Ramanujan graphs, quaternion algebras, and supersingular elliptic curves

Leivaditis, Alexandros

Alexandros Leivaditis

Ramanujan graphs, quaternions algebras, and supersingular elliptic curves

Master Thesis

July 31, 2023

Thesis Supervisor: Peter Bruin

Universiteit Leiden
Mathematisch Instituut

Contents

Acknowledgements

First and foremost, I wish to express my gratitude to my supervisor Peter Bruin for his guidance and feedback throughout this process. His willingness to share his deep knowledge of the subject has been essential in the development of this thesis. I am also thankful to my friends from 17ω for our shared paths and to Ioli for always being supportive, for all the late-night feedback sessions and editing help. Lastly, I would like to thank my lifelong friends and family for their support throughout my studies.

Introduction

Expander graphs are graphs that entertain two seemingly contradictory properties; they are sparse graphs that are highly connected. When we refer to sparsity, we generally mean that they have a small number of edges relative to the number of vertices. On the other hand, their high connectivity arises from their large edge expansion, which means that each set of vertices expands by a proportionate amount relative to its size.

Strong expanders exhibit numerous interesting graph properties such as high robustness, low diameter, and large girth. Moreover, they behave like random graphs, which has been apparent in various findings such as the Expander Mixing Lemma [AC88] and its inverse [BL06], as well as the Random Walk Sampling Theorem [AKS87]. These two facts have motivated extensive research in this area and made probabilistic techniques a natural approach for their exploration. In 1973, M. Pinsker [Pin73] was the first to prove the **existence of expanders** using such techniques and counting arguments. Surprisingly, a random graph is a good expander with high probability [Lub94].

Nevertheless, in applications, one needs **explicit constructions** of expander graphs, which were proved to be a considerably more challenging mission than the existential results. In particular, on the majority of the known constructions, while the definition of the graphs at hand is relatively easy, the analysis of their expansion is highly non-trivial and depends on various deep results of mathematics.

The first such construction was given in 1973 by G. Margulis [Mar73]. Margulis used the Kazhdan's Property (T) [Kaz67] of the group $\mathrm{SL}_3(\mathbb{Z})$ to prove that his construction was indeed an expander family. However, his proof was existential and did not explicitly bounded the expansion of these graphs. In 1981, O. Gaber and Z. Galil [GG81] followed Margulis' approach and using with tools from harmonic analysis they gave a lower bound on the spectral gap of these graphs. Another construction of expanders was given in 1988 by A. Lubotzky, R. Philips, and P. Sarnak [LPS88] and independently by Margulis [Mar88], who gave an expander family of Cayley graphs over the projective special linear group $\mathrm{PSL}_2(\mathbb{F}_p)$. These graphs constitute the first construction of Ramanujan graphs, which are the optimal expanders and will be the the main object of interest of this thesis. The proof on the bound of the expansion for these graphs relies on the Ramanujan-Petersson Conjecture, proved by P. Deligne [Del73]. In 1994, Lubotzky [Lub94] managed to show a similar result to the one of Margulis [Mar73], giving another family of Cayley expander graphs on $\mathrm{SL}_2(\mathbb{F}_p)$. Here, $\mathrm{SL}_2(\mathbb{Z})$ fails to have the Kazhdan Property (T), as it is the case for $\mathrm{SL}_3(\mathbb{Z})$ and was used by Margulis, but Lubotzky managed to use Selberg's 3/16 Theorem [Sel65] to bound the spectral gap of his graphs in an identical way as Margulis. Note that Selberg's 3/16 Theorem is essentially a special case of the Ramanujan-Petersson Conjecture, see [Kat76, p. 297]. It is also worth mentioning the first combinatorial construction of a family of expanders due to O. Reingold, S. Vadhan and A. Wigderson [RVW02]. This is an iterative process that uses their newly defined zig-zag product on graphs and a simple algebraic observation about the eigenvalues of this product.

Using explicit constructions, expanders have found **applications** in a wide range of fields in applied and pure mathematics, as well as in computer science. We name here a few such applications. The LPS construction [LPS88] gave an "explicit" improvement over the known graphs of P. Erdős and H. Sachs [ES63], which are graphs with large girth. M. Gromov [Gro09] used expanders in order to give a counterexample to the generalized form of the Baum-Connes conjecture [Val02]. In complexity theore, O. Reingold [Rei08] used expanders to show the equality of complexity classes $\mathrm{SL} = \mathrm{L}$ and I. Dinur [Din07] to prove the PCP theorem [AS98]. In network theory, expanders serve

as the key building block of robust superconcentrators [HLW06] and in particular in the celebrated AKS sorting network [AKS83].

As mentioned earlier, **Ramanujan graphs** are the optimal expanders in the sense that they obtain the optimal expansion constant. Regardless what the name suggests their nature is not number-theoretic. The name is derived from their first explicit construction [LPS88], which uses the Ramanujan conjecture to establish the expansion bound. Remarkably, every explicit construction of constant-degree Ramanujan families existing in the literature, depends on this conjecture and its generalizations. Based on the preceding discussion, the need of explicit constructions of Ramanujan graphs is apparent.

Their **history** dates back a little further. In 1986, N. Alon conjectured in [Alo86] that "most" (n, d)-graphs are nearly-Ramanujan, leaving however what "random" means undetermined. Friedman [Fri03] proved the conjecture true, where he also specifies what model of random graphs one should take.

As previously stated, the first explicit construction of a sequence of Ramanujan graphs is due to A. Lubotzky, R. Philips, and P. Sarnak [LPS88], and independently due to Margulis [Mar88]. These graphs are Cayley graphs over $\mathrm{PSL}_2(\mathbb{F}_p)$ of degree $p+1$, where p is an odd prime, and although it is easy to define them, the proof that they are indeed Ramanujan relies on the **Ramanujan-Petersson Conjecture**. Using a generalization of the LPS construction, P. Chiu [Chi92] gave an explicit construction for the remaining case $p = 2$, i.e. a family of 3-regular Ramanujan graphs. Morgenstern [Mor94] used similar techniques passing on function fields to give a family of Cayley Ramanujan graphs over $\mathrm{PSL}_2(\mathbb{F}_q(x))$ of degree $q+1$, where q is a prime power. His construction again depends on the Ramanujan-Petersson Conjecture but over global function fields, which was proved by Drinfeld [Dri88]. Another construction, again depending on the Ramanujan-Petersson conjecture, was given by A. Pizer [Piz90]. One of the two main theorems of this thesis is the proof that Pizer's graphs are indeed Ramanujan. We note here that Pizer's graphs is the first explicit construction of non-Cayley Ramanujan graphs, see [Piz90, Section 6]. There have been very few other explicit constructions of Ramanujan graphs known in the literature [JL97, JY18, BKS16]. The first two papers [JL97, JY18] generalise the LPS Ramanujan graphs and again use the Ramanujan-Petersson conjecture to establish the expansion bound, while the latter [BKS16] introduces a new family of Ramanujan graphs of unbounded degree though, which depends on Deligne's bound, again based on Deligne's work [Del73]. Some more elementary constructions of Ramanujan graphs exist but all of them are of unbounded degree, see [dR97, Gun05, BST09, MS18, HLL19].

The goal of this thesis is to describe the construction of Pizer [Piz98], prove that these graphs are indeed Ramanujan, and derive that the so-called supersingular isogeny graphs are Ramanujan likewise.

Pizer graphs. Pizer graphs are multigraphs defined by the so called Brandt matrices associated to Eichler orders over quaternion algebras. In order to use the Ramanujan-Petersson conjecture we define a space of theta series that corresponds to the elements of the class set of the Eichler order, in which space the action of the Hecke operators is given by the Brandt matrices. Then, the result is derived by the R-P conjecture for cusp forms of weight 2 for a specific congruence subgroup, proved by [Del73].

Supersingular isogeny graphs. Supersingular elliptic curves are elliptic curves over finite fields that correspond to maximal orders in quaternion algebras. Supersingular isogeny graphs are the graphs with vertices equivalence classes of supersingular elliptic curves and edges isogenies between them. We prove that these graphs are Ramanujan by using the Deuring Corre-

spondence [Deu41], which shows that these graphs are isomorphic to a certain subclass of Pizer's graphs.

This thesis is structured as follows:

We start, in Section 1, by an introduction to spectral graph theory, which enables us to study graphs via the spectrum of their adjacency matrix. In this section, we introduce the notion of the expander graph and prove the Alon-Boppana bound (Theorem 1.34), which gives an asymptotic bound on their expansion constant. Graphs that attain this bound are called Ramanujan and are the graphs

In Section 2, we examine quaternion algebras. We prove how their local behaviour characterizes them, but we primarily study their arithmetic theory: lattices, orders, and ideals. Finally, we introduce and characterize (locally) two important classes of orders, maximals orders and Eichler orders, where the latter constitutes a generalization of the former. Eichler Orders will serve as the base ground where we will define the Pizer graphs.

In Section 3, we study elliptic curves and in particular supersingular elliptic curves. These are elliptic curves such that their endomorphism algebra corresponds to quaternion algebras in contrast to their complement, namely ordinary elliptic curves, which correspond to quadratic fields. We continue by studying the arithmetic properties of their endomorphism algebras as quaternion algebras. Finally, we review the results of C. Waterhouse [Wat69] about kernel ideals, using group-schemes; this will allow us to prove the Deuring correspondence in (5.2.2) and their connection to the Eichler orders.

In Section 4, we introduce the theory of modular forms. We begin by defining modular forms over congruence subgroups and subsequently Hecke operators and how they act on the space of cusp forms. We continue by stating the Ramanujan-Petersson Conjecture, which as mentioned above is the main ingredient in the proof of the central theorem of this thesis (Theorem 5.24): Pizer graphs are Ramanujan. We conclude this section by reviewing the theory of theta series arising from quadratic forms.

The last section (Section 5) consists of the definitions of Pizer graphs and supersingular isogeny graphs and the proofs that these graphs are Ramanujan. In particular, in (5.1) we start by defining the Brandt matrices associated to orders in quaternion algebras over $\mathbb{Q}$. Then, we define the Brandt graphs, which are our Pizer graphs, and, under specific technical conditions, are the graphs with adjacency matrix the Brandt matrices. We conclude this subsection by proving the first main theorem of this thesis (Theorem 5.24). Finally, in (5.2), we define the supersingular isogeny graphs and we prove the Deuring correspondence, which gives an isomorphism between the Brandt graphs and supersingular isogeny graphs. We conclude, by proving the second main theorem of this thesis (Corollary 5.29): supersingular isogeny graphs are Ramanujan.

1 Spectral Graph Theory

We start by introducing some preliminary notions in graph theory. We follow J.-P. Serre [Ser94] and Pizer [Piz98].

Definition 1.1. An *(undirected) multigraph* G is a quintuple $G = (V, E, o, t, \bar{\cdot})$, where V is a finite set of *vertices*, E is a finite set of *edges*, $o, t : E \to V$, and $\bar{\cdot} : E \to E$ are functions such that for each edge $e \in E$ it holds that $e \neq \bar{e}, \bar{\bar{e}} = e$, $o(\bar{e}) = t(e)$, and $t(\bar{e}) = o(e)$. The *order* of G, denoted by $|G|$, is the cardinality of V.

For vertices $u, v \in V$, a (u, v)-*edge* is an edge e such that $o(e) = u$ and $t(e) = v$. Every (u, u)-edge is called a *loop*. If for vertices $u, v \in V$ there exists a (u, v)-edge then we say that u and v are adjacent and we write $u \sim v$. The *neighborhood* of a vertex $u \in V$ is the set $N_G(u) := \{e \in E \colon o(e) = u\}$. The *degree* of a vertex $u \in V$ is defined as $\deg_G(v) := \#N_G(u)$. If $v, u \in V$ we also define the set of edges between them as $E_G(v, u) := \{e \in E \colon o(e) = u, t(e) = v\}$.

We call a multigraph G, a *simple graph*, if G does not have loops and no *multiple edges*, i.e. for each vertices $u.v \in V$ there exists at most one (u, v)-edge.

When there is no confusion we may refer to a multigraph as just a graph.

Definition 1.2. Let G, G' be multigraphs. A *morphism of graphs* $\phi : G \to G'$ is a pair of functions $f : V(G) \to V(G'), g : E(G) \to E(G')$ such that for every $e \in E(G)$ it holds that $f(o(e)) = o(g(e))$, $f(t(e)) = t(g(e))$, and $\overline{g(e)} = g(\bar{e})$. A morphism of graphs $\phi = (f, g) : G \to G'$ is called an *isomorphism* if $f : V(G) \to V(G')$ is a bijection and g is a *local bijection*, i.e. for every $u, v \in V(G)$ the induced map

$$g : E_G(u, v) \longrightarrow E'_G(f(u), f(v))$$

are bijections.

Let G be a multigraph and let $u, v \in V(G)$. A (u, v)-*walk* W *of length* r in G is a sequence of edges $(e_1, \ldots, e_r)$ such that $o(e_1) = u$, $t(e_r) = v$, and for each $i = 1, \ldots, r-1$, $t(e_i) = o(e_{i+1})$. We say that W is a *closed walk* if $o(e_1) = t(e_r)$. We also say that W has a *backtracking* if there exists $i = 1, \ldots, r-1$ such that $e_{i+1} = \overline{e_i}$. A walk is called to be *without backtracking* (or just a *w.b. walk*) if it doesn't have backtracking. A *cycle of length* r is a closed w.b. walk $(e_1, \ldots, e_r)$ such that the vertices $t(e_i)$'s are pairwise distinct.

Below, we define some graph parameters that we will use.

- **Girth**. The *girth* of a graph G is the length of a shortest cycle in G, that is $\text{girth}(G) := \min\{r \geq 0; \ \exists \text{ cycle of length } r\}$.
- **Diameter**. The distance between two vertices $u, v \in V$ is defined as the length of the shortest (u, v)-walk in G and is denoted by $\text{dist}_G(u, v)$. If there does not exist such walk we write $\text{dist}_G(u, v) = \infty$. The *diameter* of G is defined as the maximum distance between vertices in G, i.e.
$$\text{diam}(G) := \max_{u,v \in V(G)} \text{dist}_G(u, v).$$
- **Independence number**. A subset $I \subseteq V(G)$ is said to be *independent set* if no vertices I are adjacent. The size of a maximum independent set in G is called the *independence number* of G and is denoted by $\alpha(G)$.

- **Chromatic number**. Given a positive integer k, we say that a function $c : V(G) \to \{1, \dots, k\}$ is a *proper k-coloring* of G if for every adjacent vertices $u, v \in V(G)$ it holds that $c(x) \neq c(y)$. The maximum value k for which there exists a proper k-coloring of G is called the *chromatic number* of G and is denoted by $\chi(G)$.

1.1 Adjacency Matrix

We start by giving the basic definitions of spectral graph theory and examine some basic properties of them. To each multigraph we assign a matrix that determines it uniquely and allows us to study graph properties algebraically.

Definition 1.3. Given a multigraph G of order n, we define its *adjacency matrix* as the n-by-n the matrix $A(G)$ on the set of vertices $V(G)$, where for each $u, v \in V(G)$,

$$A(G)_{u,v} = \#\{e \in E; o(e) = u, t(e) = v\}.$$

Remark 1.4. Given multigraph G, $A(G)$ is a real symmetric matrix with even diagonal. Conversely, a symmetric matrix A with non-negative integer entries and even diagonal determines a unique multigraph with adjacency matrix A.

Let G be a multigraph and set $A := A(G)$, For a non-negative integer r, A^r counts the number of walks of length r in the graph G. This follows from the computation

$$A^{r+1}_{u,v} = (A^r A)_{u,v} = \sum_{w \in V} A^r_{u,w} A_{w,v},$$

and the fact that a (u, v)-walk of length $r + 1$ is concatenation of a (u, w)-walk of length r and a (w, v)-edge.

