need the following definition.

Definition 2.2.9. Let F/K be a function field and $\mathbb{P}(F)$ denote its set of places.

(i) A **divisor** D is defined as a formal sum

$$D = \sum_{P \in \mathbb{P}(F)} n_P P,$$

where all but finitely many of the integer coefficients $n_p \in \mathbb{Z}$ are zero.

(ii) The **divisor group**, denoted by $(\mathrm{Div}(F), +)$, is the set of all divisors D, where the addition of two divisors is given component-wise.

(iii) The **degree of a divisor** $\deg(D)$ is defined as

$$\deg(D) := \sum_{P \in \mathbb{P}_F} n_P \cdot \deg(P).$$

As already mentioned, these divisors are important to understand function fields, but the divisor group $\mathrm{Div}(F)$ is the set of every possible divisor, which in most cases is way more than we need to describe F. We are mostly interested in specific types of divisors, one of which is introduced in the following example.

Example 2.2.10. Let $z \in F\backslash\{0\}$. Then the principal divisor of z is defined as

$$(z) := \sum_{P \in \mathbb{P}(F)} v_P(z)P.$$

The principal divisor describes the element z as a sum of its zeros and poles with multiplicities.

Now we focus on some special subgroups of $\mathrm{Div}(F)$ which will be vital in defining and understanding the structure of function field lattices.

Definition 2.2.11. Let F/K be a function field and $\mathbb{P}(F)$ denote its set of places.

(i) The **group of degree zero divisors** is given by

$$\mathrm{Div}^0(F) := \{D \in \mathrm{Div}(F) \mid \deg(D) = 0\}.$$

(ii) The **group of principal divisors** is given by

$$\mathrm{Princ}(F) := \{D \in \mathrm{Div}(F) \mid D = (x) \text{ for some } x \in F\backslash\{0\}\}.$$

Remark 2.2.12. In most cases $\mathrm{Princ}(F)$ is a proper subgroup of $\mathrm{Div}^0(F)$. That is, every element in the function field is described by a divisor but not every degree zero divisor describes an element in F. The only example we mention in which these groups are equal is the rational function field $K(x)$.

Definition 2.2.13. The **zero class group** $\mathrm{Cl}^0(F)$ is given by the quotient

$$\mathrm{Cl}^0(F) := \mathrm{Div}^0(F)/\mathrm{Princ}(F).$$

The cardinality of the zero class group is called the **class number** h of a function field.

The class number h is very important for function field lattices later. From the definition of the class zero group, we can interpret h as the number which describes "how many more" degree zero divisors than principal divisors there are.

The algebraic function fields we focus on throughout this thesis are extensions of the rational function field $K(x)$. Therefore it is important to understand what happens to the places, corresponding valuation maps, and divisors in these extensions.

Definition 2.2.14. Let F/K be an algebraic extension of $K(x)$. A place $P' \in \mathbb{P}(F')$ in the extension is said to **lie over** $P \in \mathbb{P}(K(x))$ if $P \subseteq P'$. We also say that P' is an **extension** of P. We denote this by $P'|P$.

For any place P of $K(x)$ the number of places which lie above it ranges from one to the extension degree $[F : K(x)]$. In the following definition we describe three special cases of how a place can behave in the extension.

Definition 2.2.15. Let F/K be a finite extension of $K(x)$ of degree $[F : K(x)] = n$, and let $P \in \mathbb{P}(F)$. Then

(i) P is said to **split completely** in $F/K(x)$ if there are exactly n distinct places $P' \in \mathbb{P}(F')$ with $P'|P$.

(ii) P is said to be **totally ramified** in $F/K(x)$ if there exists a unique place $P' \in \mathbb{P}(F')$ with $P'|P$ and $v_{P'}(z) = e \cdot v_P(z)$ for all $z \in F$, where $e = n$. For a general place, this integer $e(P'|P) := e$ is called the **ramification index**.

(iii) P is said to be **inert** in $F/K(x)$ if there exists a unique place $P' \in \mathbb{P}(F')$ with $P'|P$ and $\deg(P') = f \cdot \deg(P)$ with $f = n$. For a general place, this integer $f(P'|P) := f$ is called the **inertia degree**.

Now we can answer whether there is a way to introduce divisors $\mathrm{Div}(F)$ of the extension from the divisors in $\mathrm{Div}(K(x))$. To this end, we define the *conorm* of a place and of a divisor respectively.

Definition 2.2.16. Let F/K be an algebraic extension of $K(x)$. For a place $P \in \mathbb{P}(K(x))$ we define its **conorm** (with respect to $F/K(x)$) as

$$\mathrm{con}_{F/K(x)}(P) := \sum_{P'|P} e(P'|P)P',$$

where the sum runs over all places $P' \in \mathbb{P}(F)$ lying over P. The conorm map is extended to a homomorphism from the divisor group $\mathrm{Div}(K(x))$ into $\mathrm{Div}(F)$ by setting

$$\mathrm{con}_{F/K(x)}(\sum n_P P) := \sum n_P \mathrm{con}_{F/K(x)}(P).$$

The following proposition explains how we can apply the conorm on the principal divisors of the rational function field to get principal divisors of the extension.

Proposition 2.2.17. *Let $F/K(x)$ be an algebraic extension of $K(x)$. For a non-zero element $z \in F$, let $(z)^{K(x)}$ denote the principal divisor of z in $\mathrm{Div}(K(x))$, and let $(z)^F$ denote the principal divisor of z in $\mathrm{Div}(F)$. Then*

$$(z)^F = \mathrm{con}_{F/K(x)}((z)^{K(x)}).$$

We can also define the degree of a function $z \in F$. We define it as the extension degree $\deg(z) := [F : K(z)]$, which is also equal to

$$\deg(z) = \frac{1}{2} \sum_{P \in \mathbb{P}(F)} |v_P(z)| \deg(P),$$

where $v_P(z)$ is the valuation of z at a place P. We note that this is different from the degree of its principal divisor, which is always zero.

For one of the parameters of the function field lattice we further need the following invariant of a function field.

Definition 2.2.18. Let F/K be a function field. The number

$$\gamma := \min\{[F : K(z)] : z \in F\}$$

is called the **gonality**.

We note that this definition gives us the smallest degree of a transcendental $z \in F$, and this will be either 1 or 2 in most our studies.

Another important invariant of a function field is called the **genus** g of F. This positive integer roughly measures the complexity of the function field. Even though it is difficult to compute in general, we can use it in the characterisation of function fields. Further it has important consequences, such as on the number of rational places. This is known as the *Hasse-Weil* bound

$$|N_r - (q^r + 1)| \leq 2gq^{r/2},$$

where N_r is the number of rational places over F_{q^r}.

2.2.1 Automorphisms of Function Fields

In this subsection we consider the necessary background for section 5.1.

Definition 2.2.19. Let F/K be a function field. Then an **automorphism** σ of F over K is a field automorphism such that $\sigma\,|_K = \mathrm{id}$. The automorphism group of F is then the set $\mathrm{Aut}_K(F)$ of all automorphisms of F over K.

The following two lemmas are taken from [Sti09] and we present their proofs to underline the structure of automorphisms on function fields.

Lemma 2.2.20. *Let F/K be a function field and let $\sigma \in \mathrm{Aut}_K(F)$. Then σ induces a bijection on the set of places $\mathbb{P}_F$.*

Proof. Let $P \in \mathbb{P}_F$ and let $\mathcal{O}_P$ be the valuation ring of P. First we show that $\sigma(\mathcal{O}_P)$ is again a valuation ring. Assume that it is not. Then there would exist an element $y \in F$ s.t. y and y^{-1} are both not in $\sigma(\mathcal{O}_P)$. Since σ is a bijection on F there exists a $z \in F$ s.t. $\sigma(z) = y$. So by assumption neither $\sigma(z)$ nor $\sigma(z)^{-1} = \sigma(z^{-1})$ are in $\sigma(\mathcal{O}_P)$. But since $\mathcal{O}_P$ is a valuation ring, z or z^{-1} is in $\mathcal{O}_P$. W.l.o.g. assume $z \in \mathcal{O}_P$, then it follows that $\sigma(z) = y \in \mathcal{O}_P$, which is a contradiction. It follows from σ being a homomorphism that $\sigma(\mathcal{O}_P)^* = \sigma(\mathcal{O}_P^*)$ and therefore the image of a place $\sigma P = \sigma(\mathcal{O}_P \backslash \mathcal{O}_P^*)$ is again a place $\sigma(P) = \sigma(\mathcal{O}_P) \backslash \sigma(\mathcal{O}_P)^*$. Since σ is a bijection of F, it must also be a bijection on the set of places.

□

Lemma 2.2.21. *Let F/K be a function field and let $\sigma \in \mathrm{Aut}_K(F)$. Then σ preserves the degree of a place.*

Proof. The degree is $\deg(\sigma(P)) = [F_{\sigma(P)} : K]$. We know from the previous lemma that $F_{\sigma(P)} = \sigma(\mathcal{O}_P)/\sigma(P)$. Define the map $\tilde{\sigma}$ given by

$$\tilde{\sigma} : \mathcal{O}_P/P \to \sigma(\mathcal{O}_P)/\sigma(P)$$

$$z + P \mapsto \sigma(z) + \sigma(P).$$

$\tilde{\sigma}$ is a field homomorphism since σ is one. Assume $\tilde{\sigma}(z + P) = 0$ for some $z \in \mathcal{O}_P$. Then by definition

$$\tilde{\sigma}(z + P) = \sigma(z) + \sigma(P) = P = 0$$

which implies that $\sigma(z) \in \sigma(P)$. Which in turn, means that $z \in P$ and therefore $z + P = 0$ in $\mathcal{O}_P/P$. So $\tilde{\sigma}$ is injective. $\tilde{\sigma}$ being surjective follows from σ being surjective.
So $\tilde{\sigma}$ defines an isomorphism of F_P and $F_{\sigma(P)}$. Therefore $\deg(\sigma(P)) = [F_{\sigma(P)} : K] = [F_P : K] = \deg(P)$. □

These two results are important because we need to understand how the automorphisms act on certain divisors of the function field. As we will see, function field lattices are closely related to the divisors of the function field. So these results are necessary for our work in section 5.1.

2.2.2 Elliptic Function Fields

An elliptic function field over a finite field can be completely described as a function field of genus one. On the other hand, it is possible to describe them equivalently by the following proposition.

Proposition 2.2.22. *Let F/K be a function field with* $\mathrm{char}K \neq 2$. *Then F/K is an elliptic function field if and only if there exist $x, y \in F$ such that $F = K(x, y)$ and*

$$y^2 = f(x)$$

with a square-free polynomial $f(x) \in K[x]$ of degree 3.

A nice feature of the elliptic function field, is that its rational places form an abelien group. The addition in the group is defined as follows for $P, Q, R \in \mathbb{P}^1(F)$

$$\mathbf{P} \oplus \mathbf{Q} = \mathbf{R} \Longleftrightarrow P + Q \sim R + \mathcal{O}$$

where $P + Q$ and $R + \mathcal{O}$ are equivalent as divisors in $\mathrm{Div}^0(F)/\mathrm{Princ}(F)$ and $\mathcal{O}$ denotes the conorm of the place at infinity P_∞. Further this place $\mathcal{O}$ acts as the neutral element of the group.

This group structure is useful in giving a compact proof of Abel-Jacobi Theorem in terms of algebraic function field notions. This theorem is relevant for function field lattices coming from elliptic function fields, in particular for the computation of its determinant.

Theorem 2.2.23 (Abel-Jacobi)**.** *Let F/K be an elliptic function field and let*

$$D = \sum_{i=1}^{s} n_i P_i - \sum_{j=1}^{r} m_j Q_j \in \mathrm{Div}(F),$$

where the support of D is a subset of the rational places, and n_i, m_j are non-negative integers. Then, D is principal if and only if $\deg(D) = 0$ *and*

$$\sum_{i=1}^{s} [n_i] \boldsymbol{P}_i \oplus \sum_{j=1}^{r} [-m_j] \boldsymbol{Q}_j = \mathcal{O}.$$

Proof. First assume that D is a principal divisor. Then we only need to show the following condition

$$\sum_{i=1}^{s} [n_i] \mathbf{P}_i \oplus \sum_{j=1}^{r} [-m_j] \mathbf{Q}_j = \mathcal{O}$$

because every principal divisor has degree zero. We first observe that

$$[n]\mathbf{P} \sim nP - (n-1)\mathcal{O},$$

for any $n \geq 1$. Let us note that this equivalence makes sense because for any degree one divisors there exists a unique rational place which is equivalent to this

divisor. Therefore, we can easily show that for a divisor in the form of $\sum_{i=1}^{s} n_i P_i$ with positive n_i's we have the equivalence

$$[n_1]\mathbf{P}_1 \oplus \cdots \oplus [n_s]\mathbf{P}_s \sim \sum_{i=1}^{s} n_i P_i - (\sum_{i=1}^{s} n_i - s)\mathcal{O} - (s-1)\mathcal{O}.$$

Similarly, we have $[-m]\mathbf{P} \sim (m+1)\mathcal{O} - mP$ for all nonnegative interegers m. Therefore, we get the equivalence

$$[-m_1]\mathbf{Q}_1 \oplus \cdots \oplus [-m_r]\mathbf{Q}_r \sim (\sum_{j=1}^{r} m_j + r)\mathcal{O} - (r-1)\mathcal{O} - \sum_{j=1}^{r} m_j Q_j.$$

Now set $\sum_{i=1}^{s}[n_i]\mathbf{P}_i \oplus \sum_{j=1}^{r}[-m_j]\mathbf{Q}_j = R$ and suppose that $R \neq \mathcal{O}$. Then

$$\sum_{i=1}^{s}[n_i]\mathbf{P}_i + \sum_{j=1}^{r}[-m_j]\mathbf{Q}_j \sim D - (\sum_{i=1}^{s} n_i - \sum_{j=1}^{r} m_j)\mathcal{O} + 2\mathcal{O} \sim R + \mathcal{O}. \qquad (1)$$

Note that since $\deg(D) = 0$ we have $\sum_{i=1}^{s} n_i - \sum_{j=1}^{r} m_j = 0$. Therefore, $D + \mathcal{O} \sim R$ which gives a contradiction because D cannot be principal as $R \neq \mathcal{O}$.

Conversely, if we suppose that $\deg(D) = 0$ and

$$\sum_{i=1}^{s}[n_i]\mathbf{P}_i \oplus \sum_{j=1}^{r}[-m_j]\mathbf{Q}_j = \mathcal{O},$$

we obtain $D + 2\mathcal{O} \sim 2\mathcal{O}$. This shows that D is equivalent to the zero divisor and hence it is principal. □

2.2.3 Hyperelliptic Function Fields

Another example of a function field we introduce is the hyperelliptic function field. Its definition is as follows.

Definition 2.2.24. A function field F/K of genus $g \geq 2$ is called **hyperelliptic** if it contains a subfield $K(x)$ such that $[F : K(x)] = 2$.

This definition is equivalent to the following proposition.

Proposition 2.2.25. *Assume that* char$K \neq 2$.

(a) Let F/K be a hyperelliptic function field of genus g. Then there exist $x, y \in F$ such that $F = K(x, y)$ and

$$y^2 = f(x) \in K[x]$$

with a square-free polynomial $f(x)$ of degree $2g+1$ or $2g+2$.

(b) Conversely, if $F = K(x, y)$ and $y^2 = f(x) \in K[x]$ with a square-free polynomial $f(x)$ of degree $m > 4$, then F/K is hyperelliptic of genus

$$g = \begin{cases} (m-1)/2 & \text{if } m \equiv 1 \bmod 2, \\ (m-2)/2 & \text{if } m \equiv 0 \bmod 2 \end{cases}$$

We recall that every function field of genus 2 is hyperelliptic. Further, $K(x)$ is its unique rational subfield.

Remark 2.2.26. We further note that the places in $K(x)$ can go one of three ways in the extension, since by its definition $[F : K(x)] = 2$.