However, if we want to count the number of w.b. walks the task becomes slightly more difficult. We define the n-by-n matrices $A_r := A_r(G)$ on V by setting $A_r(G)_{u,v}$ to be the number of w.b. (u, v)-walks of length r in G. For length $r = 1$ all walks of length 1 are w.b. and so $A_1(G) := A(G)$. For length $r = 2$ we distinguish 2 cases: if we have a (u, v)-walk of length 2, where $u \neq v$, then it is obviously w.b. and so it is counted in $A(G)^2_{u,v}$; in the other case, where $u = v$, the (u, u)-walks that have backtracking correspond to the edges $e \in N_G(u)$ and so the number of w.b. (u, u)-walks of length 2 equals to $A(G)^2_{u,u} - \deg_G(u)$. For the general case we prove the following:

Proposition 1.5. *Let G be a multigraph of order n. Then, we have the following recursive relations for the matrices A_r:*

$$A_1 = A(G), \quad A_2 = A_1^2 - D, \text{ and}$$
$$A_{r+1} = A_r A_1 - A_{r-1}(D - I), \quad r \geq 2,$$

where D is the n-by-n diagonal matrix on V defined by $D := (\deg_G(u))_{u \in V}$.

Proof. The cases $r = 1, 2$ have been established above. So let $r \geq 2$. For vertices $u, v \in V(G)$, we need to prove that

$$\sum_{w \in V} (A_r)_{u,w} A_{w,v} = (A_{r+1})_{u,v} + (A_{r-1})_{u,v}(\deg(v) - 1). \tag{1}$$

A (u,v)-walk counted in the left sum is of the form $P = (e_1, \ldots, e_r, e_{r+1})$, where $P' = (e_1, \ldots, e_r)$ is a w.b. (u,w)-walk of length r and e_{r+1} is a (w,v)-edge. We distinguish two cases:

Case 1: $e_{r+1} \neq \overline{e_r}$. Then, P is a w.b. (u,v)-walk of length $r+1$. which is counted in $(A_{r+1})_{u,v}$.

Case 2: $e_{r+1} = \overline{e_r}$. In this case P is not a w.b. walk and so it is not counted in $(A_{r+1})_{u,v}$. Moreover, $P'' = (e_1, \ldots, e_{r-1})$ is a w.b. (u,v)-walk, since $t(e_{r-1}) = o(e_r) = o(e_{r+1}) = v$, and so e_r is a (v,w)-edge different from $\overline{e_{r-1}}$. The number of these edges equals $\deg(v) - 1$ and so the walk P in this case is counted in the second summand of (1). □

The next lemma is a generalization of a standard lemma in graph theory, the so called *Handshaking Lemma*, which will be helpful in our calculations in (1.2).

Lemma 1.6 (The Handshaking Lemma)**.** *Let G be a multigraph, A its adjacency matrix, and $k \in \mathbb{R}^{V \times V}$ a matrix. Then it holds that*

$$\sum_{u,v \in V} A_{u,v} k_{u,v} = \sum_{e \in E} k_{o(e),t(e)}.$$

Proof. This result follows by a simple double counting argument. In the left sum we add the term $k_{u,v}$, $A_{u,v}$ times for each pair of vertices $(u,v) \in V^2$ such that $A_{u,v} \neq 0$, which means that for each pair $(u,v) \in V^2$ we add the term $k_{u,v}$ for each (u,v)-edge in G. The result follows. □

By taking the all 1 matrix $k = (1)_{u,v \in V}$, Lemma 1.6 indeed implies the classical Handshaking Lemma, which states that $\sum_{u \in V} \deg_G u = |E|$.

Corollary 1.7. *Let G be a multigraph, A its adjacency matrix, and $x \in \mathbb{R}^V$ a vector. Then, the following hold:*

1. $x^T A x = \sum_{u,v \in V} A_{u,v} x_u x_v = \sum_{e \in E} x_{o(e)} x_{t(e)}$
2. $\sum_{u \in V} \deg(u) x_u^2 = \frac{1}{2} \sum_{e \in E} (x_{o(e)}^2 + x_{t(e)}^2)$
3. $x^T A x = \sum_{v \in V} \deg(u) x_u^2 - \frac{1}{2} \sum_{e \in E} (x_{o(e)} - x_{t(e)})^2$.
4. $x^T A x = -\sum_{v \in V} \deg(u) x_u^2 + \frac{1}{2} \sum_{e \in E} (x_{o(e)} + x_{t(e)})^2$

Proof. (1) follows immediate from Lemma 1.6 by taking the matrix $(x_u x_v)_{u,v \in V}$. (2) follows from the identities $\sum_{u \in V} \deg(u) x_u^2 = \sum_{u \in V} (\sum_{v \in V} A_{u,v}) x_u^2$, $\sum_{e \in E} x_{o(e)}^2 = \sum_{e \in E} x_{t(e)}^2$, and Lemma 1.6 for the matrix $(x_u^2)_{u,v \in V}$. (3) follows from (1) and (2) and the identity $2 \sum_{e \in E} x_{o(e)} x_{t(e)} - \frac{1}{2} \sum_{e \in E} (x_{o(e)}^2 + x_{t(e)}^2) = \sum_{e \in E} (x_{o(e)} - x_{t(e)})^2$. (4) follows in a similar way as (3). □

In this thesis our main focus will be on *regular* multigraphs and graphs:

Definition 1.8. Let k be a non-negative integer. A multigraph G is called *k-regular* if for every vertex $u \in V$, $\deg_G(u) = k$, or equivalently, $\sum_{v \in V} A_{u,v} = k$. The number k is called the *valency* of G.

Remark 1.9. It is important to note that a multigraph G is k-regular if and only if the unit vector $\mathbb{1}$ is an eigenvector of $A(G)$. This is indeed the case, since if $v \in V$, then $(A\mathbb{1})_v = \sum_{u \in V} A_{u,v}$.

1.2 Graph Spectrum

There are many combinatorial properties of a given graph that are determined by its spectrum. In this section, we mention some of these properties as long as some limitations of the spectral approach.

Definition 1.10. Given a multigraph G, we define its *graph spectrum* as the spectrum of its adjacency matrix $A(G)$, i.e. the set of the eigenvalues of $A(G)$ counted with multiplicities. We write $\text{spec}(G) = \{(\lambda_1)^{m_1}, \dots, (\lambda_k)^{m_k}\}$ for the multiset of the spectrum of G, where λ_i are the eigenvalues of $A(G)$ and m_i their multiplicities, respectively.

Let G be a multigraph with eigenvalues $\lambda_n \leq \cdots \leq \lambda_1$ (counted with multiplicity) and adjacency matrix A. As we have seen in Remark 1.4, A is a real symmetric matrix and thus the (finite-dimensional) Spectral Theorem tells us that A has an orthonormal basis of eigenvectors; hence it is diagonalizable. In particular, the eigenvalues of G are real numbers and there exists an orthonormal eigenbasis $x_1, \dots, x_n$ of $\mathbb{R}^V$.

Remark 1.11. Moreover, since A is diagonalizable, the algebraic multiplicity of an eigenvalue λ equals its geometric multiplicity, i.e. the multiplicity of a root λ in the characteristic polynomial $\det(xI - A)$ of A equals the dimension of the eigenspace $E_\lambda := \{x \in \mathbb{R}^V : Ax = \lambda x\}$ of λ.

The following characterization of the eigenvalues of an arbitrary symmetric matrix $A \in \mathbb{R}^{n\times n}$ will be of great use for us. For a vector $x \in \mathbb{R}^n$ we will write $R_A(x)$ (or just $R(x)$) for the *Rayleigh quotient* of A on x defined by

$$R_A(x) := \frac{x^T Ax}{x \cdot x}.$$

Theorem 1.12 (Variational Characterization of the Spectrum)**.** *Let $A \in \mathbb{R}^{n\times n}$ be a symmetric matrix, let $\lambda_n \leq \cdots \leq \lambda_1$ be the eigenvalues of A, and let $x_1, \dots, x_n$ be eigenvectors of A that form an orthonormal basis of $\mathbb{R}^n$ such that $Ax_i = \lambda_i x_i$, for each $i = 1, \dots, n$. Then, we have that*

$$\lambda_k = \max_{\substack{x \in \langle x_1, \dots, x_{k-1}\rangle^\perp \\ x \neq 0}} R_A(x).$$

Proof. We first make the following observation for two eigenvectors x_i, x_j, $1 \leq i, j \leq k$,

$$x_i^T Ax_j = \lambda_j x_i^T x_j = \begin{cases} \lambda_j, & i = j \\ 0, & i \neq j \end{cases}$$

Consider now a non-zero vector $x \in \langle x_1, \dots, x_{k-1}\rangle^\perp$. Since $\{x_1, \dots, x_k\}$ is an orthonormal basis for $\mathbb{R}^n$, we may write $x = \sum_{i=k}^n a_i x_i$ for some $a_k, \dots, a_n \in \mathbb{R}$. Thus, we get that

$$R_A(x) = \frac{x^T Ax}{x \cdot x} = \frac{\sum_{k\leq i,j\leq n} a_i a_j x_i^T Ax_j}{\sum_{k\leq i,j\leq n} a_i a_j x_i^T x_j} = \frac{\sum_{i=k}^n a_i^2 x_i^T Ax_i}{\sum_{i=k}^n a_i^2} = \frac{\sum_{i=k}^n a_i^2 \lambda_i}{\sum_{i=k}^n a_i^2} \leq \lambda_k.$$

The result follows from the fact that $R_A(x_k) = \lambda_k$ for each $k = 1. \dots, n$. □

Using the variational characterization of the eigenvalues we can prove the following properties of the spectrum as follows.

Proposition 1.13. *Let $\delta = \delta(G)$ and $\Delta = \Delta(G)$ be the minimum and the maximum degree of G, respectively. Then, the following hold:*

1. $\mathrm{tr}(A^k) = \sum_{i=1}^{n} \lambda_i^k$ *is the number of closed walks in G of length k.*
2. $-\Delta(G) \leq \lambda_n \leq \cdots \leq \lambda_1 \leq \Delta(G)$.
3. $\delta(G) \leq \lambda_1 \leq \Delta(G)$

Proof. (1) follows directly from our observation that $A^k_{u,v}$ equals the number of (u,v)-walks in G.

For (2), by applying Theorem 1.12 to A and to $-A$ we get that

$$\lambda_1 = \max_{x \neq 0} R_A(x) \qquad \text{and} \qquad \lambda_n = \min_{x \neq 0} R_A(x)$$

and thus in order to prove that $-\Delta \leq \lambda_n \leq \lambda_1 \leq \Delta$ we need to prove for every $x \neq 0$ that $-\Delta \leq R_A(x) \leq \Delta$. This follows from Corollary 1.7(3,4) as for a non-zero vector $x \in \mathbb{R}^V$ we get that

$$R_A(x) = \frac{x^T A x}{x \cdot x} \leq \frac{\sum_{u \in V} \deg(u) x_u^2}{\sum_{u \in V} x_u^2} \leq \frac{\Delta \sum_{u \in V} x_u^2}{\sum_{u \in V} x_u^2} = \Delta$$

and similarly that $R_A(x) \geq -\Delta$.

For (3), the inequality $\lambda_1 \leq \Delta$ has been proved above, so is suffices to prove that $\delta \leq \lambda_1$. As above, we have that $\lambda_1 = \max_{x \neq 0} R_A(x)$ and so by applying the unit vector $\mathbb{1}$ to the Rayleigh quotient $R_A(x)$ we get that

$$\lambda_1 \geq R_A(\mathbb{1}) = \frac{\mathbb{1}^T A \mathbb{1}}{\mathbb{1}^T \mathbb{1}} = \frac{\sum_{u,v \in V} A_{u,v}}{\sum_{u \in V} 1} = \frac{\sum_{u \in V} \deg_G(u)}{n} \geq \frac{n\delta}{n} = \delta.$$

Hence, indeed $\lambda_1 \geq \delta$. □

Regular Graphs. As the graphs of interest in this thesis are regular graphs, the following proposition, which states the basic properties of the eigenvalues of a regular graph, will play an important role.

Proposition 1.14. *Let G be a d-regular multigraph and let $A = A(G)$ be its adjacency matrix with eigenvalues $\lambda_n \leq \cdots \leq \lambda_2 \leq \lambda_1$. Then, the following hold:*

1. $\lambda_1 = d$ *and* $A\mathbb{1} = d\mathbb{1}$.
2. $-d \leq \lambda_n$.
3. *The multiplicity of the eigenvalue d equals the number of connected components of G.*
4. $\lambda_n = -d$ *iff G has a bipartite connected component. Moreover, if G is connected, then G is bipartite iff* $\mathrm{spec}(G)$ *is symmetric around* 0.

Proof. (1,2.) This is a direct corollary of Proposition 1.13, since $\delta(G) = d = \Delta(G)$ and Remark 1.9.

(3.) For every connected component C of G consider the indicator vector for this component $x_C \in \{\pm 1\}^V$ defined by $(x_C)_v = 1 \iff v \in V(C)$. Each such vector is an eigenvector of G corresponding to the eigenvalue d. Indeed, for each $v \in V$ we compute

$$(Ax_C)_v = \sum_{u \in V} A_{u,v}(x_C)_u = \sum_{u \in V(C)} A_{u,v} = \begin{cases} \deg(v) = d, & v \in V(C) \\ 0, & v \notin V(C) \end{cases}$$

which shows that $Ax_C = dx_C$. Observe that these vectors are linearly independent. We claim that these eigenvectors span the eigenspace E_d and thus they form a basis of it. It is enough to prove that if $x \in E_d$, then x is constant on each connected component of G. So let $x \in E_d$ be a non-zero eigenvector and observe that $R_A(x) = d$. By Corollary 1.7, we get that

$$R_A(x) = \frac{d\sum_{v \in V} x_u^2 - \frac{1}{2}\sum_{e \in E}(x_{o(e)} - x_{t(e)})^2}{\sum_{u \in V} x_u^2} \leq d$$

where equality holds if and only if $\sum_{e \in E}(x_{o(e)} - x_{t(e)})^2 = 0$. Thus, for every $e \in E$ we get that $x_{o(e)} = x_{t(e)}$. If now $u, v \in V$ belong to the same connected component, then there exists a walk $W = (e_1, \ldots, e_n)$ such that $o(e_1) = u$ and $t(e_n) = v$; hence

$$x_u = x_{t(e_1)} = \cdots = x_{o(e_n)} = x_v,$$

which implies the claim. Therefore, we have that $\dim E_d = \#\{\text{connected components of } G\}$. The result then follows from Remark 1.11.

(4.) This follows as in (3) by considering specific indicator vectors for the parts of the bipartite graph, see [HLW06].

□

Cospectral graphs. There are some limitations on the information we can get from the eigenvalues of a graph G. To this end we say that two graphs are *cospectral* if they have the same spectrum. Consider the graphs $K_{1,4}$ and $C_4 \sqcup K_1$ depicted below:

Figure 1: Two cospectral graphs. $K_{1,4}$ (left) and $C_4 \sqcup K_1$ (right).

These graphs are represented by the matrices

$$A(K_{1,4}) = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A(C_4 \sqcup K_1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Thus, computing the spectrum of these two graphs we conclude that they are cospectral with spectrum equal to $\{-2, (0)^3, 2\}$. From this example, we can see that, despite the fact that the number of closed walks in a graph G is completely determined by its spectrum (Proposition 1.13), the number of cycles cannot be computed by the spectrum alone, as in $C_4 \sqcup K_1$ there is a cycle of length 4, whereas in $K_{1,4}$ there's none.

1.3 Expanders

Fix a d-regular multigraph G with adjacency matrix $A = A(G)$ and order $n = |V|$.

1.3.1 Edge Expansion.

A motivating question for defining expander graphs is the following:

· *Question:* What fraction of the edges should one remove in order to get two "large" connected components?

In order to formalise this question we need the notion of the *edge expansion* of a cut of G. A *cut* of a graph G is a pair $(S, \overline{S})$, where $S \subseteq V$ and $\overline{S} = V \setminus S$. For $S, T \subseteq V$ we define $E_G(S,T) := \{e \in E \colon o(e) \in S,\ t(e) \in T\}$ and set $e_G(S,T) := |E_G(S,T)|$. We also define $E_G(S) := E_G(S,S)$ and $e_G(S) := |E_G(S)|$ for a subset $S \subseteq V$.

Definition 1.15. Let $S \subseteq V$ be a non-empty vertex set of G such that $S \neq V$. We define the *edge expansion of the cut* $(S, \overline{S})$ as follows:

$$\phi_G(S) := \frac{e_G(S, \overline{S})}{d \cdot \min\{|S|, |\overline{S}|\}}.$$

The *edge expansion of* G is then defined as

$$\phi(G) := \min_{\emptyset \subsetneq S \subsetneq V} \phi_G(S) = \min_{1 \leq |S| \leq n/2} \phi_G(S).$$

Note 1.16.