(i) P totally ramifies. Then there is one unique place P' which lies over P with $e(P'|P) = 2$ and $f(P'|P) = 1$, which implies that P' and P have the same degree.

(ii) P splits completely. Then there are exactly two places P'_1 and P'_2 which lie over P. Both of these places have $e(P'_1|P) = e(P'_2|P) = 1$ and $f(P'_1|P) = f(P'_2|P) = 1$.

(iii) P becomes inert. Then there is one unique place P' which lies over P with the ramification index $e(P'|P) = 1$, but with inertia degree $f(P'|P) = 2$.

Later we will see that the determinant of a function field lattice is closely related to the class number h. To this end, we consider a specific type of divisor which represent the classes in the zero class group $\mathrm{Div}^0(F)$ following [Sal06].

Definition 2.2.27. Let $F = K(x, y)$ be a hyperelliptic function field over an algebraically closed field. A degree zero divisor $D \in \mathrm{Div}^0(F)$ is called **reduced** if

1. $v_P(D) \geq 0$ for all $P \in \mathbb{P}(F) \backslash \{P_\infty\}$.
2. If $P \cap K(x)$ is ramified in F then $v_P(D) \in \{0, 1\}$.
3. If $P \cap K(x)$ splits in F such that $\mathrm{con}_{F/K(x)}(P) = P_1 + P_2$ then $v_{P_1}(D) > 0$ implies that $v_{P_2}(D) = 0$.
4. $\frac{1}{2}\deg(D) \leq g$.

Remark 2.2.28. When only the first three conditions are fulfilled then the divisor is called semi-reduced.

Note that in the above definition the inert places in F are not mentioned. This is because in the original definition K is assumed to be algebraically closed. When the base field is not algebraically closed we have that for an inert place P the valuation of any reduced divisor D is $v_P(D) = 0$.

Proposition 2.2.29. *Let D be a reduced divisor then $v_P(D) = 0$ whenever P is inert.*

Proof. Let P' be an inert place of F and P be the place such that $P = P' \cap K(x)$. We consider the divisor $P - P_\infty$, which is a principal divisor in $K(x)$. Then its conorm $P' - 2P_\infty$ is also principal. Now assume there is a divisor class $[D]$ in $\mathrm{Cl}^0(F)$ with a reduced divisor representative D such that $v_{P'}(D) > 0$, then there is an equivalent divisor $D' = D - v_{P'}(D)(P - 2P_\infty)$ with $v_P(D') = 0$. Then D' is still a reduced divisor. □

Theorem 2.2.30. *[Sal06] Let $F = K(x, y)$ be a hyperelliptic function field with Jacobian $\mathrm{Cl}^0(F)$. Then every class in $\mathrm{Cl}^0(F)$ contains a unique reduced divisor D.*

This theorem is useful in computing the determinant of hyperelliptic function field lattices in Section 4.2.

3 A Lattice Construction from Algebraic Function Fields

This section introduces the construction and structure of function field lattices. These lattices were developed by M.Y. Rosenbloom and M.A. Tsfasman [RT90], and H.-G. Quebbemann [Que89] with the motivation of constructing lattices which are asymptotically good. For consistency, we use the notation and introduction given in [Ate17]. First, in Subsection 3.1 we start with the basic definitions and properties supported by the example of a lattice constructed from the rational function field, or, as we say in short, the rational function field lattice. Later we focus on lattices constructed from elliptic, Hermitian and hyperelliptic function fields as special cases in Subsections 3.2, 3.3 and 3.4 respectively.

3.1 Basic Definitions and Properties

In this subsection, we introduce the fundamental notions of function field lattices. We present the results together with their proofs to elaborate the underlying structures of these lattices.

In the beginning of this construction, we fix a set $\mathcal{P}$ of $n+1$ distinct places of an algebraic function field $F/\mathbb{F}_q$

$$\mathcal{P} = \{P_0, \ldots, P_n\} \subset \mathbb{P}_{\mathbb{F}}.$$

The cardinality of $\mathcal{P}$ determines the number of coordinates of the lattice we construct.

Then correspondingly, we define the set $\mathcal{O}_{\mathcal{P}}^* \coloneqq \{z \in F \mid \mathrm{supp}(z) \subseteq \mathcal{P}\}$. It is easy to see that this set forms an abelian group with respect to field multiplication. For most of the lattices we consider in this thesis, $\mathcal{P}$ will consist of only rational places, but this is not necessary for the construction.

Definition 3.1.1. Given an $(n+1)$-tuple $\mathcal{P}$ of places of a function field $F/\mathbb{F}_q$, the associated function field lattice $\mathcal{L}_{\mathcal{P}}$ is defined as the image of the map

$$\begin{aligned} \Phi_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^* &\to \mathbb{R}^n \\ z &\mapsto (v_{P_0}(z) \cdot \deg(P_0), \ldots, v_{P_n}(z) \cdot \deg(P_n)). \end{aligned}$$

We note that the map $\Phi_{\mathcal{P}}$ is a group homomorphism. Indeed, for any two elements z_1, z_2 in $\mathcal{O}_{\mathcal{P}}^*$ we have $\Phi_{\mathcal{P}}(z_1 \cdot z_2) = \Phi_{\mathcal{P}}(z_1) + \Phi_{\mathcal{P}}(z_2)$. This becomes more obvious when comparing the lattice to the additive group of principal divisors with support in $\mathcal{P}$.

The following proposition lists what we know about the length of the vectors in function field lattices. These are important to later show properties like well-roundness, for example.

Proposition 3.1.2. *Let $\mathcal{P}$ and $\mathcal{O}_{\mathcal{P}^*}$ be as in Definition 3.1.1, then the following holds.*

(i) Let $z \in \mathcal{O}_{\mathcal{P}}^*$, then $||\Phi_{\mathcal{P}}(z)||^2 \equiv 0 \bmod 2$, which means $\mathcal{L}_{\mathcal{P}}$ is an even lattice.

(ii) Let $z \in \mathcal{O}_{\mathcal{P}}^*$, then $||\Phi_{\mathcal{P}}(z)|| \geq \sqrt{2\deg(z)}$. Moreover, equality holds if and only if the pole and zero of z completely split in the extension $F/\mathbb{F}_q(z)$.

(iii) The minimum distance of $\mathcal{L}_{\mathcal{P}}$ satisfies $d(\mathcal{L}_{\mathcal{P}}) \geq \sqrt{2\gamma}$, where γ is the gonality of F.

Proof. (i) Let $z \in \mathcal{O}_{\mathcal{P}}^*$ with principle divisor

$$(z) = v_{P_0}(z)P_0 + v_{P_1}(z)P_1 + \ldots + v_{P_n}(z)P_n$$

Then the squared length of the vector in $\mathcal{L}_{\mathcal{P}}$ is

$$\begin{aligned} ||\Phi_{\mathcal{P}}(z)||^2 &= v_{P_0}(z)\deg(P_0)^2 + v_{P_1}(z)\deg(P_1)^2 + \ldots + v_{P_n}(z)\deg(P_n)^2 \\ &\equiv v_{P_0}(z)\deg(P_0) + v_{P_1}(z)\deg(P_1) + \ldots + v_{P_n}(z)\deg(P_n) \bmod 2 \\ &\equiv 0 \bmod 2. \end{aligned}$$

The first equivalence follows from the fact that $m^2 \equiv m \bmod 2 \, \forall m \in \mathbb{Z}$ and the second from the fact that all principal divisors have degree 0.

(ii) For any $z \in \mathcal{O}_{\mathcal{P}}^* \setminus \mathbb{F}_q^*$, we know that $[F : K(z)]$ is finite. On the other hand, lattice vectors are described by principal divisors, more explicitly by the following representation

$$\Phi_{\mathcal{P}}(z) = (a_1 \deg(Z_1), \ldots, a_r \deg(Z_r), -b_1 \deg(P_1), \ldots, -b_s \deg(P_s))$$

where

$$(z) = a_1 Z_1 + \ldots + a_r Z_r - b_1 P_1 - \ldots - b_s P_s$$

with its zeros Z_i's and poles P_j's of z in $\mathcal{P}$. Then the square of the norm is

$$||\Phi(z)_{\mathcal{P}}||^2 = \sum_{i=1}^{r} a_i^2 \deg(Z_i)^2 + \sum_{j=1}^{s} b_j^2 \deg(P_j)^2.$$

Therefore, we easily have

$$||\Phi_{\mathcal{P}}(z)||^2 \geq \sum_{i=1}^{r} a_i \deg(Z_i) + \sum_{j=1}^{s} b_j \deg(P_j),$$

where the sum on the right hand side is exactly $2\deg(z)$.

(iii) This follows from the fact that the extension degree $[F : K(z)]$ is exactly the degree $\deg(z)$. And on the other hand, by the definition of the gonality γ, we have that $\gamma \leq \deg(z)$. Therefore, as an immediate consequence of (ii), we have the claimed lower bound on the minimal distance of a function field lattice.

□

The next proposition tells us that these lattices $\mathcal{L}_\mathcal{P}$ are all sublattices of a well-known class of lattice. It also shows that they are never full-rank.

Proposition 3.1.3. *Let $\mathcal{P}$ be a set of $n+1$ distinct places of a function field $F/\mathbb{F}_q$, then a function field lattice $\mathcal{L}_\mathcal{P}$ has rank n and is a sublattice of the root lattice $\mathcal{A}_n$.*

Proof. Let $\mathcal{P} = (P_0, P_1, ..., P_n)$ for $P_i \in \mathbb{P}_\mathbb{F}$ and let d_i denote the degree of the place P_i. Recall the definition of the root lattice given in example 2.1.2

$$\mathcal{A}_n \coloneqq \{v \in \mathbb{Z}^{n+1} \mid \sum_{i=0}^{n} v_i = 0\}.$$

Let v be a lattice vector of $\mathcal{L}_\mathcal{P}$, then by Definition 3.1.1 v is of the form

$$v = (v_{P_0}(z) \cdot d_0, \ldots, v_{P_n}(z) \cdot d_n)$$

for some $z \in \mathcal{O}_\mathcal{P}^*$. Then the sum of its entries is the degree of the principal divisor $(z)^F$. Since principal divisors have degree zero, this means that v is also in $\mathcal{A}_n$ and therefore $\mathcal{L}_\mathcal{P}$ is a subset of $\mathcal{A}_n$.

Consider the degree zero divisors $d_iP_0 - d_0P_i$ for $1 \leq i \leq n$. Let h be the class number, then the divisors $hd_iP_0 - hd_0P_i$ are principal because h is defined as the index $[\mathrm{Div}^0(F) : \mathrm{Princ}(F)]$. This gives us n linearly independent vectors in the function field lattice $\mathcal{L}_\mathcal{P}$, namely

$$\begin{gathered}(hd_1, -hd_0, 0, \ldots, 0),\\ \vdots\\ (hd_1, 0, 0, \ldots, -hd_0).\end{gathered}$$

On the one hand, since $\mathcal{L}_\mathcal{P}$ is a subset of $\mathcal{A}_n$, its rank is less or equal to $n = \mathrm{rank}(\mathcal{A}_n)$. But on the other hand since it contains n linearly independent vectors, its rank must be at least n. Therefore $\mathrm{rank}(\mathcal{L}_\mathcal{P}) = n$ and thus $\mathcal{L}_\mathcal{P}$ is a sublattice of $\mathcal{A}_n$. □

The following example elaborates on the lattice structure of the simplest function field lattice, that coming from the rational function field where $\mathcal{P}$ is comprised of only rational places.

Example 3.1.4. Let $\mathbb{F}_q(x)$ denote the rational function field . In this case, we can consider the tuple $\mathcal{P}$ to be any $n+1$ rational places in $K(x)$, i.e.

$$\mathcal{P} = (P_0, P_1, ..., P_n),$$

where $P_i \in \mathbb{P}^1_{K(x)}$ for each $i = 1, \ldots, n+1$. Therefore, by Definition 3.1.1, the function field lattice $\mathcal{L}_\mathcal{P}$ is equal to the root lattice $\mathcal{A}_n$. More explicitly, we first consider the divisors $P_i - P_{i+1}$ for $0 \leq i \leq n$. Since the class number of the rational function field is $h = 1$, these divisors are all principle, which means the n vectors of the form

$$(0, ..., 0, 1, -1, 0, ..., 0),$$

where 1 and -1 are in the i-th and $i+1$-th coordinates respectively, are all contained in $\mathcal{L}_\mathcal{P}$. As explained in Example 2.1.6, these vectors generate $\mathcal{A}_n$ and by Proposition 3.1.3 we know that $\mathcal{L}_\mathcal{P}$ is contained in $\mathcal{A}_n$. We conclude that the lattices $\mathcal{L}_\mathcal{P}$ and $\mathcal{A}_n$ are indeed equal.

For a fix $\mathcal{P}$, let $\mathrm{Div}^0_\mathcal{P}(F)$ denote the group of degree zero divisors whose support are in $\mathcal{P}$. Correspondingly, let $\mathrm{Princ}_\mathcal{P}(F)$ denote the subgroup of $\mathrm{Div}^0_\mathcal{P}(F)$, containing principal divisors with $\mathrm{supp}(D) \subseteq \mathcal{P}$. Now we provide a proof of the following proposition given in [Ate17] by elaborating their meaning in terms of divisors in $\mathrm{Div}(F)$. This notation gives an insight for the results in Subsection 4.2.

Proposition 3.1.5. *[Ate17, Proposition 2.2] Let $\mathcal{L}_\mathcal{P}$ be the function field lattice with $\mathcal{P} = (P_0, P_1, ..., P_n)$. Let d_i be the degrees of the places P_i, and let $d = \gcd(d_0, ..., d_n)$.*

(i) The index $[\mathcal{A}_n : \mathcal{L}_\mathcal{P}]$ is given by

$$[\mathcal{A}_n : \mathcal{L}_\mathcal{P}] = \frac{d_0 d_1 \cdots d_n}{d} \cdot h_0$$

where h_0 is an integer which divides the class number h.

(ii) The determinant of the function field lattice $\mathcal{L}_\mathcal{P}$ is given by

$$\det(\mathcal{L}_\mathcal{P}) = \sqrt{n+1} \cdot \frac{d_0 d_1 \cdots d_n}{d} \cdot h_0.$$

Proof. (i) We first note that the index $[\mathcal{A}_n : \mathcal{L}_\mathcal{P}]$ is finite since, by Proposition 3.1.3, $\mathcal{L}_\mathcal{P}$ is a sublattice of $\mathcal{A}_n$. Let us consider the sublattice of $\mathcal{L}_\mathcal{P}$, denoted by B, whose vectors are in one-to-one correspondence with divisors in $\mathrm{Div}^0_\mathcal{P}(F)$. Similarly, we consider a sublattice of the integer lattice $\mathbb{Z}^{n+1}$, denoted by C,

whose lattice vectors are in one-to-one correspondence with divisors D with $\mathrm{supp}(D) \subseteq \mathcal{P}$. More explicitly, we write

$$B \coloneqq \{x \in \mathbb{R}^{n+1} \mid x_i \equiv 0 \bmod d_i,\ \sum_{i=0}^{n} x_i = 0\} \subseteq \mathcal{A}_n$$
$$C \coloneqq \{x \in \mathbb{R}^{n+1} \mid x_i \equiv 0 \bmod d_i\} \subseteq \mathbb{Z}^{n+1}.$$

First, our goal is to compute the index $[\mathcal{A}_n : B]$. Note that $B = \mathcal{A}_n \cap C$, then by the second isomorphism theorem for modules we have the equality

$$[\mathcal{A}_n : B] = |\mathcal{A}_n/(\mathcal{A}_n \cap C)| = |(\mathcal{A}_n + C)/C|.$$

As modules we have that $C \subseteq (\mathcal{A}_n + C) \subseteq \mathbb{Z}^{n+1}$ which means our goal is now to compute the index $[(\mathcal{A}_n + C) : C]$ by way of computing both $[\mathbb{Z}^{n+1} : (\mathcal{A}_n + C)]$ and $[\mathbb{Z}^{n+1} : C]$. It is clear that $[\mathbb{Z}^{n+1} : C]$ is equal to the product of the degrees $d_0 d_1 \cdots d_n$.
For $[\mathbb{Z}^{n+1} : (\mathcal{A}_n + C)]$ let us define the map

$$\tau : \mathbb{Z}^{n+1} \to \mathbb{Z}/k\mathbb{Z}$$
$$x \mapsto \sum_{i=0}^{n} x_i \bmod d.$$

We now need to show that the kernel of this map is $\ker(\tau) = \mathcal{A}_n + C$. It is clear that $\mathcal{A}_n$ is contained in the kernel. Now let $x \in C$, then

$$x_i \equiv 0 \bmod d_i\ \forall i \Rightarrow x_i \equiv 0 \bmod d\ \forall i \Rightarrow \sum_{i=0}^{n} x_i \equiv 0 \bmod d$$

and therefore $x \in \ker(\tau)$ and $C \subseteq \ker(\tau)$. On the other hand, let $x \in \ker(\tau)$ i.e.

$$\sum_{i=0}^{n} x_i \equiv 0 \bmod d$$

then for some $r \in \mathbb{Z}$

$$\sum_{i=0}^{n} x_i = rd$$

and since k is the greatest common divisor of $d_0, ..., d_n$ there exist integers $s_i \in \mathbb{Z}$ such that

$$\sum_{i=0}^{n} x_i = r(s_0 d_0 + ... + s_n d_n).$$

Then we can rewrite the vector x as a sum

$$x = (x_0 - rsd_0, ..., x_n - rsd_0) + (rsd_0, ..., rsd_n)$$

Which proves that any element in the kernel is also an element of $\mathcal{A}_n + C$. Thus $\ker(\tau) = \mathcal{A}_n + C$ and since the map τ is surjective this proves that the index $[\mathbb{Z}^{n+1} : (\mathcal{A}_n + C)] = d$. Which means we now have that

$$[(\mathcal{A}_n + C) : C] = [\mathbb{Z}^{n+1} : C] : [\mathbb{Z}^{n+1} : (\mathcal{A}_n + C)] = \frac{d_0 d_1 \cdots d_n}{d}.$$

The second step is to compute the index $[B : \mathcal{L}_\mathcal{P}]$. To this end, define the map

$$\begin{aligned} \sigma : B &\to \mathrm{Div}^0(F)/\mathrm{Princ}(F) \\ x &\mapsto \sum_{i=0}^{n} \frac{x_i}{d_i} P_i + \mathrm{Princ}(F). \end{aligned}$$

Now we want to determine the kernel of this map.

$$\begin{aligned} \ker(\sigma) &= \{x \in B \mid \frac{x_0}{d_0} P_0 + ... + \frac{x_n}{d_n} P_n \in \mathrm{Princ}(F)\} \\ &= \{x \in B \mid \frac{x_0}{d_0} P_0 + ... + \frac{x_n}{d_n} P_n = (z) \in \mathcal{O}_\mathcal{P}^*\} \\ &= \mathcal{L}_\mathcal{P}. \end{aligned}$$

This implies that $B/\mathcal{L}_\mathcal{P}$ is a subgroup of the class group $\mathrm{Div}^0(F)/\mathrm{Princ}(F)$. Which leads to the fact that the index $[B : \mathcal{L}_\mathcal{P}] = h_0$ divides the class number h.

Finally we can combine all of this to give us the index

$$[\mathcal{A}_n : \mathcal{L}_\mathcal{P}] = [\mathcal{A}_n : B] \cdot [B : \mathcal{L}_\mathcal{P}] = \frac{d_0 d_1 \cdots d_n}{d} \cdot h_0.$$

(ii) By proposition 3.1.3 $\mathcal{L}_\mathcal{P}$ is a sublattice of $\mathcal{A}_n$. As we have already seen in example 2.1.9 we can then use that

$$\det(\mathcal{L}_\mathcal{P}) = \det(\mathcal{A}_n) \cdot [\mathcal{A}_n : \mathcal{L}_\mathcal{P}].$$

Since we have just proven in part (i) of this proposition what the index $[\mathcal{A}_n : \mathcal{L}_\mathcal{P}]$ is, we conclude

$$\det(\mathcal{L}_\mathcal{P}) = \sqrt{n+1} \cdot \frac{d_0 d_1 \cdots d_n}{d} \cdot h_0.$$

□

This proposition makes it clear that in almost all cases the only difficulty in calculating the determinant is finding h_0. From the proof it become clear that h_0 is equal to the index

$$h_0 = [\mathrm{Div}^0_{\mathcal{P}}(F) : \mathrm{Princ}_{\mathcal{P}}(F)],$$

which is the group of zero divisors with support on $\mathcal{P}$ over the group of principal divisors with support on $\mathcal{P}$.

Remark 3.1.6. While we compute the determinant using the index h_0, in Rosen's number theory in function fields [Ros13], the opposite is done, i.e. h_0 is computed using the determinant of the lattice. This provides a number theoretical proof for the formula for the determinant in Proposition 3.1.5. Indeed, [Ros13, Lemma 14.3] states that

$$h_0 = \frac{d \cdot R_S}{d_0 d_1 \cdots d_n}$$

where R_S is a minor of the basis matrix B of the lattice. By applying Cauchy-Binet, we see that $\sqrt{n+1} \cdot R_S = \sqrt{\det(BB^T)}$ and therefore we again get

$$\sqrt{\det(BB^T)} = \sqrt{n+1} \cdot \frac{d_0 d_1 \cdots d_n}{d} \cdot h_0.$$

3.2 Elliptic Function Field Lattices

In this subsection we present the literature by following the structure in Subsection 2.1. We mainly follow [FM14] and [Sha15] and the references therein. The former shows the well-roundness property of elliptic function field lattice and the latter expands on this work by showing that elliptic function field lattices have a basis of minimal vectors considering mainly the group structure of elliptic curves.

Throughout this Subsection we will take $\mathcal{P}$ to be the set of all rational places of $E/\mathbb{F}_q$, i.e. $\mathcal{P} = \mathbb{P}^1_E$ and interchangeably for the points on the corresponding elliptic curves. More explicitly, for a point $\mathbf{P}$ on an elliptic curve E, we denote its corresponding rational place in the elliptic function field E by P. Recall that the rational places of an elliptic function field form a group. In general, this group is isomorphic to the group

$$\mathcal{P} = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

where n_1 and n_2 are positive integers such that $n_1 | n_2$ and $n_1 \cdot n_2 = n + 1$. In the special case that this group is cyclic we obtain a lattice we have already introduced in example 2.1.2, namely the Barnes lattice.

Lemma 3.2.1. *[Sha15] When $\mathcal{P}$ is cyclic then the elliptic function field lattice $\mathcal{L}_{\mathcal{P}}$ is equal to the Barnes lattice $\mathcal{B}_n$.*

Proof. Assume $\mathcal{P}$ is a cyclic group isomorphic to $\mathbb{Z}/(n+1)\mathbb{Z}$, with

$$\mathcal{P} = (\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_n)$$

where $\mathbf{P}_0 = \mathcal{O}$ and without loss of generality, $\mathbf{P}_i = [i]\mathbf{P}_1$ for $1 \leq i \leq n$, where $[i]\mathbf{P}$ denotes the summation of $\mathbf{P}$ i many times. Then by the Abel-Jacobi Theorem 2.2.23, a divisor of the form

$$D = \sum_{i=0}^{n} x_i P_i$$

is principal if and only if it has degree zero and

$$\sum_{i=0}^{n} [x_i]\mathbf{P}_i = \sum_{i=0}^{n} [ix_i]\mathbf{P}_1 = \mathcal{O}.$$

Recall that we have a one to one correspondence of principal divisors with support on $\mathcal{P}$ and lattice vectors. Therefore, when translated to the lattice $\mathcal{L}_\mathcal{P}$, these two conditions become equivalent to the fact that a vector $(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}$ is contained in the lattice $\mathcal{L}_\mathcal{P}$ if and only if

$$\sum_{i=0}^{n} x_i = 0 \text{ and } \sum_{i=0}^{n} ix_i \equiv 0 \bmod (n+1).$$

This is equivalent to the definition of the Barnes lattice in example 2.1.2 and thus proves our claim. □

There are multiple ways to compute the determinant of lattices from elliptic function fields. We provide an alternative proof using the Abel-Jacobi Theorem 2.2.23. Recall that we already show the determinant of the Barnes lattice in example 2.1.9. This is a special case of an elliptic function field lattice, as shown in Lemma 3.2.1. However, the next proposition gives us the determinant of a general lattice from an elliptic function field. We elaborate this result by providing a proof following the structure of Proposition 3.1.5.

Proposition 3.2.2. *Let $\mathcal{L}_\mathcal{P}$ be an elliptic function field lattice with $|\mathcal{P}| = n+1 \geq 2$ then we have* $\det(\mathcal{L}_\mathcal{P}) = (n+1)^{\frac{3}{2}}$.

Proof. By Example 2.1.9 we know that $\det(\mathcal{A}_n) = (n+1)^{\frac{1}{2}}$ and we claim that $[\mathcal{A}_n : \mathcal{L}_\mathcal{P}] = n+1$. From this it directly follows that

$$\det(\mathcal{L}_\mathcal{P}) = \det(\mathcal{A}_n) \cdot [\mathcal{A}_n : \mathcal{L}_\mathcal{P}] = (n+1)^{\frac{3}{2}}.$$

All that is left is to prove is the claim. Consider the group homomorphism

$$\sigma : \mathcal{A}_n \to \mathrm{Div}^0(E)/\mathrm{Princ}(E)$$
$$(x_0, x_1, \ldots, x_n) \mapsto x_0P_0 + \ldots + x_nP_n + \mathrm{Princ}(E).$$

The kernel of σ satisfies

$$\begin{aligned}\mathrm{Ker}(\sigma) &= \{(x_0, \ldots, x_n) \in \mathcal{A}_n : x_0P_0 + \ldots + x_nP_n + \mathrm{Princ}(E)\} \\ &= \{(x_0, \ldots, x_n) \in \mathcal{A}_n : x_0P_0 + \ldots + x_nP_n = (z) \in \mathcal{O}_{\mathcal{P}}^*\} \\ &= \mathcal{L}_{\mathcal{P}}.\end{aligned}$$

By the First Isomorphism Theorem we have $\mathcal{A}_n/\mathcal{L}_{\mathcal{P}} \cong \mathrm{Im}(\sigma)$. The next step is to show that $|\mathrm{Im}(\sigma)| = n + 1$.
Let $(x_0, \ldots, x_n) \in \mathcal{A}_n \backslash \mathrm{Ker}(\sigma)$. Since $(x_0, \ldots, x_n)$ is not in the kernel, it is not a vector in the lattice $\mathcal{L}_{\mathcal{P}}$. By Theorem 2.2.23 this means that

$$\sum_{i=0}^{n} [x_i]\mathbf{P}_i \neq \mathcal{O}.$$

By the group structure of $\mathcal{P}$ there exists an element $\mathbf{R} \in \mathcal{P} \backslash \mathcal{O}$ s.t.

$$\sum_{i=0}^{n} [x_i]\mathbf{P}_i = \mathbf{R}.$$

And so as divisors we have the following equivalence in $\mathrm{Div}^0(E)/\mathrm{Princ}(E)$

$$\sum_{i=0}^{n} x_iP_i \sim R - \mathcal{O}.$$

This shows that every element in the image of σ is equivalent to a divisor of this form. On the other hand, for any element $\mathbf{P}_i \in \mathcal{P} \backslash \{\mathcal{O}\}$ we can construct the vector $(-1, 0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the i-th coordinate and -1 in the first coordinate in the lattice $\mathcal{A}_n$, corresponding to the divisors $P_i - \mathcal{O}$. Then the image of this vector under σ is not in the kernel since

$$\mathbf{P}_i - \mathcal{O} \neq \mathcal{O}.$$

In this way we naturally construct a bijection between $\mathrm{Im}(\sigma)$ and $\mathcal{P}$. Thus it follows that

$$[\mathcal{A}_n : \mathcal{L}_{\mathcal{P}}] = |\mathrm{Im}(\sigma)| = |\mathcal{P}| = n + 1.$$

□

We end this subsection by presenting the three following results on the minimum distance, minimal vectors and kissing number, respectively, omitting their proofs.

Proposition 3.2.3. *[FM14] Let $n+1 \geq 4$, then the minimum distance of $\mathcal{L}_{\mathcal{P}}$ is $d(\mathcal{L}_{\mathcal{P}}) = 2$ and the minimal vectors all correspond to principle divisors of the form $P+Q-R-S$, where P, Q, R and S are distinct places in $\mathcal{P}$.*

Proposition 3.2.4. *[Sha15] For $n+1 \geq 5$ the elliptic function field lattice $\mathcal{L}_{\mathcal{P}}$ has a basis of minimal vectors.*

Proposition 3.2.5. *[FM14] The kissing number of $\mathcal{L}_{\mathcal{P}}$ is*

$$\kappa(\mathcal{L}_{\mathcal{P}}) = \frac{n}{\epsilon} \cdot \frac{(n-\epsilon)(n-\epsilon-2)}{4} + (n - \frac{n}{\epsilon}) \cdot \frac{n(n-2)}{4}$$

where ϵ is the number of 2-torsion rational points in E.

3.3 Hermitian Function Field Lattices

In this section we briefly touch on lattices from Hermitian function fields. We first give a quick definition of the function field and then go over the basic properties of the Hermitian function field lattice. As before, we follow [Ate17] and for more on these lattices we refer to [Böt+16].

Definition 3.3.1. The Hermitian function field over $\mathbb{F}_{q^2}$ can be defined by

$$H := \mathbb{F}_{q^2}(x, y) \quad \text{with} \quad y^q + y = x^{q+1}.$$

It has the following properties:

(i) The genus of H is $g = q(q-1)/2$.

(ii) H has $q^3 + 1$ places of degree one over $\mathbb{F}_{q^2}$.

Proposition 3.3.2. *Let $H/\mathbb{F}_{q^2}$ be a Hermitian function field and $\mathcal{P}$ be the set of its rational places. Then the function field lattices $\mathcal{L}_{\mathcal{P}}$ has the following properties.*

(i) The determinant of $\mathcal{L}_{\mathcal{P}}$ is $\det(\mathcal{L}_{\mathcal{P}}) = \sqrt{q^3+1}(q+1)^{q^2-q}$.

(ii) The minimal distance of $\mathcal{L}_{\mathcal{P}}$ is $d(\mathcal{L}_{\mathcal{P}}) = \sqrt{2q}$.

(iii) The kissing number of $\mathcal{L}_{\mathcal{P}}$ satisfies $\kappa(\mathcal{L}_{\mathcal{P}}) = q^7 - q^5 + q^4 - q^2$.

(iv) The lattice $\mathcal{L}_{\mathcal{P}}$ has a basis of minimal vectors.

3.4 Hyperelliptic Function Field Lattices

Throughout this subsection let F be a hyperelliptic function field. More explicitly, let $F = \mathbb{F}_q(x, u)$ with defining equation

$$u^2 = f(x),$$

where $f(x)$ is a square free polynomial. In this subsection we only consider hyperelliptic function fields where the pole of x ramifies in F, hence the degree of $f(x)$ is $\deg(f(x)) = 2g + 1$, where g is the genus of F.

Let us go over our choice of $\mathcal{P}$ for these function field lattice. Recall from Remark 2.2.26 that each place can behave one of three ways in the extension. In particular this means that a degree one place will either ramify and still be degree one, split into two degree one places, or become inert of degree two. With this in mind, instead of simply choosing all the rational places of F we work almost exclusively with the following set of places for $\mathcal{P}$.

$$\mathcal{P} = (P_\infty, P_2, \ldots, P_r, Q_1, \ldots, Q_s),$$

where P_∞ denotes the pole of x, and $P_2, \ldots, P_r$ denote all of the other rational places which are ramified in F, and $Q_1, \ldots, Q_s$ denote all inert places of degree 2. In hyperelliptic function fields, the ramified places correspond one to one to all of the roots of the defining polynomial $f(x)$, which means the number of ramified places of degree one in F is $1 \leq r \leq 2g + 2$.