1. Note that in the definition of the edge expansion of a vertex set $S \subseteq V$, such that $1 \leq |S| \leq n/2$, the denominator plays the role of the maximum number of edges that can leave S, as G is d-regular. Thus, $0 \leq \phi(G) \leq 1$. Note also that $\phi(G) = 0$ if and only if G is disconnected.

2. There are other definitions of the expansion of a graph in the literature, which are all essentially equivalent up to a constant. The basic idea is that every subset of vertices of G expands by some fixed amount relatively to its size.

To answer our starting question now, we provide the following lemma, which states rougly that if the edge expansion of G is c then removing any $0 < \epsilon < c$ fraction of the edges leaves a "large" enough connected component:

Lemma 1.17. *Suppose that $\phi(G) = c \in (0,1]$ and let $E' \subseteq E$ be a subset of edges with $|E'| < \frac{dn}{2}\varepsilon$, where $0 < \varepsilon < c$. Then, $G \setminus E'$ has a connected component of at least $(1 - \frac{\varepsilon}{2c})n$ vertices.*

Proof. Let $C_1, C_2, \ldots, C_r$ be the connected components of $G \setminus E'$. Assume that $|C_1| \geq |C_2| \geq \cdots \geq |C_r|$. By the definition of $\phi(G)$ we have that for each $i = 1, \ldots n$, $e_G(C_i, \overline{C_i}) \geq cd \min(|C_i|, |\overline{C_i}|)$. If $|C_1| \leq n/2$ then

$$|E'| = \sum_{1 \leq i < j \leq r} e_G(C_i, C_j) = \frac{1}{2} \sum_{1 \leq i \leq r} e_G(C_i, \overline{C_i}) \geq \frac{cd}{2} \sum_{1 \leq i \leq r} |C_i| = \frac{cdn}{2} > \frac{\varepsilon dn}{2},$$

which is a contradiction. Thus, $|C_1| > n/2$ and so

$$cd|\overline{C_1}| \leq e_G(C_1, \overline{C_1}) \leq |E'| \leq \frac{\varepsilon dn}{2}.$$

Therefore, $|\overline{C_1}| \leq \varepsilon n/2c$ and hence $|C_1| > (1 - \frac{\varepsilon}{2c})n$. □

1.3.2 Expander Graphs.

The above discussion leads to the following definition of a certain class of graphs.

Definition 1.18. An (n,d)-*graph* is a d-regular graph of order n. An (n,d,c)-*expander graph* is an (n,d)-graph such that $\phi(G) \geq c$.

Remark 1.19. Every connected d-regular multigraph is an (n,d,c)-expander for some trivial $c \in (0,1]$, for instance we could take $c = \phi(G)$. However, the notion of interest is that of an infinite sequence of (n_i, d_i, c)-expanders with d_i's preferably small, c fixed, preferably as large as possible, and $n_i \to \infty$. In practice, one may want $d_i = d$ to be a fixed small number and sometimes $n_{i+1}/n_i \to 1$, in which case we say that the sequence of expanders is *linear*.

Definition 1.20. A *family of (constant-degree)* (d,c)-*expanders* is a family of multigraphs $\{G_n\}_{n=1}^{\infty}$ such that each G_n is a $(|G_n|, d, c)$-expander and $|G_n| \to \infty$.

Naturally, we want to describe the properties of an (n,d,c)-expander using its adjacency matrix A. There is a direct combinatorial property of the adjacency matrix that describes exactly an (n,d,c)-expander: as we have observed in Proposition 1.14, for the regularity of G, we want the unit vector $\mathbb{1}$ to be an eigenvector of G; for the edge expansion to be at least c we just want, for every vertex set $S \subseteq V$, to exist at least $cd \cdot |S|$ non-zero columns in A. However, this straightforward combinatorial property of the adjacency matrix A requires us to test all these $2^{\Omega(n)}$ possibilities. In fact, it turns out that determining the exact value of $\phi(G)$ is an **NP**-hard problem, see [BKV+81].

Surprisingly enough, there is a strong connection between the second largest eigenvalue of G and its edge expansion $\phi(G)$. This connection follows from Cheeger's inequalities, which are the discrete analogue of Cheeger's isoperimetric inequalities on compact Riemannian manifolds, proved by Cheeger [Che71] and Buser [Bus82]. The theorem below was proved by Dodziuk in [Dod84] and independently by N. Alon and V. D. Milan in [AM85] and [Alo86].

Theorem 1.21 (Cheeger's Inequalities)**.** *Let $\lambda_n \leq \cdots \leq \lambda_2 \leq \lambda_1 = d$ be the eigenvalues of G. Then, the following holds*

$$\frac{d-\lambda_2}{2d} \leq \phi(G) \leq \sqrt{\frac{2(d-\lambda_2)}{d}}.$$

The first inequality is known as the "easy direction", while the second as the "hard direction". Below we provide a proof of the easy direction of Cheeger's inequality and we refer the reader to [HLW06] for the a proof of the hard direction. It is interesting to note that the proof of the latter is algorithmic and makes use of the Spectral Partitioning Algorithm. This gives a set S of vertices of edge-expansion $\phi_G(S) = \mathcal{O}(\sqrt{\phi(G)})$.

Before we proceed to the proof of the easy direction it will be convenient for us to define the notion of *sparsity* of G. For a cut $(S, \overline{S})$ of G we define its *sparsity* as

$$\sigma(S) := \frac{e_G(S,\overline{S})}{\frac{d}{n}|S||\overline{S}|}.$$

Note that $\sigma(S) = \sigma(\overline{S})$. We thus define the *sparsity* of G as $\sigma(G) := \min_{\emptyset \subsetneq S \subsetneq V} \sigma(S)$. Note that for a subset $S \subseteq V$ with $1 \leq |S| \leq n/2$ we have that $1/2 \leq |\overline{S}|/n < 1$ and so $\sigma(S)/2 \leq \phi(S) \leq \sigma(S)$, which in turn implies that

$$\frac{\sigma(G)}{2} \leq \phi(G) \leq \sigma(G).$$

In particular, this tells as that the sparsity $\sigma(G)$ and the edge expansion $\phi(G)$ of a graph measure essentially the same thing.

Proof of Theorem 1.21 (Easy direction). We prove that

$$\frac{d-\lambda_2}{d} \leq \sigma(G),$$

which implies the desired result. By Proposition 1.14, we have that $\lambda_1 = d$ and that the unit vector $\mathbb{1}$ is an eigenvector for this eigenvalue. Thus, Theorem 1.12 implies that

$$\lambda_2 = \max_{x \in \langle \mathbb{1} \rangle^{\perp} \setminus \{0\}} \frac{x^T A x}{x \cdot x}.$$

Let now (S,T) be a cut of G and set $s := |S|$ and $t := |T| = n - s$. Consider the vector $x \in \mathbb{R}^V$ such that $x_v = -t$, for $v \in S$, and $x_v = s$, for $v \in T$, and observe that $x \perp \mathbb{1}$ and that

$$x \cdot x = \sum_{u \in S} t^2 + \sum_{u \in T} s^2 = st^2 + ts^2 = (t+s)st = nst. \tag{2}$$

Using Corollary 1.7 we compute the value $x^T A x$ for this specific vector as follows

$$x^T A x = \sum_{e \in E} x_{o(e)} x_{t(e)} = 2t^2 e(S) + 2s^2 e(T) - 2st \cdot e(S,T).$$

We need to get rid of the terms $e(S)$ and $e(T)$. In order to do this, consider the quantity $Q = \sum_{u \in S} \deg(u)$. On the one hand $Q = ds$ as G is d-regular and on the other $Q = \sum_{u \in S} \sum_{v \in V} A_{u,v} = \sum_{u,v \in S} A_{u,v} + \sum_{u \in S, v \in T} A_{u,v} = 2e(S) + e(S,T)$. Thus, $ds = 2e(S) + e(S,T)$. Similarly, we find that $dt = 2e(T) + e(S,T)$. Hence,

$$x^T A x = t^2(ds - e(S,T)) + s^2(dt - e(S,T)) - 2ste(S,T) = dstn - n^2 e(S,T) \tag{3}$$

Since $x \perp \mathbb{1}$, combining (2) and (3) we get that

$$\lambda_2 \geq R_A(x) = \frac{x^T A x}{x^T x} = \frac{dstn - n^2 e(S,T)}{nst} = d - d\frac{e(S,T)}{\frac{d}{n} st} = d - d \cdot \sigma(S)$$

and so $\frac{d-\lambda_2}{d} \leq \sigma(S)$. Result follows from the fact that (S,T) is an arbitrary cut of G.

□

Note 1.22. Both sides of the above inequality are essentially tight.

- Tight bound on the easy direction: The n-dimensional hypercube graph Q_n is the simple graph with vertex set $\{0,1\}^n$, where two vertices $x, y \in \{0,1\}^n$ are adjacent iff they differ at exactly 1 coordinate. This is clearly an n-regular graph and its spectrum is $\{2k - n \colon k = 1, \ldots, n\}\}$; so $\lambda_2(Q_n) = n - 2$. Now, for $k \in \{1, \ldots, n\}$ and for the cut $(S, \overline{S})$, where $S = \{x \in \{0,1\}^n \colon x_k = 0\}$, we have that

  $$\phi(Q_n) \leq \phi(S) = \frac{e(S,\overline{S})}{n|S|} = \frac{2^{n-1}}{n2^{n-1}} = \frac{1}{n},$$

  which attains the bound $\frac{n-\lambda_2(Q_n)}{2n} = \frac{2}{2n} = \frac{1}{n}$.

- Essentially tight bound for the hard direction: The n-cycle C_n is the simple graph with vertex set $\mathbb{Z}_n$, where two vertices $x, y \in \mathbb{Z}_n$ are adjacent if and only if $x - y = \pm 1$. Take n to be an even number. The graph C_n is clearly a 2-regular graph and it is easy to see that $S = \{x_1, \dots, x_{n/2}\}$ gives an optimal cut; hence

$$\phi(C_n) = \phi(S) = \frac{e(S, \overline{S})}{2|S|} = \frac{2}{2n/2} = \frac{2}{n} = \mathcal{O}(1/n).$$

  Now, the eigenvalues of C_n are of the form $\omega^k + \omega^{-k} = 2\cos(\frac{2\pi k}{n})$, for $k = 0, \dots, n-1$, where ω is a primitive n-th root of unity. Thus, $\lambda_2(C_n) = 2\cos(2\pi/n)$ and so using the Taylor expansion for the cos function we find that $\sqrt{\frac{2(2-\lambda_2(C_n))}{2}} = \sqrt{2 - 2\cos(2\pi/n)} = \mathcal{O}(1/n)$, as $1 - \cos(2\pi/n) = \mathcal{O}(1/n^2)$.

The quantity $d - \lambda_2(G)$, i.e. the difference of the largest and the second largest eigenvalue, is called the *spectral gap*. As it can be seen from Theorem 1.21, the edge expansion of G is large if and only if the spectral gap is large, or equivalently λ_2 is much smaller than d. More precisely, we have the following.

Corollary 1.23. *1. Any d-regular graph G on n vertices is an (n, d, c)-expander with $c = \frac{d-\lambda_2}{2d}$.*

2. If G is an (n, d, c)-expander then $d - \lambda_2 \geq dc^2/2$.

The above analysis suggests that in order to study the edge expansion $\phi(G)$ of a regular multigraph G we may study instead its second largest eigenvalue, or more generally the behavior of its eigenvalues.

Randomness of expanders. There are plenty results in the literature which suggest that expander graphs behave like random graphs. The main such result is the standard *Expander Mixing Lemma*, see [AC88]. Consider the following two random experiments on the d-regular graph G:

- Pick a vertex $u \in V$ and then pick a vertex $v \in V$ such that $u \sim v$.
- Pick independently two vertices $u, v \in V$.

Now consider two subsets $S, T \subseteq V$. What is the probability that $(u, v) \in S \times T$ in the above situations? In the first experiment the probability equals $\frac{1}{nd} e_G(S, T)$ and in the second one equals $\mu(S) \cdot \mu(T)$, where $\mu(S) := |S|/n$ and $\mu(T) := |T|/n$ is the *density* of S and T in G, respectively. Expander Mixing Lemma (Theorem 1.24) below shows that if G is a good expander, i.e. $\lambda_2(G)$ is small, by Corollary 1.23, these two probabilities are close to each other, which means that its edges are spread out, a hallmark of random graphs.

Theorem 1.24 (Expander Mixing Lemma)**.** *Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of G. For two sets $S, T \subseteq V$ we have*

$$\left| e(S, T) - \frac{d|S| \cdot |T|}{n} \right| \leq \lambda_2 \sqrt{|S| \cdot |T|}. \tag{4}$$

Proof. Let $\{x_1, \dots, x_n\}$ be an orthonormal basis of eigenvectors for $\mathbb{R}^V$ such that $Ax_i = \lambda_i x_i$ for each $i = 1, \dots, n$. By Proposition 1.14, we have that $\lambda_1 = d$ and we may assume that $x_1 = \frac{1}{\sqrt{n}}\mathbb{1}$. Consider now, the characteristic vectors $x_S, x_T \in \mathbb{R}^V$ of S, T, respectively. Note then that

$x_S^T A x_T = \sum_{v\in S, u\in T} A_{u,v} = e(S,T)$. Writing $x_S = \sum_{i=1}^n a_i x_i$ and $x_T = \sum_{i=1}^n b_i x_i$ we have that $a_1 = x_1 \cdot x_S = \frac{1}{\sqrt{n}}\mathbb{1} \cdot x_S = |S|/\sqrt{n}$ and similarly, $b_1 = |T|/\sqrt{n}$; hence,

$$e(S,T) = x_S^T A x_T = \sum_{1\le i,j\le n} a_i b_j x_i^T A x_j = \sum_{i=1}^n \lambda_i a_i b_i = d\frac{|S|\cdot|T|}{n} + \sum_{i=2}^n \lambda_i a_i b_i.$$

Therefore, by the Cauchy-Schwarz inequality we get

$$\left| e(S,T) - \frac{d|S|\cdot|T|}{n} \right| = \left| \sum_{i=2}^n \lambda_i a_i b_i \right| \le \lambda_2 \sum_{i=2}^n |a_i b_i| \le \lambda_2 \|x_S\| \cdot \|x_T\| = \lambda_2 \sqrt{|S|\cdot|T|}.$$

□

Note 1.25. The left hand-side of the inequality (4) measures the discrepancy between the number $e_G(S,T)$ of edges between the sets S, T in G and the expected number of edges between S and T in a random graph of edge density d/n, namely $\frac{d|S||T|}{n}$.

The Expander Mixing Lemma implies some significant results about the relation of the graph properties of a d-regular graph and its spectrum.

Corollary 1.26. *Let G be an (n,d)-graph with $\lambda_2(G) \le \lambda$.*

1. *The independence number of G satisfies $\alpha(G) \le \lambda n/d$.*
2. *The chromatic number of G satisfies $\chi(G) \ge d/\lambda$.*
3. *The diameter of G satisfies* $\operatorname{diam}(G) \le \left\lceil \frac{\log n}{\log(d/\lambda)} \right\rceil$.

Proof.

1. This follows from the fact that if $I \subseteq V(G)$ is an independent set, then $e(I,I) = 0$ and so the Expander Mixing Lemma implies the bound.
2. Let $c : V(G) \to \{1,\dots,k\}$ be a proper k-coloring of G. Then, by definition, each $c^{-1}(i)$, $1 \le i \le k$, is an independent set of G and so from the above we get that $n = \sum_{i=1}^k |c^{-1}(i)| \le k\lambda n/d$, which implies the bound.
3. For a proof see [HLW06].[(1)]

□

When $\lambda_2(G)$ is close to $\lambda_1(G) = d$, then the upper and the lower bound in Theorem 1.21 do not give an accurate approximation of the edge-expansion $\phi(G)$ of G; that means that a graph can be an excellent expander but still has a small spectral gap. The following theorem, which is also a converse of the Expander Mixing Lemma, provides a tighter approximation of λ_2, giving also another combinatorial description of it.

Theorem 1.27 (Converse of Expander Mixing Lemma, [BL06])**.** *Let $\alpha \in [0,d)$ be a constant. If for any disjoint vertex sets $S, T \subseteq V$ it holds that*

$$\left| e(S,T) - \frac{d|S|\cdot|T|}{n} \right| \le \alpha \sqrt{|S|\cdot|T|},$$

then, $\lambda_2 \le \mathcal{O}(\alpha(1+\log(d/\alpha))$. The bound is tight.