Our goal is to understand the generating vectors of the lattice $\mathcal{L}_\mathcal{P}$. We do this by understanding the generating elements of the ring $\mathcal{O}_\mathcal{P}^*$ first. To this end, let us define $\alpha_i, \beta_j \in \mathbb{F}_q$ for $2 \leq i \leq r$, $1 \leq j \leq s$ such that $(x - \alpha_i)$ and $(x - \beta_j)$ are prime elements of P_i and Q_j respectively.

Lemma 3.4.1. *The group $\mathcal{O}_\mathcal{P}^*$ can be described as follows:*

(i) In case $\mathrm{char}(F) = 2$ *or in case* $\mathrm{char}(F) \neq 2$ *and $f(x)$ does not split into linear factors,*

$$\mathcal{O}_\mathcal{P}^* = \{\delta \cdot \prod_{i=2}^{r} (x - \alpha_i)^{a_i} \prod_{j=1}^{s} (x - \beta_j)^{b_j} \mid \delta \in \mathbb{F}_q^*,\ a_i, b_j \in \mathbb{Z}\}.$$

(ii) In case $\mathrm{char}(F) \neq 2$ *and $f(x)$ splits into linear factors,*

$$\mathcal{O}_\mathcal{P}^* = \{\delta \cdot u^\mu \cdot \prod_{i=2}^{r} (x - \alpha_i)^{a_i} \prod_{j=1}^{s} (x - \beta_j)^{b_j} \mid \delta \in \mathbb{F}_q^*,\ \mu \in \{0, 1\},\ a_i, b_j \in \mathbb{Z}\},$$

This makes it clear which elements generate the group $\mathcal{O}_{\mathcal{P}}^*$. We mainly distinguish between two cases, where either $f(x)$ splits into linear factors or it does not. The reason we make this distinction is the following. In both cases we have the generating elements $x-\alpha_i$ and $x-\beta_j$ whose principal divisors are $(x-\alpha_i)^F = 2P_i - 2P_\infty$ and $(x-\beta_j)^F = Q_j - 2P_\infty$. But in the case where $f(x)$ splits into linear factors the principal divisor of u from the defining equation

$$u^2 = f(x)$$

has support on $\mathcal{P}$ and so is an element of $\mathcal{O}_{\mathcal{P}}^*$. The principal divisor of u is then given by

$$(u)^F = -(2g+1)P_\infty + P_2 + \ldots + P_{2g+2},$$

which cannot be generated by the elements $x-\alpha_i$ and $x-\beta_j$.

The immediate consequence of this lemma is the following.

Corollary 3.4.2. *The hyperelliptic function field lattice $\mathcal{L}_{\mathcal{P}}$ can be generated as follows.*

(i) In case $\mathrm{char}(F) = 2$ *or in case* $\mathrm{char}(F) \neq 2$ *and $f(x)$ does not split into linear factors,*

$$\mathcal{L}_{\mathcal{P}} = \langle \{ \Phi_{\mathcal{P}}(x-\alpha_i), \Phi_{\mathcal{P}}(x-\beta_j) \mid 2 \leq i \leq r,\ 1 \leq j \leq s \} \rangle.$$

(ii) In case $\mathrm{char}(F) \neq 2$ *and $f(x)$ splits into linear factors,*

$$\mathcal{L}_{\mathcal{P}} = \langle \{ \Phi_{\mathcal{P}}(x-\alpha_i), \Phi_{\mathcal{P}}(x-\beta_j) \mid 2 \leq i \leq r,\ 1 \leq j \leq s \} \cup \{ \Phi_{\mathcal{P}}(u) \} \rangle.$$

By this representation, the following main result on hyperelliptic function lattices is obtained in [Ate17].

Theorem 3.4.3. *Assume $g \geq 3$ then the following hold:*

(i) The minimum distance of $\mathcal{L}_{\mathcal{P}}$ is $d(\mathcal{L}_{\mathcal{P}}) = \sqrt{8}$ and the vectors of the form

$$\Phi_{\mathcal{P}}(x-\alpha_i), \Phi_{\mathcal{P}}(x-\beta_j) \ \text{ for } \ 2 \leq i \leq r,\ 1 \leq j \leq s$$

are minimal vectors.

(ii) The lattice $\mathcal{L}_{\mathcal{P}}$ is well-rounded.

All the algebraic function field lattices shown so far are well-rounded. The following case shows that well-roundness is not a universal property of function field lattices.

Theorem 3.4.4. *Suppose $\mathcal{P}$ contains all the extensions of at least two rational places of $\mathbb{F}_q(x)$ which split in the extension F. Then the hyperelliptic function field lattice $\mathcal{L}_\mathcal{P}$ is not well-rounded.*

In particular Theorem 3.4.4 shows that in most cases, if $\mathcal{P}$ is chosen to be the set of rational places in F, then the resulting hyperelliptic function field lattice is not well-rounded.

4 Successive Minima and Determinant of Hyperelliptic Function Field Lattices

In the previous subsection we see that not all hyperelliptic function field lattices are well-rounded. This leads us to investigate the successive minima of that type of hyperelliptic function field lattice in Subsection 4.1. In addition to this, we note that because of the difficulty of computing h_0, Proposition 3.1.5 does not explicitly allow us to compute the determinant. Motivated by this, we consider how to compute h_0 for hyperelliptic function field lattices in Subsection 4.2.

4.1 Successive Minima

In Subsection 3.4 we restrict ourselves to very specific hyperelliptic function field lattices. On the one hand we focus on a specific subset of places for $\mathcal{P}$. On the other hand Subsection 3.4 only considers well-roundness for these lattices. Here we expand on what can be said about hyperelliptic function field lattices.

First let us exhaust all possibilities for when we choose $\mathcal{P}$ like in Section 3.4. The following theorem goes over all cases and lists whether they are well-rounded or have stronger properties in each. We note that some of these stronger results were not mentioned in [Ate17], so we provide them here.

Theorem 4.1.1. *Let $F/\mathbb{F}_q(x)$ be a hyperelliptic function field with defining equation $u^2 = f(x)$ where $f(x)$ is a square-free polynomial of degree $2g+1$. Further, let $\mathcal{P}$ be the set of rational ramified places and inert places of degree 2, i.e.*

$$\mathcal{P} = \{P_\infty, P_2, \ldots, P_r, Q_1, \ldots, Q_s\}.$$

Then the following hold:

(i) If $\mathrm{char}(F) = 2$ then $\mathcal{L}_\mathcal{P}$ has a basis of minimal vectors.

(ii) If $\mathrm{char}(F) \neq 2$ and $f(x)$ does not split into linear factors then $\mathcal{L}_\mathcal{P}$ has a basis of minimal vectors.

(iii) If $\mathrm{char}(F) \neq 2$, $f(x)$ splits into linear factors and the genus is $g = 3$ then $\mathcal{L}_\mathcal{P}$ has a basis of minimal vectors.

(iv) If $\mathrm{char}(F) \neq 2$, $f(x)$ splits into linear factors and the genus is $g > 3$ then $\mathcal{L}_\mathcal{P}$ is well-rounded.

(v) If $\mathrm{char}(F) \neq 2$, $f(x)$ splits into linear factors and the genus is $g = 2$ then $\mathcal{L}_\mathcal{P}$ is not well-rounded.

Proof. By Theorem 3.4.3 well-roundness was already shown for cases $(i) - (iv)$.

Now let us elaborate the cases (i) and (ii). By Corollary 3.4.2 the vectors $\Phi_{\mathcal{P}}(x-\alpha_i), \Phi_{\mathcal{P}}(x-\beta_j)$ for $2 \leq i \leq r$, $1 \leq j \leq s$ generate the lattice and by Theorem 3.4.3 they are minimal vectors. Since there are exactly $r+s-1$ of these vectors, which is the rank of the lattice $\mathcal{L}_{\mathcal{P}}$, these vectors form a basis of minimal vectors.

To show (iii), suppose the polynomial $f(x)$ splits and hence u is an element in $\mathcal{O}_{\mathcal{P}}^*$. By Corollary 3.4.2 the vectors $\Phi_{\mathcal{P}}(x-\alpha_i), \Phi_{\mathcal{P}}(x-\beta_j)$ for $2 \leq i \leq 2g+2$, $1 \leq j \leq s$ and $\Phi_{\mathcal{P}}(u)$ generate the lattice. Consider the vector

$$\begin{aligned} v^* &= \Phi_{\mathcal{P}}(u) - \Phi_{\mathcal{P}}(x-\alpha_2) - \ldots - \Phi_{\mathcal{P}}(x-\alpha_{g+1}) \\ &= (-1,-1,\ldots,-1,1,\ldots,1,0,\ldots,0) \end{aligned}$$

where the first $g+1$ coordinates are -1 and the next $g+1$ coordinates are 1 and the last s are 0. This vector has length $||v^*|| = \sqrt{2g+2} = \sqrt{8}$, since the genus is $g=3$, and so is also a minimal vector. Now consider the set of $2g+1+s$ vectors

$$\{v^*, \Phi_{\mathcal{P}}(x-\alpha_2), \ldots, \Phi_{\mathcal{P}}(x-\alpha_{2g+1}), \Phi_{\mathcal{P}}(x-\beta_1), \ldots, \Phi_{\mathcal{P}}(x-\beta_s)\}.$$

These vectors are all minimal and the rank of the lattice is $2g+1+s$. Furthermore, they generate both $\Phi_{\mathcal{P}}(u)$ and $\Phi_{\mathcal{P}}(x-\alpha_{2g+2})$ as follows:

$$\begin{aligned} \Phi_{\mathcal{P}}(u) &= v^* + \Phi_{\mathcal{P}}(x-\alpha_2) + \ldots + \Phi_{\mathcal{P}}(x-\alpha_{g+1}) \\ \Phi_{\mathcal{P}}(x-\alpha_{2g+2}) &= 2\cdot v^* + \Phi_{\mathcal{P}}(x-\alpha_2) + \ldots + \Phi_{\mathcal{P}}(x-\alpha_{g+1}) \\ &\quad - \Phi_{\mathcal{P}}(x-\alpha_{g+2}) - \ldots - \Phi_{\mathcal{P}}(x-\alpha_{2g+1}). \end{aligned}$$

This implies that these vectors generate the whole lattice. Therefore this forms a basis of minimal vectors of $\mathcal{L}_{\mathcal{P}}$.

Lastly, we show the last point (v). First we prove that the minimum distance of $\mathcal{L}_{\mathcal{P}}$ in this case, is $d(\mathcal{L}_{\mathcal{P}}) = \lambda_1(\mathcal{L}_{\mathcal{P}}) = \sqrt{6}$. Recall that by Proposition 3.1.2 all function field lattices are even, which means for all $z \in \mathcal{O}_{\mathcal{P}}^*$ that $||\Phi_{\mathcal{P}}(z)|| = \sqrt{2t}$ for some integer $t \geq 1$. Assume there exists a z in $\mathcal{O}_{\mathcal{P}}^*$ s.t. $||\Phi_{\mathcal{P}}(z)|| < \sqrt{6}$. We go through these cases to show that this cannot be.
If $||\Phi_{\mathcal{P}}(z)|| = \sqrt{2}$ then w.l.o.g. the vector has the form

$$\pm(0,\ldots,0,1,-1,0,\ldots,0).$$

Then z has degree 1 and the extension degree $F/\mathbb{F}_q(z)$ is $[F:\mathbb{F}_q(z)] = 1$ which implies F is the rational function field and this cannot be.
If $||\Phi_{\mathcal{P}}(z)|| = \sqrt{4}$ then w.l.o.g. the vector has the form

$$\pm(0,\ldots,0,1,1,-1,-1,0,\ldots,0).$$

Then z has degree 2 and $[F : \mathbb{F}_q(z)] = 2$. Since $\mathbb{F}_q(x)$ is the unique rational subfield of degree 2 this means that $\mathbb{F}_q(x) = \mathbb{F}_q(z)$. If either the pole or zero of z splits in F then z cannot be an element of $\mathcal{O}_{\mathcal{P}}^*$ because of the way we define $\mathcal{P}$. This means the pole and zero of z are ramified or inert, in which case $\Phi_{\mathcal{P}}(z)$ must be of the form

$$\pm(0, \ldots, 0, 2, -2, 0, \ldots, 0).$$

By the same argument we can rule out any z such that the vector $\Phi_{\mathcal{P}}(z)$ has length $\sqrt{6}$ and is of the form

$$\pm(0, \ldots, 0, 2, -1, -1, 0, \ldots, 0),$$

since then z would also have degree 2.

Now consider the five vectors generated by $\Phi_{\mathcal{P}}(u)$ and $\Phi_{\mathcal{P}}(x - \alpha_i)$ for $2 \leq i \leq 6$.

$$\begin{aligned}
&(1, 1, 1, -1, -1, -1, 0, \ldots, 0),\\
&(1, 1, -1, 1, -1, -1, 0, \ldots, 0),\\
&(1, -1, 1, 1, -1, -1, 0, \ldots, 0),\\
&(-1, 1, 1, 1, -1, -1, 0, \ldots, 0),\\
&(-1, -1, 1, 1, 1, -1, 0, \ldots, 0),
\end{aligned}$$

One can check that these vectors are linearly independent and all have length $\sqrt{6}$. We need to show that there are no more vectors of length $\sqrt{6}$ which are linearly independent to these. Recall that each place Q_j for $1 \leq j \leq s$ in $\mathcal{P}$ is inert of degree 2. This means the $(6 + j)$-th entry of any vector v in $\mathcal{L}_{\mathcal{P}}$ will be a multiple of two. Since we already ruled out all z with $\Phi_{\mathcal{P}}(z)$ of length $\sqrt{6}$ with an entry equal to ± 2, this means any such element z would have support on only the ramified places in $\mathcal{P}$. Since we are restricted to six coordinates and have to fulfill that the sum of the entries is zero it stands that there could be at most five linearly independent vectors, which satisfy this. This implies that there are only at most five linearly independent minimal vectors in $\mathcal{L}_{\mathcal{P}}$, hence the lattice is not well-rounded.

□

Thus far we have not discussed the successive minima of function field lattices much, since when a lattice is well-rounded then all its successive minima are simply equal to the minimum distance. But as seen in Theorem 4.1.1 we have a specific case where it would be interesting to determine the successive minima. The following lemma delves into this.

Lemma 4.1.2. *Let $\mathcal{P}$ be as in Theorem 4.1.1. Assume* $\mathrm{char}(F) \neq 2$*, $f(x)$ splits into linear factors and the genus is $g = 2$, then the successive minima of $\mathcal{L}_{\mathcal{P}}$ are*

$$\lambda_1(\mathcal{L}_{\mathcal{P}}) = \ldots = \lambda_5(\mathcal{L}_{\mathcal{P}}) = \sqrt{6},$$
$$\lambda_6(\mathcal{L}_{\mathcal{P}}) = \ldots = \lambda_{6+s-1}(\mathcal{L}_{\mathcal{P}}) = \sqrt{8}.$$

Proof. We note that the proof of part (v) of Theorem 4.1.1 shows that the first five successive minima are

$$\lambda_1(\mathcal{L}_{\mathcal{P}}) = \ldots = \lambda_5(\mathcal{L}_{\mathcal{P}}) = \sqrt{6}.$$

The last step is simple. Again, because the lattice is even, the next shortest possible length of a lattice vector after $\sqrt{6}$ is $\sqrt{8}$. We provide the last s vectors in the lattice $\mathcal{L}_{\mathcal{P}}$ which are linearly independent to the five we already showed in the proof of part (v) of Theorem 4.1.1. These are the vectors $\Phi_{\mathcal{P}}(x - \beta_j)$ for $1 \leq j \leq s$, or more explicitly,

$$\begin{array}{cccccccccc}
(-2, & 0, & 0, & 0, & 0, & 0, & 2, & 0, & \ldots, & 0), \\
(-2, & 0, & 0, & 0, & 0, & 0, & 0, & 2, & \ldots, & 0), \\
 & & & & \vdots & & & & & \\
(-2, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & \ldots, & 2).
\end{array}$$

These all have length $\sqrt{8}$ and are clearly linearly independent to the first minimal vectors and to each other. Therefore the last s successive minima are

$$\lambda_6(\mathcal{L}_{\mathcal{P}}) = \ldots = \lambda_{6+s-1}(\mathcal{L}_{\mathcal{P}}) = \sqrt{8}.$$

□

Now that we have thoroughly discussed the cases where $\mathcal{P}$ is made up of ramified and inert places, let us try to understand what happens when $\mathcal{P}$ contains only the rational places of F and the genus is $g \geq 3$. As we mention in Theorem 3.4.4, when $\mathcal{P}$ contains all extensions of at least two rational places which split then the lattice is not well-rounded. So, naturally we are interested in what the shortest vectors in these lattices look like. To this end, we first fix some notation. Let

$$\mathcal{P} = (P_1, P_2, \ldots, P_r, S_{11}, S_{12}, S_{21}, S_{22} \ldots, S_{t1}, S_{t2}),$$

where P_i for $1 \leq i \leq r$, as before, represent the rational ramified places, and S_{j1}, S_{j2} for $1 \leq j \leq t$ represent the two extensions of a rational place S_j in $\mathbb{F}_q(x)$ which splits completely in F. The resulting lattice $\mathcal{L}_{\mathcal{P}}$ then has rank $r + 2t - 1$.

By Proposition 3.1.2 the minimum distance satisfies $d(\mathcal{L}_{\mathcal{P}}) = 2$. In [Ate17] it is detailed that the vectors that reach this minimum are those which are associated to principal divisors of the form

$$S_{i1} + S_{i2} - S_{j1} - S_{j2},$$

for $1 \leq i \neq j \leq t$. There are at most $t-1$ linearly independent vectors of this form in the lattice $\mathcal{L}_{\mathcal{P}}$.

These vectors all have length 2 which means the next shortest vectors would have length $\sqrt{6}$. The only principal divisors whose associated vectors have length $\sqrt{6}$ are of the from

$$\pm(2P_i - S_{j1} - S_{j2}),$$

for $1 \leq i \leq r$ and $1 \leq j \leq t$. We can choose r of these vectors which are linearly independent to the first $t-1$.

Now we are missing t vectors to reach the rank of the lattice. Notice how in each case so far the two extensions S_{j1}, S_{j2} of a splitting place S_j always appear together, with the same valuation. This can be explained with the following fact.

Lemma 4.1.3. *[Ate17, Propopsition 4.4.11] Let $F/\mathbb{F}_q$ be a hyperelliptic function field with genus g and let $z \in \mathcal{O}_{\mathcal{P}}^*$. If the length of the vector $||\Phi_{\mathcal{P}}(z)||$ satisfies*

$$||\Phi_{\mathcal{P}}(z)|| < \sqrt{2g+2}$$

then z belongs to $\mathbb{F}_q(x)$.

In particular this lemma implies that any element in $\mathcal{O}_{\mathcal{P}}^*$ which is not in the base field, is mapped to a vector in the lattice with length greater or equal to $\sqrt{2g+2}$. Remember that the conorm of the place S_j is $\mathrm{con}_{F/K(x)}(S_j) = S_{j1} + S_{j2}$. This means that elements in the base field $z \in \mathbb{F}_q(x)$, which by the above lemma are those with shorter length, will satisfy $v_{S_{j1}}(z) = v_{S_{j2}}(z)$.

It seems that the vectors which are linearly independent to the shortest, that we have already discussed, are those with unequal valuation at the places S_{j1} and S_{j2} for $1 \leq j \leq t$. Hence these vectors are not in the base field and then by the above lemma have length greater or equal to $\sqrt{2g+2}$.

To summarize, we end this subsection with the following conjecture on the successive minima of $\mathcal{L}_{\mathcal{P}}$.

$$\begin{cases} \lambda_i(\mathcal{L}_{\mathcal{P}}) = 2, & \text{for } 1 \leq i \leq t-1 \\ \lambda_i(\mathcal{L}_{\mathcal{P}}) = \sqrt{6}, & \text{for } t \leq i \leq t+r \\ \lambda_i(\mathcal{L}_{\mathcal{P}}) \geq \sqrt{2g+2}, & \text{for } t+r \leq i \leq 2t+r-1. \end{cases}$$

4.2 Determinant of Hyperelliptic Function Field Lattices

Recall that the determinant of a function field lattice is described in Proposition 3.1.5 as depending on the number h_0, which divides the class number h. Therefore, our focus is on determining h_0, which, as discussed, is the number of the classes h_0 in $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}_{\mathcal{P}}(F)$.

For the rational and elliptic function field lattices, we could easily determine h_0, but this is not as simple in the hyperelliptic case. In this section we go over the cases of hyperelliptic function fields where we were able to determine h_0.

Recall that Theorem 2.2.30 lets us count the classes of the Jacobian $\mathbb{J}$ by counting the possible reduced divisors. In general this would be very difficult, but we can restrict our search significantly by only considering divisors with support on $\mathcal{P}$, since we need the number of classes in $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}_{\mathcal{P}}(F)$. In our case, $\mathcal{P}$ consists of only ramified and inert places. This makes the counting process much simpler since inert places do not appear at all and ramified places appear with multiplicity at most one in any reduced divisor.

The most important thing now to check is whether every such reduced divisor represents a class in $\mathrm{Div}^0(\mathcal{P})/\mathrm{Princ}(\mathcal{P})$ and vice versa. If so, then we can determine h_0.

Lemma 4.2.1. *Let $\mathcal{P}$ be the set of r rational ramified places and s inert places of degree 2. Then each class in $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}_{\mathcal{P}}(F)$ contains a semi-reduced divisor of the form*

$$D = \sum_{i=1}^{r-1} a_i P_i - (\sum_{i=1}^{r-1} a_i) P_\infty$$

for $a_i \in \{0, 1\}$.

Proof. Let $[D]$ be a divisor class in $\mathrm{Div}^0_{\mathcal{P}}(F)$. Then by Proposition 2.2.29 there is a principal divisor $D_1 \in \mathrm{Princ}_{\mathcal{P}}(F)$ such that $D - D_1$ does not have support on any of the inert places in $\mathcal{P}$.

Similarly, we know that the divisor $2P_i - 2P_\infty$ in F is principal because it is the conorm of $P_i - P_\infty$ in K. Then for $1 \leq i \leq r-1$ let $a_i = v_{P_i}(D) \in \mathbb{Z}$. This means the divisor

$$D_2 = \sum_{i=1}^{r-1} \lfloor \frac{a_i}{2} \rfloor (2P_i - 2P_\infty)$$

is principal and $D - D_1 - D_2$ is of the desired form. Since D_1 and D_2 are principal, the class $[D] \in \mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}_{\mathcal{P}}(F)$ is equal to the class $[D - D_1 - D_2]$. Further, this divisor is semi-reduced since it only has support on ramified places where the valuation is either 1 or 0. This completes the proof. □

This is the first step in counting the different classes. The important thing to check is whether any of these semi-reduced or reduced divisors are equivalent to each other in $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}_{\mathcal{P}}(F)$. This is addressed in the proof of the following theorem.

Theorem 4.2.2. *Let $F = K(x, y)$ be a hyperelliptic function field with defining equation $y^2 = f(x)$ for a square free polynomial of degree $\deg(f(x)) = 2g + 1$. Let $\mathcal{P} = (P_\infty, P_2, \ldots, P_r, Q_1, \ldots Q_s)$ where P_i are all ramified places of degree 1 and Q_j are all inert places of degree 2. The determinant of the function field lattice $\mathcal{L}_{\mathcal{P}}$ is $\det(\mathcal{L}_{\mathcal{P}}) = \sqrt{n+1} \cdot 2^s \cdot h_0$ where h_0 is given by*

$$\begin{cases} h_0 = 2^{r-1} & \text{when } f(x) \text{ does not split into linear factors ,} \\ h_0 = 2^{2g} & \text{when } f(x) \text{ splits into linear factors} \end{cases}$$

Proof. By Lemma 4.2.1 we know that each class in $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}_{\mathcal{P}}(F)$ contains a semi reduced divisor of the form

$$D = \sum_{i=1}^{r-1} a_i P_i - (\sum_{i=1}^{r-1} a_i) P_\infty \tag{2}$$

for $a_i \in \{0, 1\}$.

Since there only two options for each a_i, this means there are 2^{r-1} different divisors of this form. First let us assume that $f(x)$ does not split into linear factors. Let D be one of these 2^{r-1} divisors. If D is a reduced divisor then by Theorem 2.2.30 any two reduced divisors are in distinct classes in $\mathrm{Div}^0(F)/\mathrm{Princ}(F)$. Since $\mathrm{Princ}_{\mathcal{P}}(F)$ lies in $\mathrm{Princ}(F)$, they must also be in distinct classes in the quotient group $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}_{\mathcal{P}}(F)$.
This shows that two reduced divisors are in distinct classes. Next we show the same for one reduced and one semi-reduced divisor. Now let D be only semi-reduced i.e. $\frac{1}{2}\deg(D) > g$. Because this divisor is already semi-reduced it is not difficult to find the equivalent reduced divisor. Let $(u)^F$ be the principal divisor of u in F

$$(u)^F = P_1 + ... + P_{r-1} + R_1 + ... + R_t - (2g+1)P_\infty$$

where $R_1, ...R_t$ are the non-rational ramified places of F with $t \geq 1$. Then the divisor $\tilde{D} = -(D - (u)^F)$ is reduced because it has

$$\frac{1}{2}(\deg(-D + (y))) = \frac{1}{2}(2g + 1 - \deg(D)) \leq g$$

and only has support on ramified places with valuation either 0 or 1. Since $(u)^F$ is principal, $\tilde{D}$ is in the same equivalence class as D in $\mathrm{Div}^0(F)/\mathrm{Prin}(F)$. This

reduced divisor is not equal to any of the reduced divisors given in Equation 2, which means that D is also in its distinct class. It follows that all 2^{r-1} divisors given in Equation 2 are in distinct classes.
Now finally assume that $f(x)$ splits into linear factors. Then similarly to before, the reduced divisors are all in distinct classes. However, now the principal divisor $(u)^F$ is an element in $\mathrm{Princ}_{\mathcal{P}}(F)$ since all ramified places are rational and therefore in $\mathcal{P}$. This means, by the same argument as before, that for any semi-reduced divisor given in Equation 2 there is an equivalent reduced divisor given in Equation 2. Therefore the number of distinct classes is equal to the number of reduced divisors with support on $\mathcal{P}$, of which there are

$$\sum_{i=0}^{g} \binom{2g+1}{i} = 2^{2g}$$

□

Remark 4.2.3. In the case where the polynomial $f(x)$ does not split into linear factors, we prove in Lemma 5.6.1 that the function field lattice is equal to $\mathcal{L}_{\mathcal{P}} = 2 \cdot \mathcal{A}_n$. This means we can easily confirm our result in Theorem 4.2.2, since the determinant is then

$$\begin{aligned} \det(\mathcal{L}_{\mathcal{P}}) &= \det(2 \cdot \mathcal{A}_n) \\ &= 2^n \det(\mathcal{A}_n) = 2^n \sqrt{n+1} \\ &= 2^{r-1} 2^s \sqrt{n+1}. \end{aligned}$$

Until now we have restricted ourselves to the case where $\mathcal{P}$ only contains the ramified places of degree one and the inert places of degree 2. Here we present one result on the case where $\mathcal{P}$ is chosen to be the set of all rational places.

Theorem 4.2.4. *Let F/K be a hyperelliptic function field over $\mathbb{F}_q$ with genus g and let h denote the class number. Take $\mathcal{P}$ to be the set of all rational places of F, i.e. $\mathcal{P} = \mathbb{P}_F^1$. If q and g satisfy*

$$\sqrt{q} + \frac{1}{\sqrt{q}} > 2 \cdot (2g-1)$$

then the determinant of the function field lattice $\mathcal{L}_{\mathcal{P}}$ is equal to

$$\det(\mathcal{L}_{\mathcal{P}}) = h\sqrt{n+1}.$$

To prove this theorem we first need the following result [Hes04, Theorem 34]. Let $N_d(F/K)$ denote the number of places of degree one in the constant field extension of F/K of degree d.

Theorem 4.2.5. *Let D_0 be a divisor of degree one in F/K and $d \in \mathbb{N}$ such that $N_d(F/K) > (g-1)2q^{\frac{d}{2}}$. Denote by $P_1, ..., P_r$ all places of degree dividing d and set $D_i = P_i - \deg(P_i)D_0$. Then $\deg(D_i) = 0$ and the classes $[D_i]$ generate $\mathrm{Cl}^0(F/K)$.*

Again, the idea here is to understand the group $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}^0_{\mathcal{P}}(F)$ and the order of its elements to determine h_0, when $\mathcal{P} = \mathbb{P}^1_F$. Using the theorem above lets us understand under what conditions $\mathrm{Cl}^0(F/K)$ is generated by places of degree one. This tells us when h_0 is equal to the class number h.

Proof of Theorem 4.2.4. We only consider the case where the place at infinity is ramified in F/K so we can choose P_∞ as our divisor D_0. Next recall by Hasse-Weil Theorem we have $\mid N_d(F/K) - (q^d - 1) \mid \leq 2gq^{\frac{d}{2}}$. If we take $d = 1$ and use this bound it becomes clear when we fulfill the necessary condition

$$N_d(F/K) \geq (q+1) - 2g\sqrt{q} > (g-1)2\sqrt{q}$$

$$q + 1 > (2g-1)2\sqrt{q}$$

$$\sqrt{q} + \frac{1}{\sqrt{q}} > 2(2g-1)$$

This means that when g and q satisfy the above inequality, then by Theorem 4.2.5 the divisor classes $[P - P_\infty]$ for $P \in \mathbb{P}^1_F$ generate $\mathrm{Cl}^0(F/K)$. This implies that every divisor class in $\mathrm{Cl}^0(F/K)$ has a representative with support on $\mathcal{P} = \mathbb{P}^1_F$. And hence, $\mathrm{Div}^0_{\mathcal{P}}(F)/\mathrm{Princ}^0_{\mathcal{P}}(F) = \mathrm{Cl}^0(F/K)$. Therefore $h_0 = h$ and the determinant of the function field lattice is $\det(\mathcal{L}_{\mathcal{P}}) = h\sqrt{n+1}$.

□

5 Automorphism Groups of Function Field Lattices

In this section we explore the automorphism groups of some function field lattices and their subgroups. In particular we want to understand how the automorphisms of the function field and the associated lattice are related, if at all. In Subsection 5.1 we first analyze how we can connect the automorphisms of a general function field, to those of the associated function field lattice. The explicit automorphism groups of specific function fields are discussed in the following subsections, when we tackle each respective case separately. We focus on the rational, elliptic, Hermitian, and hyperelliptic function fields.

5.1 General Algebraic Function Field Lattices

Let us recall the construction of a function field lattice given in Section 3.1. The constructed lattice is isomorphic to the group of principal divisors of F with support on $\mathcal{P}$.

In this section we explain how we map over automorphisms of the function field F/K to automorphisms of the function field lattice $\mathcal{L}_{\mathcal{P}}$. In order for the induced map to be well-defined, we need it to be invariant on $\mathcal{O}_{\mathcal{P}}^*$. Otherwise we could not define what the map does with a given lattice vector. This means that the automorphism $\sigma \in \mathrm{Aut}_K(F)$ must be invariant on the set of places $\mathcal{P}$. In most of the cases we consider in this chapter $\mathcal{P} = \mathbb{P}_F^1$, which guarantees that any automorphism will be invariant on $\mathcal{P}$.

At the same time, we are not interested in automorphisms which act trivially on the lattice. More explicitly, these are maps which are identity on $\mathcal{P}$. To this end we define the following subset.