By Theorem 1.24 and Theorem 1.27, we see that λ_2 and α differ by at most a logarithmic factor, which makes this approximation better.

[(1)] We mention that this result was first proved by Chung in [Chu89].

1.3.3 Constructions of Expander Graphs.

In this section we describe, without proving, some known constructions of expander graphs mentioned in the introduction.

• **Margulis-Gaber-Galil Construction [GG81].** For every positive integer n we define the 8-regular multigraph G_n with vertex set $V_n = \mathbb{Z}_n \times \mathbb{Z}_n$ as follows: consider the linear transformations

$$T_1 = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

and connect each vertex $v = (x, y) \in V_n$ with $T_1 v, T_2 v, T_1 v + e_1, T_2 v + e_2, T_1^{-1} v, T_2^{-1} v, T_1^{-1} v - e_1, T_2^{-1} v - e_2$, were e_1, e_2 is the standard basis of the vector space $V_n = \mathbb{Z}_n \times \mathbb{Z}_n$. Gaber and Galil proved that this is a family of $(8, \frac{8-5\sqrt{2}}{16})$-expander multigraphs.

Note 1.28. The original definition of these graphs by Margulis [Mar73] differs a bit from the above on the linear transformations T_1 and T_2 but it is essentially the same. Let us also note that the graphs G_p, where p is a prime number, were originally derived as Cayley graphs on the group $\mathrm{SL}_3(\mathbb{F}_p)$.

• **Lubotzky-Phillips-Sarnak Construction [LPS88].** Let $p, q \equiv 1 \pmod 4$ be different prime numbers. Consider the Diophantine equation

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p.$$

To every integer solution $\alpha = (a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ to the above equation we associate a matrix

$$\tilde{\alpha} = \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Z}/q\mathbb{Z})$$

Consider then the set

$$S = \left\{ \tilde{\alpha} \colon \alpha = (a_0, a_1, a_2, a_3) \in \mathbb{Z}^4, \begin{array}{c} a_0^2 + a_1^2 + a_2^2 + a_3^2 = p, \\ a_0 > 0 \text{ odd}, \ a_1, a_2, a_3 \text{ even} \end{array} \right\}.$$

By Jacobi's 4-square Theorem it can be seen that the cardinality of S is exactly $p+1$. Moreover, it can be easily seen that S is a symmetric subset of $\mathrm{PGL}_2(\mathbb{Z}/q\mathbb{Z})$. Thus, we define the graphs $X^{p,q}$ as the Cayley graphs

$$X^{p,q} := \begin{cases} \Gamma(\mathrm{PSL}_2(\mathbb{Z}/q\mathbb{Z}), S), & \left(\frac{p}{q}\right) = 1 \\ \Gamma(\mathrm{PGL}_2(\mathbb{Z}/q\mathbb{Z}), S), & \left(\frac{p}{q}\right) = -1 \end{cases}$$

The graphs $X^{p,q}$ are $(p+1)$-regular connected graphs, with optimal expansion. This is an example of a Ramanujan graph, which we define in the next section.

• **Lubotzky Construction [Lub94].** For every prime p define the graph Y_p with vertex set $V(Y_p) = \mathbb{P}^1(\mathbb{Z}_p) = \mathbb{Z}_p \cup \{\infty\}$ and connect every vertex $x \in \mathbb{P}(\mathbb{Z}_p)$ to $x+1, x-1, -\frac{1}{x}$. Then, the sequence $\{Y_p\}_p$, indexed by the prime numbers, is a family of 3-regular expander graphs with $\lambda_2 < 1 - 1/10^4$.

• **Reingold-Vadhan-Wigderson Construction [RVW02].** We will demonstrate how this recursive construction works using their theorem about the properties of the zig-zag product, without

defining it. For an (n,k)-multigraph G and a (k,d)-multigraph H we denote their *zig-zag product* by $G(z)H$. Given a multigraph G, we also define the multigraph G^2 as the multigraph with adjacency matrix $A(G^2) = A(G)^2$, see Remark 1.4. Observe that if G is an (n,d)-multigraph then G^2 is an (n,d^2)-multigraph with second largest eigenvalue $\lambda_2(G^2) = \lambda_2(G)^2$. We will use the following theorem:

> **Theorem** (The Zig-Zag Theorem, [RVW02])**.** Let G be an (n,k)-multigraph with $\lambda_2(G)/d \leq \alpha$ and H be a (k,d)-multigraph with $\lambda_2(H)/d \leq \beta$. Then, the zig-zag product $G(z)H$ is an (nk,d^2) with $\lambda_2(G(z)H)/d \leq \alpha + \beta + \beta^2$.

So, take a (d^4,d)-multigraph H with $\lambda_2(H)/d \leq 1/5$ and define recursively the sequence (G_n) as follows:

$$G_1 := H^2 \qquad \text{and} \qquad G_{n+1} = (G_n)^2 (z) H.$$

This is a family of $(d^2, 1/4)$-expander multigraphs. First note that each zig-zag product is well-defined, since each $(G_n)^2$ has degree d^4 which equals the order of H, and that each G_n has order d^{4n}. To prove that $\phi(G_n) \geq 1/4$, we need to prove that $\lambda_2(G_n) \leq d/2$. This follows by induction and the Zig-Zag Theorem as

$$\lambda_2((G_n)^2 (z) H)/d \leq 1/2^2 + 1/5 + 1/5^2 = 49/100 < 1/2.$$

Note 1.29. In the case where the graphs are Cayley, the notion of the zig-zag product is related to that of the semi-direct product of groups, see [ALW01].

1.4 Ramanujan Graphs.

As we have established in the previous sections, see Corollary 1.23, in order to study expanders we may study their spectrum. Thus, the natural question now to ask is:

- *Question:* How large can the spectral gap of an (n,d,c)-expander be?

If we allow our graphs to be infinite then the infinite d-regular tree, denoted by $\mathbf{T}^d$, see Figure 2, provides the answer and in a way it is the "ultimate" expander (although it is a tree), as we will see below.

In order to define $\mathbf{T}^d$ we construct it from a finite d-regular multigraph G as follows. let $v \in V(G)$ and define $V(\mathbf{T}^d)$ to be the set of w.b. walks in G starting at v. Two vertices $w, w' \in V(\mathbf{T}^d)$ are adjacent if and only if there exists an edge $e \in E(G)$ such that w' occurs from w by concatenating e, that is w' is a single step extension of w. It is easy to see that this construction is independent of the vertex v and that the obtained graph is an infinite d-regular connected acyclic graph; thus it is indeed $\mathbf{T}^d$.

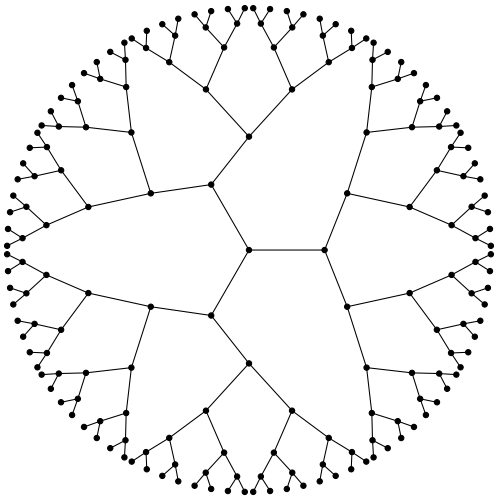

Figure 2: The infinite 3-regular tree.

Note 1.30. Obviously there is a more direct combinatorial way to define the infinite d-regular tree $\mathbf{T}^d$ but this way enables us to realise it as the universal cover of every d-regular multigraph, which will play an essential role in the proof of Theorem 1.34.

In the case of an infinite graph G we generalize the edge expansion as

$$\phi(G) := \inf_{\substack{S \subseteq V \\ |S| < \infty}} \frac{e_G(S, \overline{S})}{d|S|}.$$

So to compute $\phi(\mathbf{T}^d)$ consider a finite subset $S \subseteq V(\mathbf{T}^d)$. The induced subgraph, denoted by $\mathbf{T}^d[S]$, from S in $\mathbf{T}^\mathbf{d}$ can be assumed to be connected, since it can be seen that otherwise it wouldn't minimize the above fraction. Thus, $\mathbf{T}^d[S]$ is a finite tree and so $|E(\mathbf{T}^d[S])| = |S| - 1$. Hence, $e(S, \overline{S}) = |S|d - 2(|S| - 1) = |S|(d-2) + 2$ and therefore,

$$\phi(\mathbf{T}^d) = \lim_{k \to \infty} \left(\frac{d-2}{d} + \frac{2}{k} \right) = \frac{d-2}{d}.$$

Thus, indeed $\mathbf{T}^d$ serves the role of the "ultimate expander", as it has the maximum expansion. Let us examine next its spectrum.

For the spectrum of $\mathbf{T}^d$, let $A_\mathbf{T}$ be its (infinite) adjacency matrix and consider it as a linear operator on the space $L^2(\mathbf{T}^d) = \{f : V(\mathbf{T}^d) \to \mathbb{C} \colon \sum_x |f(x)|^2 < \infty\}$. Then, as above, we generalize the spectrum of an infinite graph as

$$\operatorname{spec}(A_\mathbf{T}) := \left\{ \lambda \in \mathbb{C} \colon (A_\mathbf{T} - \lambda \operatorname{id}) \in L^2(\mathbf{T}^d) \text{ is non-invertible} \right\}.$$

Equivalently, $\lambda \in \operatorname{spec}(A_\mathbf{T})$ if and only if the operator $\ker(A_\mathbf{T} - \lambda \operatorname{id}) \neq 0$.

Theorem 1.31 (Cartier, [Car72])**.** *The spectrum of $A_\mathbf{T}$ is the closed interval*

$$\operatorname{spec}(A_\mathbf{T}) = [-2\sqrt{d-1}, 2\sqrt{d-1}].$$

For a proof of Theorem 1.31 we also refer to [Fri91]. The fact that $\mathbf{T}$ is the universal cover of d-regular graphs together with the $2\sqrt{d-1}$ for its spectrum will give us the asymptotic bound $2\sqrt{d-1}$ for finite graphs too.

Now, we return to finite d-regular multigraphs and ask again how large can the spectral gap be, or more generally is there an (asymptotic) bound for their non-trivial spectrum? By non-trivial spectrum of a d-regular multigraph G, we mean the set of the eigenvalues of G different from $\pm d$, see Proposition 1.14. For that purpose we define the parameter

$$\lambda(G) := \max\{|\lambda| \colon \lambda \in \operatorname{spec}(G), \lambda \neq \pm k\}.$$

Note 1.32. By Proposition 1.14, for a connected d-regular multigraph G, we have that $\lambda(G) = \max\{|\lambda_2|, |\lambda_{n-1}|\}$, if G is bipartite, and $\lambda(G) = \max\{|\lambda_2|, |\lambda_n|\}$, if G is not bipartite.

Observe that if $\lambda(G)$ is small then so is $\lambda_2(G)$. Our purpose is to bound $\lambda(G)$ asymptotically, that is as the order of G goes to infinity. In order to do this, we will approximate a d-regular graph, specifically its eigenvalues, by $\mathbf{T}^d$, interpreting it as its universal cover.

So, consider a d-regular multigraph G and interpret both G and $\mathbf{T}^d$ as 1-dimensional CW-complexes. Then, the map $p : \mathbf{T}^d \to G$ sending a walk $w \in V(\mathbf{T}^d)$ to its end-vertex defines a covering map. This is easy to see as for each vertex $w \in V(T^d)$, the restriction map $p|_{N_{\mathbf{T}^d}(w)} : N_{\mathbf{T}^d}(w) \to N_G(p(w))$ is a bijection. See [HLW06] for a more concrete analysis. Now, the fact that $\mathbf{T}^d$ is a tree is equivalent to the fact that $\mathbf{T}^d$ is simply connected as a CW-complex. Thus, we've established the following.

Proposition 1.33. *The infinite d-regular tree $\mathbf{T}^d$ is the universal cover of every d-regular multigraph.*

Theorem 1.34 below employs Proposition 1.33 and uses the path-lifting property of covering spaces to achieve an asymptotic lower bound on $\lambda(G)$. The result below was first proven by Alon and Boppana [Alo86], and has been proved in many ways since, see for example [LPS88, Piz98, Nil91, HLW06, Ser97, Lub94]. Here we follow the proof of [LPS88].

Theorem 1.34 (Alon-Boppana bound)**.** *Let $\{G_n\}_{n=1}^{\infty}$ be a sequence of connected d-regular multigraphs such that $|G_n| \to \infty$. Then,*

$$\liminf_{n\to\infty} \lambda(G_n) \geq 2\sqrt{d-1}.$$

Proof. We assume, without loss of generality, that for each $n \in \mathbb{Z}_{\geq 1}$, $|G_n| = n$. By Proposition 1.13, we have that the number of closed walks in G_n of length $2l$ is equal to

$$\operatorname{tr}(A(G_n)^{2l}) = \sum_{v \in V(G_n)} A(G_n)^{2l}_{v,v} = \sum_{i=1}^{n} \lambda_i^{2l}(G_n),$$

where by the discussion on (1.1), $A(G_n)^{2l}_{v,v}$ is equal to the number of closed walks in G_n from v to v of length $2l$. Denote then by t_l the number of closed walks in $\mathbf{T}^d$ from a certain vertex $x \in V(\mathbf{T}^d)$ to itself of length $2l$ (note that t_l is independent of the particular vertex x). Then, since $\mathbf{T}^d$ is the universal cover of G_n, by Proposition 1.33, we have that for each $v \in V(G_n)$, $A(G_n)^{2l}_{v,v} \geq t_l$ and so

$$\sum_{i=1}^{n} \lambda_i^{2l}(G_n) \geq n t_l.$$

Now, by Proposition 1.14, we have that $\lambda_1(G_n) = d$ and $\lambda_n(G_n) \geq -d$, thus we find that

$$2d^{2l} + (n-2)\lambda(G_n)^{2l} \geq 2d^{2l} + \sum_{i=2}^{n-1} \lambda_i^{2l}(G_n) \geq nt_l \geq (n-2)t_l,$$

which in turn implies that

$$\lambda(G_n)^{2l} \geq t_l - \frac{2d^{2l}}{n-2}. \tag{5}$$

We compute the number t'_l of closed walks in $\mathbf{T}^d$ from a certain vertex x to itself of length $2l$ that visits x exactly 2 times. It is easy to see that $t'_l = dk_{l-1}$, where k_l denotes the number of closed walks in $\mathbf{T}_y^{d-1}$, the infinite complete $(d-1)$-ary rooted sub-tree of $\mathbf{T}^d$ with root y, from y to itself of length $2l$. Thus, we have to compute the number k_l. To do this we find a recurrence relation for k_l. Observe that to make such a closed walk we have first to pass through a neighbor z of the root y, then make a closed walk in $\mathbf{T}_z^{d-1}$ from z to itself of length $2i$, then return to y, and then make again a closed walk in $\mathbf{T}_y^{d-1}$ from y to itself of length $2l-2i-2 = 2(l-i-1)$. Thus, we find that

$$k_0 = 1 \qquad \text{and} \qquad k_{l+1} = (d-1)\sum_{i=0}^{l} k_i k_{l-i}.$$

Now, it is easy to see that the sequence $C_l = k_l/(d-1)^l$ satisfies the recurrence relation $C_{l+1} = \sum_{i=0}^{l} C_i C_{l-i}$ with $C_0 = 1$, which is exactly the recurrence relation defining the Catalan numbers $C_l = \frac{1}{l+1}\binom{2l}{l}$, see [Sta15]. Hence, $k_l = \frac{1}{l+1}\binom{2l}{l}(d-1)^l$ and so

$$t'_l = d(d-1)^{l-1}\frac{1}{l}\binom{2l-2}{l-1}.$$

Obviously, $t_l \geq t'_l$ and therefore we get from (5) that

$$\lambda(G_n)^{2l} \geq \left(\sqrt{d-1}\right)^{2l}\frac{1}{l}\binom{2l-2}{l-1} - \frac{2d^{2l}}{n-2}.$$

Result follows from that fact that $\binom{2l}{l}^{1/2l} \xrightarrow{l\to\infty} 2$. □

Note 1.35. 1. For tighter estimates for the bound on $\lambda(G)$ see [HLW06] and [Nil91], where it is proved that

$$\lambda(G) \geq 2\sqrt{d-1}(1 - \mathcal{O}(1/\Delta)),$$

where $\Delta = \operatorname{diam}(G)$ is the diameter of G.