Definition 5.1.1. Let F/K be a function field and let $\mathcal{P}$ be a finite subset of $\mathbb{P}_F$. Then define $\mathrm{Inv}(\mathcal{P})$ to be the subgroup of all automorphisms of F/K which are identity on $\mathcal{P}$.

When $\mathcal{P}$ is the set of all places of a fixed degree then $\mathrm{Inv}(\mathcal{P})$ is a normal subgroup of $\mathrm{Aut}_K(F)$. We briefly explain why. Let $\mathcal{P}$ be all the places of degree $d \in \mathbb{N}$. Let $\sigma \in \mathrm{Inv}(\mathcal{P})$ and $\tilde{\sigma} \in \mathrm{Aut}_K(F)$. As stated in Lemmas 2.2.20 and 2.2.21 an automorphism acts as a bijection on the places of a given degree. This means that the map $\tilde{\sigma}\sigma\tilde{\sigma}^{-1}$ will permute the places of degree d and then permute them back. Hence it is again an element of $\mathrm{Inv}(\mathcal{P})$.

Under the assumption that $\mathcal{P}$ is the set of places of a fixed degree, we define the following map:

$$\Psi_{\mathcal{P}} : \mathrm{Aut}_K(F)/\mathrm{Inv}(\mathcal{P}) \to \mathrm{Aut}(\mathcal{L}_{\mathcal{P}}),$$
$$[\sigma] \mapsto \Big(\Phi_{\mathcal{P}}(z) \mapsto \Phi_{\mathcal{P}}(\sigma(z))\Big).$$

Theorem 5.1.2. *Let F/K be a function field over a finite field $\mathbb{F}_q$. Let $\mathcal{P} = \mathbb{P}^1_F$. Then the map $\Psi_{\mathcal{P}}$ is an injective group homomorphism.*

Proof. First of all, the next five steps show that $\Psi_{\mathcal{P}}([\sigma])$ is, in fact, an automorphism of the lattice $\mathcal{L}_{\mathcal{P}}$.

First, we show that if $\Phi_{\mathcal{P}}(z)$ is a lattice vector then $\Phi_{\mathcal{P}}(\sigma(z))$ is again in the lattice. Let $z \in \mathcal{O}^*_{\mathcal{P}}$. We showed in Lemmas 2.2.20 and 2.2.21 that σ permutes the places of a given degree. The divisor of z has support on places of degree 1, since $\mathcal{P} = \mathbb{P}^1_F$. Therefore the divisor of $\sigma(z)$ will also have support on places of degree one. This means $\sigma(z) \in \mathcal{O}^*_{\mathcal{P}}$ and therefore $\Phi_{\mathcal{P}}(\sigma(z))$ is a lattice vector.

Recall that the function $\Phi_{\mathcal{P}}$ in Definition 3.1.1 is not injective. So next, we show that $(\Phi_{\mathcal{P}}(z) \mapsto \Phi_{\mathcal{P}}(\sigma(z))$ is well-defined. Let $[\sigma] \in \mathrm{Aut}_K(F)/\mathrm{Inv}(\mathcal{P})$ and let z_1 and z_2 be functions in $\mathcal{O}^*_{\mathcal{P}}$ s.t. $\Phi_{\mathcal{P}}(z_1) = \Phi_{\mathcal{P}}(z_2)$. Then by our definition of $\Phi_{\mathcal{P}}$, z_1 and z_2 have the same principal divisor which means they differ at most by a constant in $\mathbb{F}^*_q$. By its definition, σ is the identity on constants of the function field, hence $\Phi_{\mathcal{P}}(\sigma(z_1)) = \Phi_{\mathcal{P}}(\sigma(z_2))$.

As an automorphism of a lattice, $\Psi_{\mathcal{P}}([\sigma])$ should be an isometry, so in particular we need to show that $\Psi_{\mathcal{P}}([\sigma])$ is a linear map. To show this, let $\Phi_{\mathcal{P}}(z_1)$ and $\Phi_{\mathcal{P}}(z_2)$ be vectors in the lattice and let $a \in \mathbb{Z}$. One can show using the definition of $\Psi_{\mathcal{P}}$ and the fact that $\Phi_{\mathcal{P}}$ and σ are homomorphisms that

$$\Psi_{\mathcal{P}}([\sigma])(\Phi_{\mathcal{P}}(z_1)) + \Psi_{\mathcal{P}}([\sigma])(\Phi_{\mathcal{P}}(z_2)) = \Psi_{\mathcal{P}}([\sigma])(\Phi_{\mathcal{P}}(z_1) + \Phi_{\mathcal{P}}(z_2))$$

and

$$a \cdot \Psi_{\mathcal{P}}([\sigma])(\Phi_{\mathcal{P}}(z)) = \Psi_{\mathcal{P}}([\sigma])(a \cdot \Phi_{\mathcal{P}}(z)).$$

Using a basis of the lattice and the vector which is orthogonal to this basis, we can extend the map $\Psi_{\mathcal{P}}([\sigma])$ to a linear map of $\mathbb{R}^n$. Each basis vector of the lattice is sent to its image under $\Psi_{\mathcal{P}}([\sigma])$ and the last vector is mapped to itself.

$\Psi_{\mathcal{P}}([\sigma])$ should be bijective. We have shown that σ is invariant on $\mathcal{O}^*_{\mathcal{P}}$ since $\mathcal{P} = \mathbb{P}^1_F$. We also note that the preimage of $\mathcal{O}^*_{\mathcal{P}}$ under σ is contained in $\mathcal{O}^*_{\mathcal{P}}$. Since σ is a bijection on F it is therefore a bijection when restricted to $\mathcal{O}^*_{\mathcal{P}}$. Surjectivity of $\Psi_{\mathcal{P}}([\sigma])$ follows from the surjectivity of $\Phi_{\mathcal{P}}$ and σ. Next, to prove injectivity,

$\Phi_{\mathcal{P}}(\sigma(z_1)) = \Phi_{\mathcal{P}}(\sigma(z_2))$ implies that $\sigma(z_1)$ and $\sigma(z_2)$ differ by a constant. Since σ is an automorphism, $\sigma(z_1)$ and $\sigma(z_2)$ differ by a constant if z_1 and z_2 differ by a constant. It follows that $\Phi_{\mathcal{P}}(z_1) = \Phi_{\mathcal{P}}(z_2)$.

$\Psi_{\mathcal{P}}([\sigma])$ should be length preserving. Let $z \in \mathcal{O}_{\mathcal{P}}^*$ then we need to show that $\|\Phi_{\mathcal{P}}(z)\| = \|\Phi_{\mathcal{P}}(\sigma(z))\|$. Recall that $\Phi_{\mathcal{P}}(z) = (v_{P_0}(z), \ldots, v_{P_{n-1}}(z))$ and so

$$\begin{aligned}\|\Phi_{\mathcal{P}}(\sigma(z))\|^2 &= \sum_{i=0}^{n} v_{P_i}(\sigma(z))^2 \\ &= \sum_{i=0}^{n} v_{\sigma^{-1}(P_i)}(z)^2 \\ &= \sum_{i=0}^{n} v_{P_i}(z)^2,\end{aligned}$$

where the second equality follows $v_P(\sigma(z)) = v_{\sigma^{-1}(P)}(z)$ for an automorphism σ and the last one follows that σ defines a permutation on $\mathcal{P}$. We conclude that $\|\Phi_{\mathcal{P}}(\sigma(z))\| = \|\Phi_{\mathcal{P}}(z)\|$.

So far, we have shown that $\Psi_{\mathcal{P}}([\sigma])$ is an automorphism of $\mathcal{L}_{\mathcal{P}}$.

We next show that $\Psi_{\mathcal{P}}$ is well-defined. Note that it is sufficient to show that it is a group homomorphism which maps the identity to the identity. To this end let $[\sigma_1]$ and $[\sigma_2]$ be in $\mathrm{Aut}_K(F)/\mathrm{Inv}(\mathcal{P})$. By the definition of $\Psi_{\mathcal{P}}$ we can show

$$\begin{aligned}(\Psi_{\mathcal{P}}([\sigma_2]) \circ \Psi_{\mathcal{P}}([\sigma_1]))(\Phi(z)) &= \Psi_{\mathcal{P}}([\sigma_2])(\Phi_{\mathcal{P}}(\sigma_1(z))) \\ &= \Phi_{\mathcal{P}}(\sigma_2(\sigma_1(z))) \\ &= \Phi_{\mathcal{P}}(\sigma_2 \circ \sigma_1(z)) = \Psi_{\mathcal{P}}([\sigma_2 \circ \sigma_1])(\Phi_{\mathcal{P}}(z)).\end{aligned}$$

Let $\sigma \in \mathrm{Inv}(\mathcal{P})$ and let $z \in \mathcal{O}_{\mathcal{P}}^*$. Then z only has support on $\mathcal{P}$ and by definition σ is the identity on all places in $\mathcal{P}$ and constants. This implies $\sigma(z) = z$ and therefore $\Phi_{\mathcal{P}}(\sigma(z)) = \Phi_{\mathcal{P}}(z)$. Therefore $\Psi_{\mathcal{P}}([\sigma])$ is the identity on the lattice $\mathcal{L}_{\mathcal{P}}$.

Lastly, we need to show that $\Psi_{\mathcal{P}}$ is injective. Let $[\sigma] \in \mathrm{Aut}_K(F)/\mathrm{Inv}(\mathcal{P})$ such that $\Psi_{\mathcal{P}}([\sigma]) = \mathrm{id}_{\mathcal{L}_{\mathcal{P}}}$. Then necessarily, σ is the identity on all places in $\mathcal{P}$. Assume it is not, then there would exist $0 \leq i, j \leq n$ with $i \neq j$, such that $\sigma(P_i) = P_j$. Then let h be the class number of F/K. Now the divisor $D = h \cdot (P_i - P_j)$ is principal. By abuse of notation $\Phi_{\mathcal{P}}(D)$ is a lattice vector and

$$\begin{aligned}\Psi_{\mathcal{P}}([\sigma])(\Phi_{\mathcal{P}}(D)) &= \Phi_{\mathcal{P}}(\sigma(D)) \\ &= \Phi_{\mathcal{P}}(h \cdot (P_j - \sigma(P_j))) \\ &\neq \Phi_{\mathcal{P}}(D)\end{aligned}$$

This contradicts that $\Psi_{\mathcal{P}}([\sigma])$ is the identity on the lattice. Therefore $\sigma \in \mathrm{Inv}(\mathcal{P})$ and $[\sigma] = [\mathrm{id}_F]$.

□

Remark 5.1.3. For all lattices, and so in particular also for function field lattices, the map which multiplies all vectors by -1 is an automorphism.
For a function field lattice, multiplying all vectors by -1 is like sending the underlying function $z \in F$ to its inverse z^{-1} since this negates the valuations at any place

$$v_P(z^{-1}) = -v_P(z).$$

But the map $z \mapsto z^{-1}$ is not an automorphism of the function field, since it is not a field homomorphism. This does mean however that the automorphism group of a function field and that of the derived lattice can never be isomorphic, if neither is trivial. In particular it means that the images under our map $\Psi_{\mathcal{P}}$ will always have an index of at least 2.

Adding onto this, the existence of the subgroup $\mathrm{Inv}(\mathcal{P})$ implies that there are often automorphism of the function field, which do not define automorphisms on the lattice. So the two automorphism groups are often not subgroups of each other. This is why, in the next section, we are motivated to observe them separately and then study their connection to each other.

5.2 Rational Function Field Lattices

Recall that the automorphism group of the rational function field is the set of maps of the form of Möbius transformations, that is, $x \mapsto \frac{ax+b}{cx+d}$, where $ad - bc \neq 0$. It is well-known that this group, more explicitly, is the projective linear group

$$\mathrm{Aut}(K(x)/K) \simeq \mathrm{PGL}_2(K).$$

In this chapter, we claim that the automorphism group of the rational function field is a proper subgroup of that of the lattice, denoted by $\mathrm{Aut}(\mathcal{A}_n)$. To this end, we first analyze $\mathrm{Aut}(\mathcal{A}_n)$ separately and then apply what we consider in subsection 5.1. The following lemma in [Mar13] is the first step in our analysis. For the sake of completeness we also include its proof here.

Lemma 5.2.1. *For $n \geq 2$, $\mathrm{Aut}(\mathcal{A}_n)$ is isomorphic to $\{\pm\mathrm{Id}\} \times S_{n+1}$. Here, S_{n+1} denotes the permutation group given by permutations of the $n+1$ coordinates in $\mathbb{R}^{n+1}$ and $\{\pm\mathrm{Id}\}$ denotes the identity matrix and its additive inverse.*

Proof. We first note that $\mathcal{A}_n$ is the intersection

$$\mathcal{A}_n = \mathbb{Z}^{n+1} \cap H,$$

where $\mathbb{Z}^{n+1}$ stands for the integer lattice and,

$$H = \{x \in \mathbb{R}^{n+1} | \sum_{i=1}^{n+1} x_i = 0\},$$

for the hyperplane. It is trivial that every element $\sigma \in \{\pm \mathrm{Id}\} \times S_{n+1}$ is a bijection on both $\mathbb{Z}^{n+1}$ and H, and is length preserving. Therefore, σ can be interpreted as an element in the automorphism group of their intersection, namely $\mathcal{A}_n$.
Conversely, any automorphism of $\mathcal{A}_n$ has, by its definition, a unique extension to an isometry of $\mathbb{R}^{n+1}$ which stabilizes

$$H^{\perp} = \langle \{\mathbf{1}\} \rangle,$$

where $\mathbf{1} \in \mathbb{R}^{n+1}$ is the vector whose entries are all 1. This isometry, denoted by $\tilde{\sigma}$, preserves $S(\mathcal{A}_n)$ or in other words, every vector of the form $e_i - e_j$ for $1 \leq i, j \leq n+1$ is sent to $\tilde{\sigma}(e_i - e_j) = e_k - e_l$ for some $1 \leq k, l \leq n+1$, where e_i are the standard basis vectors. It can be shown, using this and the fact that $\tilde{\sigma}(\sum_{i=1}^{n+1} e_i) = \sum_{i=1}^{n+1} e_i$, that $\tilde{\sigma}$ preserves $S(\mathbb{Z}^{n+1})$. Therefore this isometry defines an automorphism of $\mathbb{Z}^{n+1}$ and we get

$$\mathrm{Aut}(\mathcal{A}_n) \subseteq \mathrm{Aut}(\mathbb{Z}^{n+1}).$$

It is immediate to see that flipping the sign of some, but not all, coordinates of a vector does not preserve the hyperplane H. Therefore the only maps in $\mathrm{Aut}(\mathbb{Z}^{n+1})$ which restrict to automorphisms of A_n are $\{\pm \mathrm{Id}\} \times S_{n+1}$.

□

Now we can discuss how the automorphism groups of the rational function field and the rational function field lattice are connected. The next theorem shows that they are indeed subgroups of one another. This is a nicer version of the result in the previous subsection, Theorem 5.1.2.

Theorem 5.2.2. *Let K(x)/K be the rational function field. When $\mathcal{P} = \mathbb{P}_F^1$ is the set of all rational places, then we have $\mathcal{L}_{\mathcal{P}} = \mathcal{A}_n$ where $|\mathcal{P}| = n + 1$ and*

$$\mathrm{Aut}(K(x)) \subset \mathrm{Aut}(\mathcal{A}_n).$$

Proof. By Theorem 5.1.2 we know that $\mathrm{Aut}(K(x))/\mathrm{Inv}(\mathcal{P})$ is a subgroup of $\mathrm{Aut}(\mathcal{A}_n)$, which means that the only thing left to show here is that the subgroup $\mathrm{Inv}(\mathcal{P})$ is trivial.
Let $\sigma \in \mathrm{Inv}(\mathcal{P})$ where σ is given by $\sigma(x) = \frac{ax+b}{cx+d}$ with $a, b, c, d \in K$ and $ad - bc \neq 0$. Since σ is the identity on all rational places it must, in particular, send x to an element in $K(x)$ which also has the divisor $P_x - P_\infty$. Since $\sigma(x) = \frac{ax+b}{cx+d}$ we can immediately conclude that c and b equal 0. Then we are left with $\sigma(x) = \frac{a}{d}x$ and since $\frac{a}{d}$ is a constant this map is equivalent to $\sigma(x) = x$. Therefore σ is the identity map and $\mathrm{Inv}(\mathcal{P})$ is trivial.