2. It is worth mentioning a quantitative variation of Theorem 1.34 by J.-P. Serre, who is also considered as the originator of the following theorem.

> **Theorem** (J.-P. Serre, [Ser97])**.** For every $\epsilon > 0$ and every integer $d > 0$ there is a constant $c = c(\epsilon, d) > 0$, such that for every (n,d)-graph the number of eigenvalues λ with $\lambda > (2-\epsilon)\sqrt{d-1}$ is at least $c \cdot n$.

This essentially tells that for every $\epsilon > 0$ every (n,d)-graph has a positive proportion of eigenvalues larger than $2\sqrt{d-1} - \epsilon$ and thus implies the Alon-Boppana bound. For a proof of this theorem of Serre see also [HLW06].

Motivated by the above analysis and Theorem 1.34 we define a specific kind of expanders, which attain the Alon-Boppana bound.

Definition 1.36. A d-regular graph is said to be a *Ramanujan graph* if $\lambda(G) \leq 2\sqrt{d-1}$.

To put it differently, according to Theorem 1.31, a d-regular graph G is Ramanujan if its non-trivial eigenvalues lie in the spectrum of its universal cover. In view of Theorem 1.34 and Theorem 1.21, Ramanujan (multi)graphs are the optimal expander graphs.

Note 1.37. As in the case of expanders (see Remark 1.19), we are interested in sequences of constant-degree Ramanujan multigraphs such that their orders tend to ∞, i.e. sequences $\{G_n\}_{n\geq 1}$ of d-regular multigraphs such that $\lambda(G_n) \leq 2\sqrt{d-1}$ and $|G_n| \to \infty$.

We conclude this section by stating an open problem about Ramanujan graphs.

- *Open Problem.* Lubotzky in Problem 10.7.3 of his book [Lub94] asked whether infinite families of d-regular Ramanujan graphs exist for every degree $d > 2$. Until 2013, the only known infinite Ramanujan graph families remained to be of degree $q + 1$, for some prime power $q = p^r$, [LPS88, Chi92, Mor94]. Marcus, Spielman, and Srivastava in their breakthrough paper [MSS15] proved Lubotzky's conjecture true by proving the existence of infinite families of bipartite Ramanujan graphs for every degree $d > 2$. They did it by proving the signing conjecture of Bilu and Linial, who suggested in [BL06], a way of constructing Ramanujan graphs through a sequence of 2-*lifts*, which are just 2-fold covering graphs, of a base Ramanujan graph. However, their construction uses a probabilistic result about 2-lifts and does not provide an explicit construction. It remains yet an open problem to make an explicit construction of Ramanujan of arbitrary degrees.

2 Arithmetic of Quaternion Algebras

For the following notions we refer to [AM69] and [Voi21]. All rings considered in this text will be associative and contain a multiplicative identity 1. Every ring-homomorphism preserves 1 and every subring of a ring contains the same 1. Throughout the section every ring R will be assumed to be a PID and every field $\mathbb{F}$ will be of $\mathrm{char}\mathbb{F} \neq 2$, unless we mention otherwise. Fix also an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$.

The *center* of a ring R is the subring of R defined by

$$Z(R) := \{r \in R \colon \forall s \in R \ (rs = sr)\}.$$

An $\mathbb{F}$-*algebra* is a ring A equipped with a ring-homomorphism $\phi : \mathbb{F} \to A$ such that $\operatorname{im}\phi \subseteq Z(A)$. An $\mathbb{F}$-algebra A is said to be *central* of $Z(A) = \mathbb{F}$. An $\mathbb{F}$-algebra homomorphism (or just an $\mathbb{F}$-*homomorphism*, $\phi : A_1 \to A_2$ between two algebra $\phi_1 : \mathbb{F} \to A_1$ and $\phi_2 : \mathbb{F} \to A_2$ is a ring homomorphism that commutes with the action of $\mathbb{F}$ into A_1 and A_2, i.e. that $\phi \circ \phi_1 = \phi_2$. An $\mathbb{F}$-algebra A is said to be a *division algebra* if every non-zero element $a \in A$ has a two-sided inverse, i.e. there exists $b \in A$ such that $ab = ba = 1$. We call A *simple* if the only two-sided ideals of A are $\{0\}$ and A.

2.1 Quaternion Algebras

Definition 2.1. A *quaternion algebra* B is an $\mathbb{F}$-algebra that is generated as an $\mathbb{F}$-algebra by two elements $i, j \in B$ satisfying the following relations

$$i^2 = a, j^2 = b, \text{ and } ij = -ji, \tag{6}$$

for some $a, b \in \mathbb{F}^\times$. We denote this quaternion algebra by $\left(\frac{a,b}{\mathbb{F}}\right)$ and we call the generators i, j which satisfy the relations (6) *standard generators* with respect to a, b.

Note 2.2. Given a quaternion algebra $B = \left(\frac{a,b}{\mathbb{F}}\right)$, where $a, b \in \mathbb{F}^\times$, with standard generators i, j, one can see, via direct calculations, that the elements $1, i, j, ij$ are $\mathbb{F}$-linearly independent [Voi21, Lemma 2.2.5] and so the quaternion algebra $B = \left(\frac{a,b}{\mathbb{F}}\right)$ can be equivalently defined as an $\mathbb{F}$-algebra generated as an $\mathbb{F}$-vector space by $1, i, j, k := ij$, satisfying (6). Using the relations (6) between i and j, we can calculate the multiplication table of the generators which is given as follows:

	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

Figure 3: Multiplication table for the quaternion algebra $\left(\frac{a,b}{\mathbb{F}}\right)$.

Examples 2.3. 1. The $\mathbb{F}$-algebra $M_2(\mathbb{F})$ of 2×2 matrices with entries in $\mathbb{F}$ is a quaternion algebra isomorphic to $\left(\frac{1,1}{\mathbb{F}}\right)$ and is generated by the matrices $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

2. The quaternion algebra $\mathbb{H} := \left(\frac{-1,-1}{\mathbb{R}}\right)$ is called *Hamilton's quaternions* and is the unique division quaternion algebra over $\mathbb{R}$, as we will prove in Corollary 2.5.

Proposition 2.4. *Let $a, b \in \mathbb{F}^\times$. Then, the following hold:*

1. $\left(\frac{a,b}{\mathbb{F}}\right) \simeq \left(\frac{b,a}{\mathbb{F}}\right)$;
2. $\left(\frac{a,b}{\mathbb{F}}\right) \simeq \left(\frac{a,-ab}{\mathbb{F}}\right) \simeq \left(\frac{b,-ab}{\mathbb{F}}\right)$;
3. $\left(\frac{a,b}{\mathbb{F}}\right) \otimes_{\mathbb{F}} \mathbb{K} \simeq \left(\frac{a,b}{\mathbb{K}}\right)$ *for every field extension* $\mathbb{K}/\mathbb{F}$;
4. $\left(\frac{a,b}{\mathbb{F}}\right) \simeq \left(\frac{ax^2,by^2}{\mathbb{F}}\right)$ *for every* $x, y \in \mathbb{F}^\times$;
5. $\left(\frac{1,b}{\mathbb{F}}\right) \simeq M_2(\mathbb{F})$.

Proof. The isomorphisms in (1) and (2) are just given by permutation of the generators as one can see by Figure 3. (3) is obvious. For (4) let i and j be standard generators of $B = \left(\frac{a,b}{\mathbb{F}}\right)$ and i', j' be standard generators of $B' := \left(\frac{ax^2,by^2}{\mathbb{F}}\right)$. Then, the map $B' \to B$ induced by

$$B' \to B; \qquad i' \mapsto ix, \quad j' \mapsto jy$$

is an isomorphism. For (5), let i, j be standard generators of $B = \left(\frac{1,b}{\mathbb{F}}\right)$. Then, the map $\phi : B = \left(\frac{1,b}{\mathbb{F}}\right) \to M_2(\mathbb{F})$ induced by

$$B \to M_2(\mathbb{F}); \qquad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

is an isomorphism. □

Since, now $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$ and $\mathbb{F}^\times/\mathbb{F}^{\times 2} = \{1\}$, for an algebraically closed field $\mathbb{F}$, Proposition 2.4(4,5) have the following consequence, that classifies the quaternion algebras over $\mathbb{R}$ and $\mathbb{F}$.

Corollary 2.5. *Let $B = \left(\frac{a,b}{\mathbb{F}}\right)$ be a quaternion algebra over $\mathbb{F}$ with $a, b \in \mathbb{F}^\times$.*

1. *If $\mathbb{F} = \mathbb{R}$ then $B \simeq M_2(\mathbb{R})$ or $B \simeq \mathbb{H}$.*
2. *If $\mathbb{F}$ is algebraically closed then $B \simeq M_2(\mathbb{F})$.*

Reduced norm and trace. Let $B = \left(\frac{a,b}{\mathbb{F}}\right)$ be a quaternion algebra, where $a, b \in \mathbb{F}^\times$. Let $\alpha = t + xi + yj + zk \in B$. We define its *quaternion conjugate* as $\overline{\alpha} = t - xi - yj - zk$. The map

$$\bar{\cdot} : B \longrightarrow B; \qquad \alpha \mapsto \overline{\alpha} \tag{7}$$

is a *standard involution* in the sense that it satisfies the properties of the following proposition.

Proposition 2.6. *The quaternion conjugation (7) is an $\mathbb{F}$-linear map satisfying the following properties:*

1. $\overline{1} = 1$;

2. $\overline{\overline{\alpha}} = \alpha$ *for all* $\alpha \in B$;

3. $\overline{\alpha\beta} = \overline{\beta}\ \overline{\alpha}$ *for all* $\alpha, \beta \in B$;

4. $\alpha\overline{\alpha} = \overline{\alpha}\alpha \in \mathbb{F}$ *for all* $\alpha \in B$.

Proof. The proof follows from straightforward calculations, see [Voi21, 3]. □

Definition 2.7. Let V be a finite-dimensional $\mathbb{F}$-algebra. An $\mathbb{F}$-linear map $V \to V$ satisfying the properties (1)-(3) of Proposition 2.6 is called an *involution* and if it further satisfies (4) it is called a *standard involution*.

Note 2.8. If $\bar{\cdot} : B \longrightarrow B$ is a standard involution, then for all $\alpha \in B$ we have that $\alpha\overline{\alpha} \in \mathbb{F}$, by Proposition 2.6 and moreover we have that $\alpha + \overline{\alpha} \in \mathbb{F}$. Indeed, this follows from the formula

$$(\alpha + 1)\overline{(\alpha + 1)} = (\alpha + 1)(\overline{\alpha} + 1) = \alpha\overline{\alpha} + \alpha + \overline{\alpha} + 1, \tag{8}$$

since $(\alpha + 1)\overline{(\alpha + 1)}, \alpha\overline{\alpha}, 1 \in \mathbb{F}$.

We define the *reduced norm* and *reduced trace* of an element $\alpha = t + xi + yj + zk \in B$ as follows:

$$\begin{aligned} \mathrm{trd}(\alpha) &:= \alpha + \overline{\alpha} = 2t \in \mathbb{F} \\ \mathrm{nrd}(\alpha) &:= \alpha\overline{\alpha} = \overline{\alpha}\alpha = t^2 - ax^2 - by^2 + abz^2 \in \mathbb{F}. \end{aligned}$$

Note that, by Proposition 2.6, the reduced trace map $\mathrm{trd} : B \to \mathbb{F}$ is $\mathbb{F}$-linear and the reduced norm map is multiplicative. More precisely, in (5.1.4), we will see that the reduced norm defines a quadratic form over B

Remark 2.9. Let $\alpha \in B$. Observe that α satisfies the polynomial

$$x^2 - \mathrm{trd}(\alpha)x + \mathrm{nrd}(\alpha) \in \mathbb{F}[x]. \tag{9}$$

This is called the *reduced characteristic polynomial* of α and is the minimal polynomial of α, if $\alpha \in B \setminus \mathbb{F}$.

Example 2.10. Let $B = M_2(\mathbb{F})$. The *adjugate map*

$$\mathrm{adj} : B \longrightarrow B; \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \mathrm{adj}(A) := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

defines a standard involution on B. Note that by Lemma 2.11, this is the unique standard involution on B and so the reduced trace and norm in the matrix quaternion algebra $M_2(\mathbb{F})$ coincide with the usual trace and determinant.

Structure of quaternion algebras. There is a non-explicit definition of quaternion algebras, which, due to its more abstract nature, provides a further understanding of the notion and is sometimes more useful than the explicit one with generators. First, we prove that a standard involution in a quaternion algebra is unique.

Lemma 2.11. *Let B be a quaternion algebra. Then, the quaternion conjugation*

$$\alpha = t + xi + yj + zk \mapsto \overline{\alpha} = t - xi - yj - zk$$

is the unique standard involution on B.

Proof. Let $B \ni \alpha \mapsto \tilde{\alpha} \in B$ be a standard involution on B. Since a standard involution is $\mathbb{F}$-linear, it is enough to prove that $\tilde{i} = -i$, $\tilde{j} = -j$, and $\tilde{k} = -k$. We just prove it for i. We have that $i^2 = a \in \mathbb{F}$ and that i satisfies the characteristic polynomial (9), i.e. it holds that $a = i^2 = \mathrm{trd}(i)i - \mathrm{nrd}(i)$, where $\mathrm{nrd}(i), \mathrm{trd}(i) \in \mathbb{F}$, see (8). From the uniqueness of writing an element in B in terms of the basis elements, we get that $\mathrm{trd}(i) = i + \tilde{i} = 0$ and so $\tilde{i} = -i$, as desired. □

Theorem 2.12. *Let V be a division $\mathbb{F}$-algebra such that every element $\alpha \in B \setminus \mathbb{F}$ satisfies a polynomial of degree 2. Then, one of the following holds:*

1. *$V = \mathbb{F}$;*
2. *$V = K$ is a quadratic field extension of $\mathbb{F}$; or*
3. *$V = B$ is a division quaternion algebra over $\mathbb{F}$.*

Proof. See [Voi21, 3.5.1]. □

We state the following theorem due to J. Wedderburn and E. Artin in order to use to prove the equivalent characterization of quaternion algebras. For a proof of Theorem 2.13 see [Voi21, 7.1.1].

Theorem 2.13 (Wedderburn-Artin)**.** *Let B be a finite-dimensional $\mathbb{F}$-algebra. Then, B is simple if and only if $B \simeq M_n(D)$, where $n \geq 1$ and D is a finite-dimensional division $\mathbb{F}$-algebra.*

For a more elementary proof of the following corollaries, namely 2.15 and 2.14, without referring to Theorem 2.13, see [Voi21, Corollary 7.1.2].

Corollary 2.14. *Let B be an $\mathbb{F}$-algebra. Then, the following are equivalent:*

1. *B is a quaternion algebra over $\mathbb{F}$;*
2. *$B \otimes_{\mathbb{F}} \overline{\mathbb{F}} \simeq M_2(\overline{\mathbb{F}})$; and*
3. *B is a central simple $\mathbb{F}$-algebra of dimension $\dim_{\mathbb{F}} B = 4$.*

Proof. (1) $\implies$ (2). This follows from Proposition 2.4(3) and Corollary 2.5(2).

(2) $\implies$ (3): By Examples 2.3 one can see that $M_2(\overline{\mathbb{F}})$ is a central simple $\mathbb{F}$-algebra of dimension 4. We prove that this also holds for B. First, it is straightforward to check that $Z(B) = Z(B \otimes_{\mathbb{F}} \overline{\mathbb{F}}) \cap B = \mathbb{F} \cap B = \mathbb{F}$ and so B is central. Now, if $I \subseteq B$ is a non-zero two-sided ideal of B then $I \otimes_{\mathbb{F}} \overline{\mathbb{F}}$ is a non-zero two-sided ideal of $B \otimes_{\mathbb{F}} \overline{\mathbb{F}}$ and so $I \otimes_{\mathbb{F}} \overline{\mathbb{F}} = B \otimes_{\mathbb{F}} \overline{\mathbb{F}}$. By intersecting with B, the latter implies that $I = B$ and so B is simple. To conclude, we have that $\dim_{\mathbb{F}} B = \dim_{\overline{\mathbb{F}}} B \otimes_{\mathbb{F}} \overline{\mathbb{F}} = \dim_{\overline{\mathbb{F}}} M_2(\overline{\mathbb{F}}) = 4$.