□

5.3 Lattices from Finite Abelian Groups

To understand the automorphisms of elliptic, hyperelliptic and Hermitian function field lattices we need the following construction given in [Böt+15].

Definition 5.3.1. Let G be an abelian group and $S = \{g_0 = 0, g_1, ...g_n\}$ a subset of G. Then we define the lattice $\mathcal{L}_G(S)$ by

$$\mathcal{L}_G(S) \coloneqq \left\{ (x_0, ..., x_n) \in \mathcal{A}_n \mid \sum_{i=0}^{n} x_i g_i = 0 \right\}.$$

For these types of lattices there are some useful results. We can induce automorphisms of the lattice from automorphisms of the underlying group or set which gives the lattice its structure. This means we can use the automorphism groups of finite abelian groups, for which more is known. We will mainly use the following two lemmas.

Lemma 5.3.2. *Let G be a finite abelian group and let S be a subgroup of G. Then*

$$\mathrm{Aut}(S) \cong \mathrm{Aut}(\mathcal{L}_G(S)) \cap S_n.$$

In more general cases S is not a subgroup. Then we need to consider the set of permutations on S, which extend to automorphisms of the whole group G. Let us denote this set by $\mathrm{Aut}(G, S)$. This is a subgroup of $\mathrm{Aut}(G)$.

Lemma 5.3.3. *Let G be a finite abelian group and S a subset of G. Then* $\mathrm{Aut}(G, S)$ *is a subgroup of* $\mathrm{Aut}(\mathcal{L}_G(S)) \cap S_n$.
Moreover, if S is a generating set of G then $\mathrm{Aut}(G, S) \cong \mathrm{Aut}(\mathcal{L}_G(S)) \cap S_n$.

5.4 Elliptic Function Field Lattices

In Subsection 5.2 the automorphism group of the rational function field lattice is completely determined. However, finding all possible automorphisms of a lattice is not an easy task, in general. For this reason, we focus on finding large subgroups of the automorphism group instead. To find such large subgroups there are two main approaches. The first possible approach is the following. Since all function field lattices are sublattices of $\mathcal{A}_n$, we look for a subgroup of $\mathrm{Aut}(\mathcal{A}_n)$ which stabilize a sublattice $\mathcal{L}$. This is done in [Mar13] when studying the Barnes lattice $\mathcal{B}_n$. This means looking at which permutations in S_{n+1} still stabilize the lattice.

A different approach is taken in [Böt+15] on lattices generated by finite Abelian groups as explained in Subsection 5.3. Recall that it considers that these lattices have rank n and therefore focus on subgroups of S_n instead. As we see in this section, elliptic function field lattices fall under this category of lattice.

Function field lattices are always of size $n+1$ and rank n. The basic difference in thought between these two approaches is whether one thinks of these automorphisms as permutations of the coordinates of the lattice vectors or as permutations of the basis vectors.

We use a little from both of these approaches to, hopefully, paint a more complete picture of the automorphism group of these lattices.

Let us first examine the automorphisms of elliptic function fields themselves. We closely follow the results of this paper [MX20] for this.

Theorem 5.4.1. *Let E be an elliptic function field over $\mathbb{F}_q$. Let $\mathrm{Aut}(E, \mathcal{O})$ be the subgroup of automorphisms over $\mathbb{F}_q$ which stabilize the place at infinity $\mathcal{O}$ and let T_E be the translation group of E. Then the automorphism group of E is given by*

$$\mathrm{Aut}(E) = T_E \rtimes \mathrm{Aut}(E, \mathcal{O}).$$

Naturally, T_E has the structure of the group of rational places of the elliptic function field, where each place Q induces an automorphism $\tau_Q(P) = P \oplus Q$. The subgroup $\mathrm{Aut}(E, \mathcal{O})$ on the other hand, is a subgroup of the automorphisms of the elliptic curve and can have at most 24 elements.

In this case, $\mathrm{Inv}(\mathcal{P})$ is trivial since all of these maps affect the rational places of E. However, these automorphisms do not encompass the full automorphism group of these lattices. For this, we are better off approaching the lattices directly.

Let $\mathcal{P} = \{P_0, P_1, ..., P_n\}$ be the set of rational places of E where $P_0 = \mathcal{O}$ is the place at infinity. We recall that the set of rational places in an elliptic function field forms a group. Then, as stated in the beginning of this chapter, lattices from elliptic function fields are special cases of lattices generated by abelian groups. They can equivallently be defined by

$$\mathcal{L}_{\mathcal{P}} = \left\{ x \in \mathcal{A}_n \mid \sum_{i=0}^{n} [x_i]\mathbf{P}_i = \mathcal{O} \right\},$$

where $\mathbf{P}_i$ denotes the corresponding point of the rational place P_i.

Now we can apply Lemma 5.3.2 to our lattices from elliptic function fields.

Theorem 5.4.2. *Let $\mathcal{P}$ be the group of rational places of an elliptic function field E. Let $\mathcal{L}_{\mathcal{P}}$ denote the lattice from $\mathcal{O}^*_{\mathcal{P}}$. Then*

$$\mathrm{Aut}(\mathcal{L}_{\mathcal{P}}) \cap S_n \cong \mathrm{Aut}(\mathcal{P}).$$

Recall that the group of rational places is isomorphic to the group $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ where $n_1 | n_2$ and $n_1 \cdot n_2 = n + 1$.

The automorphism groups of abelian groups have been studied in [HR07]. Here, we give a short note on how this applies to $\mathrm{Aut}(\mathcal{P})$ in the following remark.

Remark 5.4.3. When the group $\mathcal{P}$ is cyclic, i.e. $\mathcal{P} \cong \mathbb{Z}/(n+1)\mathbb{Z}$, then the number of automorphisms is simply $\varphi(n+1)$, where φ is the Euler Totient function.

When the group is not cyclic, we use the fact that for two groups G and H with relatively prime order we have $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$. Thus we reduce this problem to the case $\mathcal{P} \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \mathbb{Z}/p^{e_2}\mathbb{Z}$ where p is prime and $e_1 \leq e_2$. We have two cases, the order of the automorphism group $\mathrm{Aut}(\mathbb{Z}/p^{e_1}\mathbb{Z} \times \mathbb{Z}/p^{e_2}\mathbb{Z})$ is

$$\begin{cases} \varphi(p^{e_1})^2 \cdot p^{2e_1-1} \cdot (p+1) & \text{for } e_1 = e_2, \\ \varphi(p^{e_1}) \cdot \varphi(p^{e_2}) \cdot p^{2e_1-1} \cdot p & \text{for } e_1 \neq e_2 \end{cases}$$

Note that all these automorphisms coming from $\mathrm{Aut}(\mathcal{P})$ fix the place at infinity and so fix the first coordinate of the lattice vectors. This is because the automorphism of a group fixes the neutral element and this is why we intersect the automorphism group $\mathrm{Aut}(\mathcal{L}_\mathcal{P})$ with S_n instead of S_{n+1}. However, this limits the types of maps we might consider for the automorphism group. What is missing, is the group of translations T_E which, as we discussed in the beginning of this section, are also automorphisms of the elliptic function field. Recall that this subgroup is isomorphic to the group of rational places $\mathcal{P}$.

Lemma 5.4.4. *Let $\mathcal{L}_\mathcal{P}$ be an elliptic function field lattice with $\mathcal{P} = \mathbb{P}_E^{(1)}$. Then the automorphism group $\mathrm{Aut}(\mathcal{L}_\mathcal{P})$ has a subgroup isomorphic to*

$$\{\pm \mathrm{Id}\} \times (\mathcal{P} \rtimes \mathrm{Aut}(\mathcal{P})),$$

where $\rtimes$ denotes the semi-direct product of two groups.

Proof. We know that by Theorem 5.4.2 that $\mathrm{Aut}(\mathcal{P})$ is a subgroup of $\mathrm{Aut}(\mathcal{L}_\mathcal{P})$. By Theorem 5.4.1 and Theorem 5.1.2 we map over the group of translations T_E, which is isomorphic to $\mathcal{P}$, to the automorphism group of the lattice. This implies that $\mathcal{P}$ is also a subgroup of $\mathrm{Aut}(\mathcal{L}_\mathcal{P})$. It is easy to see that the intersection of these two subgroups is only the identity, since all other elements from $\mathcal{P} \cong T_E$ shift the coordinate of the lattice associated to $\mathcal{O}$ and all elements in $\mathrm{Aut}(\mathcal{P})$ fix it.

Now we claim that $\mathcal{P}$ is normal in the product $\mathcal{P} \cdot \mathrm{Aut}(\mathcal{P})$. Let $P, Q, R \in \mathcal{P}$ and $\sigma \in \mathrm{Aut}(\mathcal{P})$ so that $\tau_Q \circ \sigma$ is an element in the group $\mathcal{P} \cdot \mathrm{Aut}(\mathcal{P})$ and τ_P is an element in $\mathcal{P} \cong T_E$. Then

$$\begin{aligned} (\sigma^{-1} \circ \tau_{-Q}) \circ \tau_P \circ (\tau_Q \circ \sigma)(R) &= \sigma^{-1}(\sigma(R) + Q + P - Q) \\ &= \sigma^{-1}(\sigma(R) + P) \\ &= R + \sigma^{-1}(P) \\ &= \tau_{\sigma^{-1}(P)}(R). \end{aligned}$$

This proves that the product of these two subgroups is isomorphic to their semidirect product. Hence $\mathcal{P} \rtimes \mathrm{Aut}(\mathcal{P})$ is isomorphic to a subgroup of $\mathrm{Aut}(\mathcal{L}_\mathcal{P})$. □

To the best of our knowledge this gives us a quite large subgroup of the automorphism group of elliptic function field lattices. It is difficult to say how much larger the full group could be. However, in the specific case where $\mathcal{P}$ is cyclic, we can determine the full automorphism group. Indeed, when $\mathcal{P}$ is cyclic then this lattice is the Barnes lattice introduced in Example 2.1.2. In [Mar13] it has been proven that for $n \geq 11$ the subgroup in Lemma 5.4.4 is the full automorphism group of the lattice and has order $2 \cdot (n+1) \cdot \varphi(n+1)$ where φ is the Euler Totient function.

Remark 5.4.5. In this section we almost treat the automorphism group of the Barnes lattice $\mathcal{B}_n$, like a subgroup of that of the root lattice $\mathcal{A}_n$. However, in some dimensions $\mathcal{B}_n$ has automorphism which $\mathcal{A}_n$ does not have, i.e. it has more than those we have shown so far. This is also explained in [Mar13], that we can use the dual of the lattice to perhaps find more automorphism of the lattice. We hint at this in subsection 2.1.3. This can be seen by Remark 2.1.26 and Lemma 2.1.33. By [Mar13, Theorem 5.3.7.] for $6 \leq n \leq 10$ the dual of the Barnes lattice $\mathcal{B}_n^*$ has more vectors of length $d(\mathcal{A}_n^*)$ than $\mathcal{A}_n^*$ does.

5.5 Hermitian Function Field Lattices

In this section we closely follow the results in [Böt+16]. Hermitian function field lattices are also lattices from finite abelian groups. In this case the group G is the zero class group $\mathrm{Cl}^0(F)$ and S is the set of divisor classes

$$S = \big\{[P_i - P_\infty] \mid 0 \leq i \leq n\big\},$$

where the places $P_0 = P_\infty, P_1, \ldots, P_n$ are all the rational places in $H/K(x)$. Then, using the notation as in Definition 5.3.1, the Hermitian function field lattice $\mathcal{L}_\mathcal{P}$ is isomorphic to

$$\mathcal{L}_{\mathrm{Cl}^0(F)}(S) \coloneqq \left\{ (x_0, ..., x_n) \in \mathcal{A}_n \;\middle|\; \sum_{i=1}^{n} x_i[P_i - P_\infty] = [0] \in \mathrm{Cl}^0(F) \right\}.$$

In this case S is a generating set of the zero class group, while $\mathcal{P}$ is the set of rational places in H. Therefore, by Lemma 5.3.3 we conclude the following result on the automorphism group of the function field lattice. Recall that $\mathrm{Aut}(\mathrm{Cl}^0(F), S)$ is the group of permutations on S, which extend to automorphisms of $\mathrm{Cl}^0(F)$.

Lemma 5.5.1. *Let $H/K(x)$ be a hermitian function field. Let $\mathcal{P}$ be the set of rational places of H. Then* $\mathrm{Aut}(\mathrm{Cl}^0(F), S) \cong \mathrm{Aut}(\mathcal{L}_\mathcal{P}) \cap S_n$.

Remark 5.5.2. As it is mentioned in [Böt+16], we know that the zero class group of Hermitian function fields is isomorphic to the group $\mathbb{Z}_{q+1}^{q^2-q}$. Hence we know

that $\mathrm{Aut}(\mathrm{Cl}^0(F), \mathcal{P})$, and therefore by extension $\mathrm{Aut}(\mathcal{L}_\mathcal{P}) \cap S_n$, is a subgroup of $\mathrm{Aut}(\mathbb{Z}_{q+1}^{q^2-q})$.

Next we check the connection between the automorphisms of the function field and those of the lattice. From Theorem 5.1.2, we know that $\mathrm{Aut}(H)/\mathrm{Inv}(\mathcal{P})$ is a subgroup of the automorphism group of the lattice. Fortunately, it is shown in [Böt+16] that in the case of Hermitian function fields $\mathrm{Inv}(\mathcal{P})$ is trivial.

Theorem 5.5.3. $\mathrm{Aut}(H)$ *is a subgroup of* $\mathrm{Aut}(\mathcal{L}_\mathcal{P})$.

Much is known on the automorphisms of Hermitian function fields, see [Sti09].

5.6 Hyperelliptic Function Field Lattices

In this section, we represent our main results on automorphism groups of hyperelliptic function fields.

Lemma 5.6.1. *Let H be a hyperelliptic function field with defining equation $y^2 = f(x)$ for a square free polynomial $f(x)$. Let $\mathcal{P}$ be the set of ramified places of degree 1 and inert places of of degree 2 in H, with $|\mathcal{P}| = n + 1$. If either* $\mathrm{char}(H) = 2$, *or* $\mathrm{char}(H) \neq 2$ *and $f(x)$ does not split into linear factors, then the hyperelliptic function field lattice $\mathcal{L}_\mathcal{P}$ is similar to $\mathcal{A}_n$.*

Proof. By Theorem 4.1.1 we know that when $\mathrm{char}(H) = 2$, or when $f(x)$ does not split into linear factors, that the lattice $\mathcal{L}_\mathcal{P}$ has a basis of minimal vectors. On top of this, by Theorem 3.4.3 we know that these basis vectors and the minimal vectors of $\mathcal{L}_\mathcal{P}$ are all vectors of the form

$$(0, \ldots, 0, 2, 0, \ldots, 0, -2, 0, \ldots, 0)$$

These vectors are all exactly 2 times the minimal vectors of the root lattice $\mathcal{A}_n$, which also form a basis of $\mathcal{A}_n$. Hence there are basis matrices of these two lattices, which fulfill the relation

$$B_H = 2 \cdot B_A.$$

This implies that they are similar. □

This lemma yields an immediate corollary on the automorphism group of hyperelliptic function field lattices.

Corollary 5.6.2. *Let $\mathcal{L}_\mathcal{P}$ be a hyperelliptic function field lattice as defined in Lemma 5.6.1. Then the automorphism group of $\mathcal{L}_\mathcal{P}$ is*

$$\mathrm{Aut}(\mathcal{L}_\mathcal{P}) \cong \{\pm \mathrm{Id}\} \times S_{n+1}.$$

Proof. By Lemma 5.6.1, we know that the function field lattice is similar to $\mathcal{A}_n$. Therefore, By Lemma 2.1.32 means they have isomorphic automorphism groups. □

We note that this result only covers a specific case. Next we analyze what happens when $f(x)$ splits into linear factors. We recall that by Corollary 3.4.2 this case in particular is interesting because the lattice is generated by the vectors of the form $\Phi_{\mathcal{P}}(2P_i - 2P_j)$, which have length 2, and one additional vector $\Phi_{\mathcal{P}}(u)$, which has length $\sqrt{2g+2}$. The following theorem tackles this case.

Theorem 5.6.3. *Let H be a hyperelliptic function field with defining equation $y^2 = f(x)$, where $f(x)$ is a square-free polynomial of degree $2g+1$, which splits into linear factors. Let $\mathcal{P}$ be the set of ramified places and inert places of of degree 2 in H, with $|\mathcal{P}| = n+1$. Then the automorphism group of the function field lattice $\mathrm{Aut}(\mathcal{L}_{\mathcal{P}})$ has a subgroup isomorphic to*

$$S_{2g+2} \times S_s$$

where $2g+2$ is the number of ramified places and s is the number of inert places of degree 2.

Proof. For this proof we are fundamentally splitting the lattice in two. First we tackle the s coordinates associated with the inert places of degree 2. Remember that all function field lattices are sublattices of the root lattice $\mathcal{A}_n$, which has automorphism group $\{\pm \mathrm{Id}\} \times S_{n+1}$. Then we can focus on the subgroup $S_s \subset S_{n+1}$ which only permutes the last s coordinates of the vector. We claim that these automorphisms of $\mathcal{A}_n$ all define automorphisms on $\mathcal{L}_{\mathcal{P}}$.

Let $v \in \mathcal{L}_{\mathcal{P}}$ and let $\sigma \in S_s$ be an automorphism of $\mathcal{A}_n$ which only permutes the last s places. This means σ defines a bijection on the places $Q_1, ..., Q_s$. We just need to check that $\sigma(v)$ is still in the lattice $\mathcal{L}_{\mathcal{P}}$. For convenience we will work with the equivalent principle divisor, instead of the vector v,

$$D = \sum_{i=0}^{2g+1} a_i P_i + \sum_{j=1}^{s} b_j Q_j.$$

Then the image of this divisor under σ is

$$\begin{aligned}\sigma(D) &= \sum_{i=0}^{2g+1} a_i P_i + \sum_{j=1}^{s} b_{\sigma(j)} Q_{\sigma(j)} \\ &= \sum_{i=0}^{2g+1} a_i P_i + \sum_{j=1}^{s} b_j Q_j + \sum_{j=1}^{s} b_{\sigma(j)}(Q_{\sigma(j)} - Q_j).\end{aligned}$$

Because the places Q_i and Q_j are inert and of the same degree, the divisor $Q_i - Q_j$ is the conorm of a principal divisor in $K(x)$ and therefore is principal itself. This implies that $\sigma(D)$ is really equal to

$$\sigma(D) = D + \tilde{D}$$

where $\tilde{D}$ is a principal divisor with support on $\mathcal{P}$. This means $\sigma(D)$ is again a principal divisor with support on $\mathcal{P}$ and therefore a vector of the lattice $\mathcal{L}_{\mathcal{P}}$. This is enough to show that σ, when restricted to $\mathcal{L}_{\mathcal{P}}$, is an automorphism.

Next we focus on the ramified places. Hyperelliptic function field lattices can also be viewed as a type of lattice generated by abelian groups. The natural choice for the group from Definition 5.3.1 is $\mathrm{Cl}^0(F)$ and we take the set S to be the set of divisor classes $[P_i - P_\infty]$ for $1 \leq i \leq 2g+1$ and $[Q_j - 2P_\infty]$ for $1 \leq j \leq s$. Then the lattice $\mathcal{L}_{\mathcal{P}}$ is equivalent to

$$\mathcal{L}_{\mathrm{Cl}^0(F)}(S) = \Bigg\{ (a_0, ..., a_{2g+1}, b_1, ..., b_s) \in A_n \mid \sum_{i=1}^{2g+1} a_i[P_i - P_\infty] + \sum_{j=1}^{s} b_j[Q_j - 2P_\infty] = [0] \in \mathrm{Cl}^0(F) \Bigg\}.$$

Again, recall that all of the divisors $Q_j - 2P_\infty$ are already principal, since they are the conorms of principal divisors in $K(x)$, so the above equation simplifies to

$$\mathcal{L}_{\mathrm{Cl}^0(F)}(S) = \left\{ (a_0, ..., a_{2g+1}, b_1, ..., b_s) \in A_n \mid \sum_{i=1}^{2g+1} a_i[P_i - P_\infty] = [0] \in \mathrm{Cl}^0(F) \right\}.$$

Even though $\mathrm{Cl}^0(F)$ seems like the natural choice here, we actually get the exact same lattice if we just use the subgroup generated by the elements $[P_i - P_\infty]$. From [Sti09] we know that this group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g}$, since these divisors all have order two and they fulfill the relation $\sum_{i=1}^{2g+1}[P_i - P_\infty] = [0]$. Therefore this lattice is equivalent to

$$\mathcal{L}_{(\mathbb{Z}/2\mathbb{Z})^{2g}}(S) = \left\{ (a_0, ..., a_{2g+1}, b_1, ..., b_s) \in A_n \mid \sum_{i=1}^{2g+1} a_i[P_i - P_\infty] = [0] \in (\mathbb{Z}/2\mathbb{Z})^{2g} \right\}.$$

Now we can apply Lemma 5.3.3 to this lattice. We need to check $\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^{2g}, S)$, i.e. the permutations of S which extend to automorphisms of $(\mathbb{Z}/2\mathbb{Z})^{2g}$. We claim that all permutations of S can be extended to automorphisms of this group.

Let σ be a permutation in S_{2g+1}. We can view $(\mathbb{Z}/2\mathbb{Z})^{2g}$ as a $2g$ dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$. Then define the map $\varphi : (\mathbb{Z}/2\mathbb{Z})^{2g} \to (\mathbb{Z}/2\mathbb{Z})^{2g}$ by sending the generating elements $P_1, ..., P_{2g}$ to $P_{\sigma(i)}, ..., P_{\sigma(2g)}$ respectively. Then the last place $P_{2g+1} = \sum_{i=1}^{2g} P_i$ is mapped to $\sigma(P_{2g+1}) =$

$$\varphi(P_{2g+1}) = \varphi(\sum_{i=1}^{2g} P_i) = \sum_{i=1}^{2g} P_\sigma(i) = P_{\sigma(2g+1)}.$$

Since σ is a bijection the map φ is a bijective homomorphism and therefore an automorphism of the group. This shows that S_{2g+1} is a subgroup of the automorphism group of the lattice.

Then we can explicitly construct a transposition of the coordinates of the place at infinity P_∞ and another ramified place P_1. To this end, define the map τ on $\mathbb{R}^{2g+2+s}$ to be the linear map which permutes the first two coordinates of the vectors. Since this is already an isometry, we only need to show that is sends lattice vectors to lattice vectors. Again let us consider principal divisors instead of vectors for convenience. Let $D = a_0 P_\infty + \sum_{i=1}^{2g+1} a_i P_i + \sum_{j=1}^{s} b_i Q_i$ be a principal divisor of F. Then $\tau(D)$ is equal to

$$\begin{aligned}\tau(D) &= a_1 P_\infty + a_0 P_1 + \sum_{i=2}^{2g+1} a_i P_i + \sum_{j=1}^{s} b_i Q_i \\ &= D + [(a_1 - a_0)P_\infty + (a_0 - a_1)P_1].\end{aligned}$$

Since D is principal and the places P_∞, P_1 are ramified, we know that the integers a_0 and a_2 are either both even or both odd. This follows from how these divisors are generated, see Corollary 3.4.2. Hence $(a_1 - a_0)$ and $(a_0 - a_1)$ are both even. Therefore the divisor $(a_1 - a_0)P_\infty + (a_0 - a_1)P_1$ is principal since it is the conorm of the divisor $\frac{1}{2}(a_1 - a_0)P_\infty + \frac{1}{2}(a_0 - a_1)P_1$ in $K(x)$. This implies that $\tau(D)$ is the sum of two principal divisors, making it also principal. We conclude that τ defines a lattice automorphism of $\mathcal{L}_\mathcal{P}$.

Together, τ and S_{2g+1} generate a subgroup of the automorphism group which is isomorphic to S_{2g+2}. In addition, it is easy to check that the two subgroups S_{2g+2} and S_s intersect trivially.

□

Remark 5.6.4. Unlike in the first case, any permutation of a ramified and inert place will not define an automorphism on the lattice. Because of the inclusion of vectors like $\Phi_\mathcal{P}(u)$ it becomes obvious that entries in coordinates associated to inert places are always even whereas entries in those associated to ramified places are not. This means permuting these would result in a map which is not a bijection on the lattice.

Let us now take an explicit look at the case where the genus g is equal to 3. As mentioned in previous sections, lattices which are more symmetric or which have large kissing numbers will usually have larger automorphism groups. When $g = 3$ and the defining polynomial $f(x)$ splits into linear factors, the generating vectors all have the same length. The function field lattice in that case has a much larger kissing number than other lattices from hyperelliptic function fields.

Luckily, $g = 3$ is small enough to be easily implemented by hand in magma. Which means it is easy to check what the exact automorphism group is.

Example 5.6.5. Let H be the hyperelliptic function field over $\mathbb{F}_{11}$, with defining equation $y^2 = f(x)$, where

$$f(x) = x^7 + 5x^6 + 3x^5 + 9x^4 + 4x^3 + 2x^2 + 9.$$

Then H has genus $g = 3$ and has 8 ramified places of degree 1, which are the roots of $f(x)$ and the place at infinity, and two inert places of degree 2. The resulting lattice is of length 10 and rank 9 with basis matrix

$$B = \begin{pmatrix} -7 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ -2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

With a given basis matrix it is easy to implement the lattice in magma and compute the size of its automorphism group.

```
> L := Lattice(10, [-7,1,1,1,1,1,1,1,0,0, -2,0,2,0,0,0,0,0,0,0,
-2,0,0,2,0,0,0,0,0,0,0, -2,0,0,0,2,0,0,0,0,0,0, -2,0,0,0,0,2,0,0,0,
0, -2,0,0,0,0,0,0,2,0,0,0, -2,0,0,0,0,0,0,0,2,0,0, -2,0,0,0,0,0,0,0,
0,2,0, -2,0,0,0,0,0,0,0,0,0,2]);
> G := AutomorphismGroup(L);
> FactoredOrder(G);
[ <2, 9>, <3, 2>, <5, 1>, <7, 1> ]
```

The result is that this lattice has an automorphism group of size $2 \cdot 8! \cdot 2!$. By Theorem 5.6.3 the group is therefore isomorphic to $\{\pm \mathrm{Id}\} \times S_8 \times S_2$. This is rather surprising, since we would expect that, if any of the hyperelliptic function field lattices had a larger automorphism group, it would be this one.

6 Open Problems

In specific cases we were able to compute the determinant and the successive minima of hyperelliptic function field lattices. However, these problems in a more general setting are still not completely solved. This is due to the difficulty of understanding the structure of the extensions of places which split in the hyperelliptic function field. In such cases, even constructing a basis for these lattices is not trivial. Our hope is that more results in this direction will follow.

For many function field lattices we were not able to compute their entire automorphism groups. One approach could be to use the dual lattice and another could be to use Galois theory of function fields to find more automorphisms.

7 References

[Ajt98] Miklós Ajtai. "The shortest vector problem in L2 is NP-hard for randomized reductions". In: *Proceedings of the thirtieth annual ACM symposium on Theory of computing*. 1998, pp. 10–19.

[AS16] Leyla Ateş and Henning Stichtenoth. "A note on short vectors in lattices from function fields". In: *Finite Fields and Their Applications* 39 (2016), pp. 264–271.

[Ate17] Leyla Ateş. "On lattices from function fields". PhD thesis. 2017.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system I: The user language". In: *Journal of Symbolic Computation* 24.3-4 (1997), pp. 235–265.

[Böt+15] Albrecht Böttcher et al. "On lattices generated by finite Abelian groups". In: *SIAM Journal on Discrete Mathematics* 29.1 (2015), pp. 382–404.

[Böt+16] Albrecht Böttcher et al. "Lattices from Hermitian function fields". In: *Journal of Algebra* 447 (2016), pp. 560–579.

[Cas+09] Ignacio Cascudo et al. "Asymptotically good ideal linear secret sharing with strong multiplication over any fixed finite field". In: *Annual International Cryptology Conference*. Springer. 2009, pp. 466–486.

[CS13] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*. Vol. 290. Springer Science & Business Media, 2013.

[CS95] John H Conway and Neil JA Sloane. "A lattice without a basis of minimal vectors". In: *Mathematika* 42.1 (1995), pp. 175–177.

[DM20] Mohamed Taoufiq Damir and Guillermo Mantilla-Soler. "Bases of minimal vectors in tame lattices". In: *arXiv preprint arXiv:2006.16794* (2020).

[Emd81] Peter van Emde Boas. "Another NP-complete problem and the complexity of computing short vectors in a lattice". In: *Tecnical Report, Department of Mathmatics, University of Amsterdam* (1981).

[Fis01] Mitschrift Roger Fischlin. "Vorlesungen von Prof. Dr. CP Schnorr: Gittertheorie und algorithmische Geometrie, Reduktion von Gitterbasen und Polynomidealen". In: (2001).

[FM14] Lenny Fukshansky and Hiren Maharaj. "Lattices from elliptic curves over finite fields". In: *Finite Fields and Their Applications* 28 (2014), pp. 67–78.

[Gru93] Peter M Gruber. "Geometry of numbers". In: *Handbook of convex geometry*. Elsevier, 1993, pp. 739–763.

[Hes04] Florian Hess. “Computing relations in divisor class groups of algebraic curves over finite fields”. In: *preprint* (2004), p. 2.

[HMM21] Camilla Hollanti, Guillermo Mantilla-Soler, and Niklas Miller. “Dense generic well-rounded lattices”. In: *arXiv preprint arXiv:2107.00958* (2021).

[HR07] Christopher J Hillar and Darren L Rhea. “Automorphisms of finite abelian groups”. In: *The American Mathematical Monthly* 114.10 (2007), pp. 917–923.

[Mar13] Jacques Martinet. *Perfect lattices in Euclidean spaces*. Vol. 327. Springer Science & Business Media, 2013.

[MX20] Liming Ma and Chaoping Xing. “The group structures of automorphism groups of elliptic function fields over finite fields and their applications to optimal locally repairable codes”. In: *arXiv preprint arXiv:2008.12119* (2020).

[Que89] Heinz-Georg Quebbemann. “Lattices from curves over finite fields”. In: *Preprint (April 1989)* (1989).

[Reg04] O Regev. “Lattices in computer science. Lecture 8: dual lattices”. In: *University Lecture* (2004).

[Ros13] Michael Rosen. *Number theory in function fields*. Vol. 210. Springer Science & Business Media, 2013.

[RT90] Michael Yu Rosenbloom and Michael A Tsfasman. “Multiplicative lattices in global fields”. In: *Inventiones mathematicae* 101.1 (1990), pp. 687–696.

[Sal06] Gabriel Daniel Villa Salvador. *Topics in the theory of algebraic function fields*. Springer, 2006.

[Sha15] Min Sha. “On the lattices from elliptic curves over finite fields”. In: *Finite Fields and Their Applications* 31 (2015), pp. 84–107.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Vol. 254. Springer Science & Business Media, 2009.

[TVZ82] Michael A Tsfasman, SG Vlădutx, and Th Zink. “Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound”. In: *Mathematische Nachrichten* 109.1 (1982), pp. 21–28.

[Wen18] Jinming Wen. “Some properties of successive minima and their applications”. In: *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2018, pp. 686–690.