(3) $\implies$ (1): Suppose that B is a central simple algebra of dimension $\dim_{\mathbb{F}} B = 4$. By the proof of Corollary 2.15 we get that $B \simeq M_2(\mathbb{F})$ or B is a division ring. If $B \simeq M_2(\mathbb{F})$ then it is a quaternion algebra, so suppose that B is a division ring. Let now $\alpha \in B \setminus \mathbb{F}$ and consider the subalgebra $\mathbb{F}[\alpha]$ of B generated by α. Then, $\mathbb{F}[\alpha]$ is a commutative subalgebra of the 4-dimensional division ring B. Thus, $\mathbb{F}[\alpha]$ is a field, $\mathbb{F}[\alpha] \neq B$, and $\dim_{\mathbb{F}} \mathbb{F}[\alpha] = 1, 2$, or 3. But we have that

$$[B : \mathbb{F}[\alpha]] \cdot [\mathbb{F}[\alpha] : \mathbb{F}] = [B : \mathbb{F}] = \dim_{\mathbb{F}} B = 4$$

and so $\dim_{\mathbb{F}} \mathbb{F}[\alpha] = [\mathbb{F}[\alpha] : \mathbb{F}] = 1$ or 2. Since $\alpha \in B \setminus \mathbb{F}$ we conclude that $\dim_{\mathbb{F}} \mathbb{F}[\alpha] = 2$. This implies that every elements $\alpha \in B \setminus \mathbb{F}$ satisfies a polynomial of degree 2 and so we may apply Theorem 2.12 to conclude that B is a quaternion algebra. □

Corollary 2.15. *A quaternion algebra B is either a division ring or isomorphic to $B \simeq M_2(\mathbb{F})$.*

Proof. By Corollary 2.14, we have that B is a simple algebra and so by Theorem 2.13, it follows that $B \simeq M_n(D)$, for some division $\mathbb{F}$-algebra D. Comparing dimensions we get the equality $4 = \dim_{\mathbb{F}} B = n^2 \dim_{\mathbb{F}} D$. Hence, either $n = 1$, in which case $B \simeq D$ is a division algebra or $n = 2$ and $\dim_{\mathbb{F}} D = 1$, in which case $D \simeq \mathbb{F}$ and $B \simeq M_2(\mathbb{F})$. □

2.2 Lattices and Orders

Fix a PID R, $\mathbb{F} := \mathrm{Frac}(R)$ be the fraction field of R, and let B be a quaternion algebra over $\mathbb{F}$. We start the arithmetic theory of quaternion algebras by defining and examining the naturally arising integral structures inside B.

Definition 2.16. An *R-lattice* in B is a finitely-generated R-submodule I of $\mathbb{F}$ such that the natural map $I \otimes_R \mathbb{F} \to B$ is an isomorphism.

Remark 2.17.

- We will abbreviate the notation by writing $I \otimes_R \mathbb{F} = B$. Note also that this condition is equivalent to the fact that I contains an $\mathbb{F}$-basis of B. Indeed, if the natural map $I \otimes_R \mathbb{F} \to B$ is an isomorphism then we can write every element of a given basis of B as an $\mathbb{F}$-linear combination of elements of I, which elements give another basis of B.

  Moreover, note that by the non-commutative analogue of [AM69, Proposition 3.5], we have that $B = I \otimes_R \mathbb{F} = (R \setminus \{0\})^{-1} I := \{x/r \colon x \in I, r \in R \setminus \{0\}\}$.

- If R is a PID then by the structure theorem for finitely-generated modules over a PID we get that every R-lattice in B is of the form

$$I = Rx_1 \oplus Rx_2 \oplus Rx_3 \oplus Rx_4,$$

  where $\{x_1, x_2, x_3, x_4\}$ is an $\mathbb{F}$-basis for B. Indeed, B has no torsion elements as it is an $\mathbb{F}$-algebra and so I has neither, as $I \subseteq B$. Thus, I is a torsion-free R-module. Since R is a PID we get that I is free. The result follows from the fact that $I \otimes_R \mathbb{F} = B$.

Lemma 2.18 (Lattice criterion)**.** *Let $I \subseteq B$ be an R-lattice and let $J \subseteq B$ be a finitely generated R-submodule. Then, the following hold:*

1. *For every $x \in B$ there exists $r \in R \setminus \{0\}$ such that $rx \in I$.*
2. *There exists $r \in R \setminus \{0\}$ such that $rJ \subseteq I$.*
3. *J is an R-lattice if and only if there exists $r \in R \setminus \{0\}$ such that $rI \subseteq J \subseteq r^{-1}I$.*

Proof. 1. By Remark 2.17, we have that I contains an $\mathbb{F}$-basis $\{x_1, \dots, x_4\}$ of B and so $R_1x_1 \oplus \cdots \oplus R_nx_4 \subseteq I$. So, let $x \in B$. Writing $x = a_1x_1 + \cdots + a_4x_4$, for some $a_i = \frac{r_i}{s_i} \in \mathbb{F}$, we get that $x = \frac{1}{s}(r_1x_1 + \cdots + r_4x_4)$, where $s = s_1s_2s_3s_4 \in R \setminus \{0\}$.

2. Let J be R-generated by the set $\{y_1, \dots, y_n\} \subseteq J \subseteq B$. By (1) we get that for each $i = 1, \dots, n$, there exists $r_i \in R \setminus \{0\}$ such that $r_i y_i \in I$; hence for $r = r_1 \cdots r_n \in R \setminus \{0\}$ we have that $rJ \subseteq I$.

3. If J is an R-lattice then (since also I is an R-lattice), by (2), we have that there exist $r, s \in R \setminus \{0\}$ such that $rJ \subseteq I$ and $sI \subseteq J$. Then, $rs \neq 0$ and

$$(rs)I \subseteq rJ \subseteq I \subseteq s^{-1}J \subseteq s^{-1}r^{-1}I = (rs)^{-1}I.$$

Conversely, if there exists $r \in R \setminus \{0\}$ such that $rI \subseteq J \subseteq r^{-1}I$, then tensoring with $\mathbb{F}$ we get

$$B = rB = rI \otimes_R \mathbb{F} \subseteq J \otimes_R \mathbb{F} \subseteq r^{-1}I \otimes_R \mathbb{F} = r^{-1}B = B$$

and hence the equality $J \otimes_R \mathbb{F} = B$.

□

Just like the commutative case we define the notion of an order, which appears to be as important in this context as in the commutative case for number fields, though (naturally) their structure is much more complicated. For an extensive exposition of orders we refer to [Rei75].

Definition 2.19. An R-order $\mathcal{O}$ in B is an R-lattice that is also a subring of B.

Note 2.20. Note that $1 \in \mathcal{O}$ or equivalently, $R \subseteq \mathcal{O}$.

Examples 2.21. 1. The R-algebra $M_2(R)$ is an R-order in the quaternion algebra $M_2(\mathbb{F})$.

2. Let B be a quaternion algebra generated by $i, j \in B$. Then, the R-lattice

$$\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rk$$

is an R-order in B, Indeed, by Figure 3 one can check that $\mathcal{O}$ is closed under multiplication of each 2 of its generators.

Lemma 2.22. *Let I be an R-lattice in B such that $1 \in I$. Then, the following hold:*

1. *$I \cap \mathbb{F} = R$;*
2. *I has an R-basis containing 1.*

In particular, an R-order $\mathcal{O}$ has a basis containing 1.

Proof. 1. Since $1 \in I$, we have that $R \subseteq I \cap \mathbb{F}$. Now, let $\alpha \in I \cap \mathbb{F}$. Then, we have an injection of R-modules

$$R[\alpha] \hookrightarrow I \cap \mathbb{F} \hookrightarrow I$$

and since R is Noetherian and I finitely generated, we have that $R[\alpha]$ is finitely-generated. Hence, α is integral over R, but R is integrally closed and so $\alpha \in R$. Claim follows.

2. Since $1 \in I$ we have a short exact sequence

$$0 \to R \hookrightarrow I \to I/R \twoheadrightarrow 0. \tag{10}$$

Now, by (1), I/R is a torsion free R-module. Indeed, if $\alpha \in I$ and $r \in R \setminus \{0\}$ are such that $r\alpha \in R$ then $\alpha \in r^{-1}R \subseteq \mathbb{F}$; hence $\alpha \in I \cap \mathbb{F} = R$ and so α is 0 in I/R. Thus, since R is a PID, I/R if free and the sequence (10) splits, giving a basis of I containing 1.

□

Every R-lattice I comes with an important construction of orders, that realise I as a left and right order, respectively.

Definition 2.23. Let I be an R-lattice in B. We define the *left order of I right order of I* as

$$\mathcal{O}_L(I) := \{\alpha \in B \colon \alpha I \subseteq I\} \qquad \text{and} \qquad \mathcal{O}_R(I) := \{\alpha \in B \colon I\alpha \subseteq I\},$$

respectively.

Lemma 2.24. *Let I be an R-lattice in B. Then, the left (resp. right) order $\mathcal{O}_L(I)$ (resp. $\mathcal{O}_R(I)$) of I is an R-order in B.*

Proof. It is easy to see that $\mathcal{O}_L(I)$ is an R-submodule of B that is also a subring. We prove $\alpha \in B$ and consider the R-submodule $\alpha I \subseteq B$. Since, I is finitely generated, so is αI and so by Lemma 2.18, it follows that there exists $r \in R \setminus \{0\}$ such that $r\alpha I \subseteq I$. Thus, $r\alpha \in \mathcal{O}_L(I)$ and so $\alpha \in r^{-1}\mathcal{O}_L(I) \subseteq (R \setminus \{0\})^{-1}\mathcal{O}_L(I)$.

Finally, we prove that $\mathcal{O}_L(I)$ is finitely generated as an R-submodule. Again, by Lemma 2.18, there exists $r \in R \setminus \{0\}$ such that $r = r \cdot 1 \in I$. Thus, by the definition of $\mathcal{O}_L(I)$ we have that $\mathcal{O}_L(I)r \subseteq I$, which implies that $\mathcal{O}_L(I) \subseteq Ir^{-1}$. Now, since R is Noetherian (as it is Dedekind) and since Ir^{-1} is finitely generated (as I is), I is a Noetherian module; hence, $\mathcal{O}_L(I)$ is also finitely generated as an R-module. □

Remark 2.25. Since R is a PID, it is integrally closed and so an element $\alpha \in B$ is integral over R if and only if the minimal polynomial of α over $\mathbb{F}$ has coefficients in R which, if $\alpha \in B \setminus R$, is the reduced characteristic polynomial (9). Hence, an element $\alpha \in B$ is integral over R iff $\mathrm{nrd}(\alpha), \mathrm{trd}(\alpha) \in R$. Therefore, since $\mathcal{O}$ is a subring of B that is finitely generated as an R-module then, by [Voi21, 10.3.2] (which is the non-commutative analogue of the standard [AM69, 5.1]), every $\alpha \in \mathcal{O}$ is integral over R and so $\mathrm{nrd}(\alpha), \mathrm{trd}(\alpha) \in R$.

2.3 Localization and Completion

As it is the usual case, lattices and orders are characterized by their local behaviour. For the further reference for the following notions see [AM69] and [Voi21, 9.4,9.5].

Localization of Lattices. Let $\mathfrak{p}$ be a prime ideal of R. For an R-module M we define the *localization of M to $\mathfrak{p}$* as the $R_{(\mathfrak{p})}$-module $M_{(\mathfrak{p})} := M \otimes_R R_{(\mathfrak{p})} = \{x/s \colon x \in M, s \in R \setminus \mathfrak{p}\}$, where $R_{(\mathfrak{p})}$ is the localization of R at $\mathfrak{p}$.

Note 2.26. If I is an R-lattice in B then $I_{(\mathfrak{p})}$ is an $R_{(\mathfrak{p})}$-lattice in B.

By a non-commutative analogue of the standard [AM69, Proposition 3.8], we have the following.

Lemma 2.27. *Let $I \subseteq B$ be an R-lattice. Then, it holds that*

$$I = \bigcap_{\mathfrak{p}} I_{(\mathfrak{p})} = \bigcap_{\mathfrak{m}} I_{(\mathfrak{m})},$$

where the first intersection is over all prime ideals $\mathfrak{p}$ of R and the second over all maximal ideals $\mathfrak{m}$ of R.

Therefore, we get that containment of R-lattices is a local property, as the following corollary states.

Corollary 2.28. *Let I, J be R-lattices in M. Then, the following are equivalent:*

1. *$I \subseteq J$;*
2. *$I_{(\mathfrak{p})} \subseteq J_{(\mathfrak{p})}$ for every prime ideal $\mathfrak{p} \subseteq R$; and*
3. *$I_{(\mathfrak{m})} \subseteq J_{(\mathfrak{m})}$ for every maximal ideal $\mathfrak{m} \subseteq R$.*

Proof. The directions (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) are immediate. The direction (3) $\Longrightarrow$ (1) follows directly from Lemma 2.27. □

Thus, we get a much useful theorem, which serves as a *local-global principle for lattices* for apparent reasons.

Theorem 2.29 (Local-global principle for lattices)**.** *Let $I \subseteq B$ be an R-lattice. Then, the map*

$$\begin{aligned} \Phi : \{J \subseteq B \colon J \text{ is an } R\text{-lattice}\} &\longrightarrow \left\{ (J^{\mathfrak{p}})_{\mathfrak{p}} \colon \begin{array}{c} J^{\mathfrak{p}}\text{'s are } R_{(\mathfrak{p})}\text{-lattices s.t. } I_{(\mathfrak{p})} = J^{\mathfrak{p}} \\ \text{for all but fin. many prime ideal } \mathfrak{p} \subseteq R \end{array} \right\} \\ J &\longmapsto (J_{(\mathfrak{p})})_{\mathfrak{p}} \end{aligned}$$

is a bijection.

Proof. The map Φ is well-defined. Indeed, let $J \subseteq B$ be an R-lattice. Then, by Lemma 2.18, there exists $r \in R \setminus \{0\}$ such that

$$rI \subseteq J \subseteq r^{-1}I. \tag{11}$$

But since R is a Dedekind domain it holds that r is contained in finitely many prime ideal $\mathfrak{p}$ of R. Thus, for those primes $\mathfrak{p}$, r is invertible in $R_{(\mathfrak{p})}$ and so by tensoring (11) with $R_{(\mathfrak{p})}$ we get that $I_{(\mathfrak{p})} = rI_{(\mathfrak{p})} \subseteq J_{(\mathfrak{p})} \subseteq r^{-1}I_{(\mathfrak{p})} = I_{(\mathfrak{p})}$ and so we get the equality $J_{(\mathfrak{p})} = I_{(\mathfrak{p})}$.

To prove that Φ is a bijection we prove that the map

$$\Psi : (J^{\mathfrak{p}})_{\mathfrak{p}} \mapsto \bigcap_{\mathfrak{p}} J^{\mathfrak{p}} =: J$$

is the inverse of Φ. We first prove that J is indeed an R-lattice in B. Let Σ be the set of prime ideals in R such that $J^{\mathfrak{p}} \neq I_{(\mathfrak{p})}$, which by assumption is finite. By Lemma 2.18, for every $\mathfrak{p} \in \Sigma$, there exists $r_{\mathfrak{p}} \in R \setminus \{0\}$ such that $r_{\mathfrak{p}} I_{(\mathfrak{p})} \subseteq J^{\mathfrak{p}} \subseteq r_{\mathfrak{p}}^{-1} I_{(\mathfrak{p})}$. Set $r := \prod_{\mathfrak{p} \in \Sigma} r_{\mathfrak{p}}$. Then, $rI_{(\mathfrak{p})} \subseteq J^{\mathfrak{p}} \subseteq r^{-1}I_{(\mathfrak{p})}$. Now, for every $\mathfrak{p} \notin \Sigma$ we have equality $I_{(\mathfrak{p})} = J^{\mathfrak{p}}$ and so $rI_{(\mathfrak{p})} \subseteq J^{\mathfrak{p}} \subseteq r^{-1}I_{(\mathfrak{p})}$. Therefore, by Lemma 2.27, we have that $rI \subseteq J \subseteq r^{-1}I$ and so by Lemma 2.18 we get that J is indeed an R-lattice.

Now, $\Psi \circ \Phi = \mathrm{id}$ follows from the fact that if J is an R-lattice then $J = \cap_{\mathfrak{p}} J_{(\mathfrak{p})}$ from Lemma 2.27. To see that $\Phi \circ \Psi = \mathrm{id}$, let $(J^{\mathfrak{p}})_{\mathfrak{p}}$ be a family of $R_{(\mathfrak{p})}$-lattices. Then, for every prime $\mathfrak{q} \subseteq R$ we get $(\cap_{\mathfrak{p}} J^{\mathfrak{p}})_{(\mathfrak{q})} = (J^{\mathfrak{q}})_{(\mathfrak{q})} = J^{\mathfrak{q}}$, since in a Dedekind domain, every prime is maximal. □

Completion of Lattices. We now define the completion of R with respect to a prime ideal $\mathfrak{p} \subseteq R$. For the (little) category theory background needed we refer to [ML98]. Notice that for each $n \geq 1$ we have a natural map

$$R/\mathfrak{p}^{n+1} \to R/\mathfrak{p}^n$$

and that these maps are compatible with each other. Thus we can form then inverse limit of R w.r.t. that system of natural maps:

$$R_{\mathfrak{p}} := \varprojlim_n R/\mathfrak{p}^n = \left\{ a \in \prod_{n=1}^{\infty} R/\mathfrak{p}^n \colon \forall n \geq 1 \ (a_{n+1} \equiv a_n \pmod{\mathfrak{p}^n}) \right\}$$

We call $R_{\mathfrak{p}}$ the *completion of* R *at* $\mathfrak{p}$. Notice that we have a natural map

$$R \to R_{\mathfrak{p}}; \quad a \mapsto (a \pmod{\mathfrak{p}^n})_n. \tag{12}$$

Given an R-module M we define its *completion at* $\mathfrak{p}$ as the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}} := M \otimes_R R_{\mathfrak{p}}$.

Note 2.30. If $I \subseteq B$ is an R-lattice, then $I_{\mathfrak{p}} \subseteq B$ is an $R_{\mathfrak{p}}$-lattice in the quaternion algebra $B_{\mathfrak{p}} := B \otimes_R R_{\mathfrak{p}}$. Indeed, $I_{\mathfrak{p}}$ is finitely generated over $R_{\mathfrak{p}}$ since we have the map (12) and $I_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} \mathbb{F}_{\mathfrak{p}} = I \otimes_R \mathbb{F}_{\mathfrak{p}} = I \otimes_R \mathbb{F} \otimes_R R_{\mathfrak{p}} = B \otimes_R R_{\mathfrak{p}} = I_{\mathfrak{p}}$.

Proposition 2.31. *If R is a DVR with maximal ideal $\mathfrak{p} \subseteq R$ then the maps*

$$\begin{aligned} \{J \subseteq B \colon J \ R\text{-lattice}\} &\longrightarrow \{J \subseteq B_{\mathfrak{p}} \colon J \ R_{\mathfrak{p}}\text{-lattice}\} \\ J &\longmapsto J_{\mathfrak{p}} \\ J \cap B &\longmapsfrom J \end{aligned}$$

are mutually inverse bijections, which preserve the inclusion relation.

Proof. See [Voi21, 9.5.3] □

Note 2.32. From Proposition 2.31, one can see that Theorem 2.29 holds also if we replace localizations with completions.

2.4 Quaternion Algebras over the Rationals.

In this section we prove a structure theorem for quaternion algebras over $\mathbb{Q}$, which states that the isomorphism class of a quaternion algebra over $\mathbb{Q}$ depends only on its local behaviour.

Let B be a quaternion algebra over $\mathbb{Q}$. Recall that by Corollary 2.15, a quaternion algebra over a field $\mathbb{F}$ is isomorphic to either a division algebra or the matrix algebra $M_2(\mathbb{F})$.

Definition 2.33. We define the set of *places* of $\mathbb{Q}$, denoted by $\mathrm{Pl}(\mathbb{Q})$ as the set of prime numbers $p \in \mathbb{Z}$ together with the infinity symbol ∞. For $v = \infty$, we define $\mathbb{Q}_\infty := \mathbb{R}$ and $B_\infty := B \otimes_{\mathbb{Q}} \mathbb{R}$. Let $v \in \mathrm{Pl}(\mathbb{Q})$ be a place. We say that the quaternion algebra B is *ramified* at v if B_v is a division algebra and we say that it is *unramified* (or *split*) if $B_v \simeq M_2(\mathbb{Q})$. Define the set $\mathrm{Ram}\, B$ to be the subset of $\mathrm{Pl}(\mathbb{Q})$ of places that B is ramified at. We say that B is *definite* if $\infty \in \mathrm{Ram}\, B$.

Definition 2.34. Let $a, b \in \mathbb{F}^\times$. For every place $v \in \mathrm{Pl}(\mathbb{Q})$, we define the *Hilbert symbol* of the pair (a, b), as the number $(a, b)_v \in \{\pm 1\}$, where $(a, b)_v = 1$ if and only if the quaternion algebra $\left(\frac{a,b}{\mathbb{Q}_v}\right)$ is split.

The following theorem by Hilbert, shows that $\operatorname{Ram} B$ is a finite set of even cardinality. For a proof we refer to [Voi21, 14.2.1]

Theorem 2.35 (Hilbert Reciprocity)**.** *For all $a, b \in \mathbb{Q}^\times$ it holds that*

$$\prod_{v \in \operatorname{Pl}\mathbb{Q}} (a,b)_v = 1.$$

Let $\mathbb{F}$ be a field and let $\operatorname{CSA}(\mathbb{F})$ be the set of isomorphism classes of central simple algebras over $\mathbb{F}$. We define on $\operatorname{CSA}(\mathbb{F})$ an equivalence relation, called *Morita equivalence*, defined as follows:

$$A \sim B \iff \exists m, n \in \mathbb{Z}_{\geq 1} : \ M_m(A) \simeq M_n(B).$$

Under this equivalence the set $\operatorname{CSA}(\mathbb{F})/\sim$ has the structure of an abelian group under the operation of the tensor product $\otimes_{\mathbb{F}}$ over $\mathbb{F}$, with $1 = [\mathbb{F}]$ and $[A]^{-1} = [A^{\mathrm{op}}]$, where A^{op} denotes the *opposite algebra* of A, which is the $\mathbb{F}$-algebra with the same $\mathbb{F}$-vector space structure, but with reversed multiplication, i.e. $\alpha \cdot_{\mathrm{op}} \beta = \beta \cdot \alpha$ for $\alpha, \beta \in A$, see [Voi21, 8.3.2]. We call this group the *Brauer group* of $\mathbb{F}$ and we denote by $\operatorname{Br}(\mathbb{F}) := \operatorname{CSA}(\mathbb{F})/\sim$.

Remark 2.36. Note that if B is a quaternion algebra then by Corollary 2.15, B is either isomorphic to $M_2(\mathbb{F})$, in which case $[B] = [\mathbb{F}]$ the identity or B is a division algebra in which case, by Proposition 2.6, the standard involution defines an isomorphism $\bar{\cdot} : B \xrightarrow{\sim} B^{\mathrm{op}}$. This shows that quaternion algebras are inside $\operatorname{Br}(\mathbb{F})[2]$, the 2-torsion subgroup of $\operatorname{Br}(\mathbb{F})$. If for a field $\mathbb{F}$, we define $\operatorname{Quat}(\mathbb{F}) := \{\text{quaternion algebras over } \mathbb{F}\}/\simeq$, then the above discussion means that we have an injection $\operatorname{Quat}(\mathbb{F}) \hookrightarrow \operatorname{Br}(\mathbb{F})[2]$.

Moreover, for $\mathbb{F} = \mathbb{Q}$, recall from Corollary 2.5, that for the place $v = \infty$, there is a unique division algebra over $\mathbb{R}$. This is the case also for all the finite places.

Theorem 2.37. *For every prime p, there is a unique division quaternion algebra over $\mathbb{Q}_p$, i.e. $\operatorname{Quat}(\mathbb{Q}_p) \simeq \{\pm 1\}$. In particular, if $p \neq 2$, then every division quaternion algebra over $\mathbb{Q}_p$ is isomorphic to $\left(\frac{e,p}{\mathbb{Q}_p}\right)$, where e is a quadratic non-residue modulo p.*

Proof. See [Voi21, 12.3.12]. □

The last ingredient in order to classify the quaternion algebras over $\mathbb{Q}$ is the *fundamental exact sequence* of global class field theory:

Theorem 2.38. *There is an exact sequence*

$$1 \longrightarrow \operatorname{Br}(\mathbb{Q}) \longrightarrow \bigoplus_{v \in \operatorname{Pl}\mathbb{Q}} \operatorname{Br}(\mathbb{Q}_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 1, \tag{13}$$

where the first map is $[A] \mapsto ([A_v])_v$ and the second is the sum of the local invariant maps $\operatorname{inv}_v : \operatorname{Br}(\mathbb{F}_v) \to \mathbb{Q}/\mathbb{Z}$ *defined in [Mil13, III.2.1].*

Proof. See [Mil13, VIII.4.3] and [Voi21, 13.4.3,14.6.10]. □

Combining the above we get the following classification theorem.

Theorem 2.39. *The map*

$$\mathrm{Quat}(\mathbb{Q}) \longrightarrow \left\{ \Sigma \subseteq \mathrm{Pl}\,\mathbb{Q} \colon \begin{array}{c} \Sigma \text{ finite of} \\ \text{even cardinality} \end{array} \right\}; \qquad B \longmapsto \mathrm{Ram}(B)$$

is a bijection.

Proof. By taking the 2-torsion part of the fundamental exact sequence (13), and taking the injections according to Remark 2.36 we get the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Br}(\mathbb{Q})[2] & \longrightarrow & \bigoplus_{v\in \mathrm{Pl}\,\mathbb{Q}} \mathrm{Br}(\mathbb{Q}_v)[2] & \xrightarrow{\sum_v \mathrm{inv}_v} & (\mathbb{Q}/\mathbb{Z})[2] & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mathrm{Quat}(\mathbb{Q}) & \longrightarrow & \bigoplus_{v\in \mathrm{Pl}\,\mathbb{Q}} \{\pm 1\} & \xrightarrow{\prod} & \{\pm 1\} & \longrightarrow & 1 \end{array}$$

where the first bottom map is $B = \left(\frac{a,b}{\mathbb{Q}}\right) \mapsto \left((a,b)_v\right)_v$ and the second bottom map is the product map. Note that the first bottom map is well-defined by Theorem 2.37. The result follows from Theorem 2.35 and the fact that the the local invariant map restricted to classes of quaternion algebras over $\mathbb{Q}_v$ behaves as $\mathrm{inv}_v B_v = 0, 1/2$, according as B_v is split or ramifies, respectively, see [Voi21, 14.6.10]. □

2.5 Ideals

As in the case of commutative rings, where we study them by their ideals, so we do in the non-commutative case. Let again R be a PID, $\mathbb{F} := \mathrm{Frac}(R)$, and B a quaternion algebra.

Definition 2.40. Let $\mathcal{O} \subseteq B$ be an R-order. An R-lattice $I \subseteq B$ is called a *left $\mathcal{O}$-ideal* if $\mathcal{O} \subseteq \mathcal{O}_L(I)$ and a *right $\mathcal{O}$-ideal* if $\mathcal{O} \subseteq \mathcal{O}_R(I)$.

Remark 2.41. If B is a division quaternion algebra and $I \subseteq \mathcal{O}$ is a non-zero left ideal of $\mathcal{O}$ in the usual sense then, I is also a left fractional $\mathcal{O}$-ideal, in which case it is called *integral*. Indeed, since $I \subseteq \mathcal{O}$ is a left ideal of $\mathcal{O}$ it follows that $\mathcal{O}I \subseteq I$ and so $\mathcal{O} \subseteq \mathcal{O}_L(I)$. Moreover, since $\mathcal{O}$ is an R-submodule of B so is I. The fact that I is finitely generated follows from the fact that it is an R-submodule of a finitely-generated R-module $\mathcal{O}$ over a Noetherian ring R. To conclude, we prove that $I \otimes_R \mathbb{F} = B$. Since I is a non-zero left ideal of $\mathcal{O}$, $I \otimes_R \mathbb{F}$ is a non-zero left ideal of $B = \mathcal{O} \otimes_R \mathbb{F}$, but B is a division algebra and thus it does not have non-trivial left ideals. Hence, $I \otimes_R \mathbb{F} = B$.

For two R-lattices $I, J \subseteq B$ we define their product, denoted by IJ, in B as the R-submodule of B generated by the set

$$\{\alpha \cdot \beta \colon \alpha \in I, \beta \in J\}.$$

Notice that IJ is again an R-lattice in B. Indeed, IJ is obviously finitely generated as I and J are. Now, by Lemma 2.18 we have that there exists $r \in R \setminus \{0\}$ such that $r = r \cdot 1 \in I$. Thus, $rJ \subseteq IJ$ and so again by Lemma 2.18 we get that IJ is an R-lattice.

Definition 2.42. Let $\mathcal{O}$ be an R-order in B and $I, J \subseteq B$ be two $\mathcal{O}$-ideals. We say that the product IJ is *compatible* or that I is *compatible with* J if $\mathcal{O}_R(I) = \mathcal{O}_L(J)$.

If I is compatible with J then the product IJ can be seen as the usual tensor product of modules, i.e. there is an isomorphism of R-modules $IJ \xrightarrow{\sim} I \otimes_{\mathcal{O}} J$, where $\mathcal{O} := \mathcal{O}_R(I) = \mathcal{O}_L(J)$. Indeed, first of all, notice that by compatibility the tensor product $I \otimes_{\mathcal{O}} J$ is well defined. Now, considering the $\mathcal{O}$-linear map $\phi : I \otimes_{\mathcal{O}} J \to IJ;\ \alpha \otimes \beta \mapsto \alpha\beta$ and tensoring with $\mathbb{F}$ we get a commutative diagram

$$\begin{array}{ccc} I \otimes_{\mathcal{O}} J & \xrightarrow{\phi} & IJ \\ \downarrow & & \downarrow \\ B \otimes_B B & \xrightarrow{\sim} & B \end{array}$$

where the below horizontal map is an isomorphism of B-modules, which restricts to ϕ, giving that ϕ is also an $\mathcal{O}$-linear isomorphism and thus an isomorphism of R-lattices.

Definition 2.43. Let $I \subseteq B$ be an R-lattice. We say that I is *invertible* if there exists an R-lattice $I' \subseteq B$ such that we have the compatible products:

$$II' = \mathcal{O}_L(I) = \mathcal{O}_R(I') \qquad \text{and} \qquad I'I = \mathcal{O}_L(I') = \mathcal{O}_R(I).$$

We say that I' is a *(two-sided) inverse* of I. Let $\mathcal{O}$ be an R-order. If I is a right (resp. left) $\mathcal{O}$-ideal we say that I is *invertible* if it is invertible as an R-lattice and $\mathcal{O} = \mathcal{O}_L(I)$ (resp. $\mathcal{O} = \mathcal{O}_R(I)$).

Definition 2.44. We define the *quasi-inverse* of an R-lattice I as the R-module

$$I^{-1} := \{\alpha \in B \colon I\alpha I \subseteq I\}.$$

Note 2.45. The fact that I^{-1} is again an R-lattice follows as in Lemma 2.24.

The quasi-inverse I^{-1} of I is essentially the inverse of I as the following lemma suggests.

Lemma 2.46. *Let I be an R-lattice. Then the following are equivalent:*

1. *I is invertible;*
2. *$II^{-1} = \mathcal{O}_L(I)$ and $I^{-1}I = \mathcal{O}_R(I)$;*
3. *$II^{-1}I = I$, $1 \in II^{-1}$, and $1 \in I^{-1}I$.*

In particular, if I is invertible, then the inverse of I is unique and equals I^{-1}.

Proof. See [Voi21, 16.5.8]. □

Definition 2.47. An R-lattice is called *principal* if there exists $a \in B^\times$ such that $I = \mathcal{O}_L(I)\alpha = \alpha\mathcal{O}_R(I)$. I is called *locally principal* if for every prime ideal $\mathfrak{p} \subseteq R$, $I_{(\mathfrak{p})} = I_R \otimes_R R_{(\mathfrak{p})}$ is principal.

Remark 2.48. It is easy to see that only one of the equalities $I = \mathcal{O}_L(I)\alpha$ and $I = \alpha\mathcal{O}_R(I)$ suffices. Moreover, any principal lattice $I = \alpha\mathcal{O}_R(I)$ is invertible with inverse $I^{-1} = \mathcal{O}_R(I)\alpha^{-1}$

Lemma 2.49. *An R-lattice I is invertible if and only if it is locally invertible, i.e. $I_{(\mathfrak{p})}$ is invertible for every prime ideal $\mathfrak{p} \subseteq R$.*

Proof. By Lemma 2.46, we have that I is invertible if and only if $II^{-1}I = I$ and $1 \in II^{-1}$, $1 \in I^{-1}I$. But, by Corollary 2.28, $II^{-1}I = I$ if and only if $I_{(\mathfrak{p})}I_{(\mathfrak{p})}^{-1}I_{(\mathfrak{p})} = (II^{-1}I)_{(\mathfrak{p})} = I_{(\mathfrak{p})}$ and $1 \in II^{-1}$ if and only if $1 \in I_{(\mathfrak{p})}I_{(\mathfrak{p})}^{-1} = (II^{-1})_{(\mathfrak{p})}$. This proves the lemma. □

Definition 2.50. The *reduced norm* of an R-lattice is the R-submodule, denoted by $\mathrm{nrd}(I)$, of $\mathbb{F}$ generated by the set $\{\mathrm{nrd}(\alpha)\colon \alpha \in I\}$. When $R = \mathbb{Z}$, we simply define $\mathrm{nrd}(I)$ as the g.c.d. of the elements in $\{\mathrm{nrd}(\alpha)\colon \alpha \in I\}$.

Remark 2.51.

1. The R-module $\mathrm{nrd}(I)$ is a non-zero finitely-generated R-submodule of $\mathbb{F}$. Indeed, since $I \otimes \mathbb{F} = B$ and $\mathrm{nrd}(B) \neq 0$ it follows that $\mathrm{nrd}(I) \neq 0$. Now, if $\{\alpha_i\}_{i=1}^4$ is an R-basis of I then it can be easily seen that the elements
$$\{\mathrm{nrd}(\alpha_i)\}_{1\leq i\leq 4} \qquad \text{and} \qquad \{\mathrm{nrd}(\alpha_i+\alpha_j)-\mathrm{nrd}(\alpha_i)-\mathrm{nrd}(\alpha_j)\}_{1\leq i,j\leq 4}$$
generate $\mathrm{nrd}(I)$ as an R-module.
2. For every prime ideal $\mathfrak{p} \subseteq R$ it holds that $\mathrm{nrd}(I)_{(\mathfrak{p})} = \mathrm{nrd}(I_{(\mathfrak{p})})$ and so by Corollary 2.28, we have that $\mathrm{nrd}(I) = \bigcap_{\mathfrak{p}} \mathrm{nrd}(I_{(\mathfrak{p})})$.
3. If $I = \alpha\mathcal{O}_R(I)$ is principal then $\mathrm{nrd}(I)$ is generated by the element $\mathrm{nrd}(\alpha)$. This follows directly from Remark 2.25.

The following proof is due to I. Kaplansky [Kap69].

Theorem 2.52. *An R-lattice I is invertible if and only if it is locally principal.*

Proof. By Lemma 2.49, I is invertible iff it is locally invertible and so we may assume that R is a DVR and prove that I is invertible iff it is principal. If I is principal then it is obviously invertible, as seen in Remark 2.48.

Suppose that I is invertible. We may further assume that I has the properties $1 \in I$ and $\mathrm{nrd}(I) = R$. Indeed, $\mathrm{nrd}(I)$ is a fractional ideal of $\mathbb{F}$ and since R is a DVR, it is generated by an element of minimal valuation, say $\mathrm{nrd}(\alpha)$ for some $\alpha \in I$. Then, the R-lattice $\alpha^{-1}I$ has the aforementioned properties and it is invertible (resp. principal) iff it I is invertible (resp. principal). So assume that $1 \in I$ and that $\mathrm{nrd}(I) = R$. Note first that, since $1 \in I$, then using the relation (8) we get that $\mathrm{trd}(\alpha) \in R$, for every $\alpha \in R$. Furthermore, by Lemma 2.22, there is an R-basis $\alpha_0 = 1, \alpha_1, \alpha_2, \alpha_3$ of I.

We claim that $I^3 = I^4$. Since $1 \in I$, we have that $I^3 \subseteq I^4$. In order to prove that $I^4 \subseteq I^3$ it is enough to prove that the product of 4 of the generators of I, say $\alpha_i\alpha_j\alpha_k\alpha_l$ $(0 \leq i,j,k,l \leq 3)$ is in I^3. If one of the i,j,k,l is 0 then we are done since $\alpha_0 = 1$, so suppose that this is not the case. Then, by the Pigeonhole Principle, we get that two of i,j,k,l are equal. If necessary, we may use the formula
$$\alpha\beta + \beta\alpha = \mathrm{trd}(\beta)\alpha + \mathrm{trd}(\alpha)\beta - \mathrm{trd}(\alpha\overline{\beta})$$
in order the push the right instance of this double term in the product $\alpha_i\alpha_j\alpha_k\alpha_l$ to the left. Thus, we may assume that this product has a term of the form α_i^2 and two other terms α_j, α_k. But, then we have that
$$\alpha_i^2 = \mathrm{trd}(\alpha_i)\alpha_i - \mathrm{nrd}(\alpha_i)$$
which is in I, since $\mathrm{nrd}(\alpha_i), \mathrm{trd}(\alpha_i) \in I$. Hence, this product belongs to I^3 and thus the equality $I^3 = I^4$ holds. Now, since I is invertible, by multiplying $I^3 = I^4$ by $(I^{-1})^3$ we get that $I = \mathcal{O}_L(I)$, and thus I is principal. □

From the proof of Theorem 2.52 we get also the following characterization of orders.

Corollary 2.53. *An R-lattice I is an R-order if and only if I is invertible, $1 \in I$, and every element of I is integral.*

The characterization of an invertible ideal given in Theorem 2.52 should be compared to that description of modules over schemes and constitutes a major tool in our analysis of invertible ideals.

Lemma 2.54. *Let I, J be R-lattices such that IJ is compatible and either I or J is invertible, then* $\operatorname{nrd}(IJ) = \operatorname{nrd}(I)\operatorname{nrd}(J)$.

Proof. Suppose that I is invertible. Then, by Theorem 2.52, I is locally principal. The statement we want to prove is local and so we may suppose that I is principal, say by $\alpha \in B^\times$. Then, we get

$$IJ = \alpha\mathcal{O}_R(I)J = \alpha\mathcal{O}_L(J)J = \alpha J$$

Hence, $\operatorname{nrd}(IJ) = \operatorname{nrd}(\alpha J) = \operatorname{nrd}(\alpha)\operatorname{nrd}(J) = \operatorname{nrd}(I)\operatorname{nrd}(J)$. □

The following notion of a conjugate of an ideal will give us an arithmetic description of the inverse of an ideal.

Definition 2.55. Let I be an R-lattice in B. We define the *conjugate lattice* of I as the R-lattice $\overline{I} := \{\overline{\alpha} \in B \colon \alpha \in I\}$.

Note 2.56.
1. For R-lattices I, J it holds that $\overline{IJ} = \overline{J}\,\overline{I}$.
2. If $\mathcal{O}$ is an R-order then $\overline{\mathcal{O}} = \mathcal{O}$. Indeed, this follows from the fact that if $\alpha \in \mathcal{O}$, then by Remark 2.25, it holds that $\operatorname{trd}(\alpha) = \alpha + \overline{\alpha} \in R$. Since O is an R-order, $R \subseteq \mathcal{O}$ and so $\overline{\alpha} \in \mathcal{O}$.
3. $\mathcal{O}_R(I) = \mathcal{O}_L(\overline{I})$ and $\mathcal{O}_L(I) = \mathcal{O}_R(\overline{I})$. This follows from 1. and 2 above.

Lemma 2.57. *Let I be an invertible R-lattice in B. Then, the following hold*

$$I\overline{I} = \operatorname{nrd}(I)\mathcal{O}_L(I) \qquad \textit{and} \qquad \overline{I}I = \operatorname{nrd}(I)\mathcal{O}_R(I).$$

Proof. By Remark 2.51(2) and Theorem 2.52 we may prove it locally and so we may suppose that R is a DVR and I is principal, say $I = \alpha\mathcal{O}_R(I) = \mathcal{O}_L(I)\alpha$, for some $\alpha \in B^\times$. Then, we have that $\operatorname{nrd}(I) = \operatorname{nrd}(\alpha)R$ and that $\overline{I}$ is also principal generated by $\overline{\alpha}$, since $\overline{I} = \overline{\alpha\mathcal{O}_R(I)} = \overline{\mathcal{O}_R(I)}\overline{\alpha} = \mathcal{O}_L(\overline{I})\overline{\alpha}$ and similarly $\overline{I} = \overline{\alpha}\mathcal{O}_R(\overline{I})$. Hence,

$$I\overline{I} = \mathcal{O}_L(I)\alpha\overline{\alpha}\mathcal{O}_R(\overline{I}) = \mathcal{O}_L(I)\operatorname{nrd}(\alpha)\mathcal{O}_L(I) = \operatorname{nrd}(I)\mathcal{O}_L(I).$$

and similarly, $\overline{I}I = \operatorname{nrd}(I)\mathcal{O}_R(I)$. □

Class set. In analogy with that of the maximal order in a quadratic number field we can define the class set of an order in a quaternion algebra B. In this case however, the class set will not form a group because B lacks commutativity.

Definition 2.58. We say that two R-lattices $I, J \subseteq B$ are *right equivalent* if there exists $\alpha \in B^\times$ such that $J = \alpha I$. We write $I \sim_R J$. Similarly we define the relation $I \sim_L J$.

Note that the relation $\sim_R$ (resp. $\sim_L$) on the set of R-lattices is an equivalence relation. We denote the equivalence class of an R-lattice I under $\sim_R$ (resp. $\sim_L$) by $[I]_R$ (resp. $[I]_L$). Note also that if I is invertible then every R-lattice in $[I]_R$ is invertible.

Lemma 2.59. *Let $I, J \subseteq B$ be R-lattices. Then, $I \sim_R J$ if and only if $\mathcal{O}_R(I) = \mathcal{O}_R(J) =: \mathcal{O}$ and $I \simeq J$ as right $\mathcal{O}$-modules.*

Proof. If $I \sim_R J$ then there exists $\alpha \in B^\times$ such that $J = \alpha I$. Then, $\mathcal{O}_R(J) = \mathcal{O} = \mathcal{O}_R(I)$ and the map $\alpha \cdot - : I \xrightarrow{\sim} J$ given by left multiplication by α defines an isomorphism of $\mathcal{O}$-modules.

Conversely, suppose that $\mathcal{O}_R(I) = \mathcal{O} = \mathcal{O}_R(J)$ and that $\phi : I \xrightarrow{\sim} J$ is an isomorphism of $\mathcal{O}$-modules. Tensoring ϕ with $\mathbb{F}$ we get an automorphism

$$\phi_{\mathbb{F}} : B = I \otimes_R \mathbb{F} \xrightarrow{\sim} J \otimes_R \mathbb{F} = B$$

of B, which is given by left multiplication by $\alpha := \phi_{\mathbb{F}}(1)$. Thus, restricting it again to I we get that $J = \alpha I$. □

Definition 2.60. Let $\mathcal{O} \subseteq B$ be an R-order. We define the *right class set* of $\mathcal{O}$ as the set

$$\mathrm{Cls}_R(\mathcal{O}) := \{\text{invertible right } \mathcal{O}\text{-ideal}\} \,/\, \sim_R$$

Similarly, we define the *left class set* of $\mathcal{O}$, $\mathrm{Cls}_L(\mathcal{O})$. The cardinality of the right class set $\mathrm{Cls}_R(\mathcal{O})$ is called the *class number* of $\mathcal{O}$ and we denote it by $h(\mathcal{O})$.

Note that using the standard (anti-)involution of the quaternion algebra B, we have a bijection

$$\mathrm{Cls}_R(\mathcal{O}) \longrightarrow \mathrm{Cls}_L(\mathcal{O}); \qquad [I] \longmapsto [\overline{I}]$$

Thus, we may choose, without loss of generality, to work with $\mathrm{Cls}_R(\mathcal{O})$. This fact also justifies the absence of a subscript in the class number number $h(\mathcal{O})$ of $\mathcal{O}$.

Remark 2.61. Using Minkowski's Geometry of numbers one can prove the finiteness of the class set in any definite quaternion algebra, see [Voi21, 17.5.6]. We will give an explicit formula for $h(\mathcal{O})$ in (5.1.2), using the *Eichler Trace Formula*.

2.6 Maximal Orders

The greatest class of orders is that of maximal order, which are also the order which we understand better. For further reading for maximal orders in algebras see [Rei75].

Definition 2.62. An R-order $\mathcal{O} \subseteq B$ is called *maximal* if it is not properly contained in any non-trivial R-order of B.

Being a maximal order is a local property as the following lemma shows.

Lemma 2.63. *An R-order $\mathcal{O}$ in B is maximal if and only if $\mathcal{O}_{(\mathfrak{p})}$ is an $R_{(\mathfrak{p})}$-order for every prime ideal $\mathfrak{p} \subseteq R$.*

Proof. Let $\mathcal{O} \subseteq B$ be an R-order. If for every prime ideal $\mathfrak{p} \subseteq R$, $\mathcal{O}_{(\mathfrak{p})}$ is a maximal then since containment of orders is local by Corollary 2.28 it follows that $\mathcal{O}$ is maximal.

For the converse, suppose that $\mathcal{O}$ is maximal and suppose, towards a contradiction, that for some non-zero prime ideal $\mathfrak{p} \subseteq R$, there exists an $R_{(\mathfrak{p})}$-order $\mathcal{O}^{\mathfrak{p}}$ such that $\mathcal{O}_{(\mathfrak{p})} \subsetneq \mathcal{O}^{\mathfrak{p}}$. Consider then, the R-lattice

$$\mathcal{O}' := \mathcal{O}^{\mathfrak{p}} \bigcap \left(\cap_{\mathfrak{q} \neq \mathfrak{p}} \mathcal{O}_{(\mathfrak{p})} \right).$$

For all $\mathfrak{q} \neq \mathfrak{p}$, $\mathcal{O}'_{(\mathfrak{p})} = \mathcal{O}_{(\mathfrak{p})}$ and so by Theorem 2.29, $\mathcal{O}'$ is an R-order. Now, locally $\mathcal{O}'$ is an order and, since this is a local property by Lemma 2.27, $\mathcal{O}'$ is an R-order. Thus, by Corollary 2.28, we get that $\mathcal{O} \subsetneq \mathcal{O}'$, a contradiction to the assumption that $\mathcal{O}$ is maximal. □

Let B be a quaternion algebra over $\mathbb{Q}$ and $\mathcal{O} \subseteq B$ be a maximal order in B. As Lemma 2.63 suggests, we are going to characterize the orders locally. Let p be a prime number and $B_p = B \otimes \mathbb{Q}_p$.

Split case. $B_p \simeq M_2(\mathbb{Q}_p)$. Set $R := R_p$ and $\mathbb{F} = \mathbb{Q}_p$. We first realise $M_2(\mathbb{F})$ as the endomorphism algebra of a 2-dimensional $\mathbb{F}$-vector space. So let V be an $\mathbb{F}$-vector space of $\dim_{\mathbb{F}} V = 2$ and consider an isomorphism $\mathrm{End}_{\mathbb{F}}(V) \xrightarrow{\sim} M_2(\mathbb{F})$, given by a choice of basis of V. Let now $M \subseteq V$ be an R-lattice of V, i.e. a finitely generated free R-submodule of V of rank 2. Then, the R-module

$$\mathrm{End}_R(M) := \{f \in \mathrm{End}_{\mathbb{F}}(V) \colon f(M) \subseteq M\}$$

is an R-order in $\mathrm{End}_{\mathbb{F}}(V)$, which can be proved as in Lemma 2.24.

Consider now the R-order $M_2(R)$ in $M_2(\mathbb{F})$. Since R is a PID, it is integrally closed and thus $M_2(R)$ is a maximal order in $M_2(\mathbb{F})$. Indeed, if $\mathcal{O} \supseteq M_2(R)$ is another R-order in $M_2(\mathbb{F})$ then, consider the R-submodule L of $\mathbb{F}$ that contains exactly those elements of $\mathbb{F}$ that occur as an entry in a matrix $A \in \mathcal{O}$. It can be easily seen that $R \subseteq L \subseteq \mathbb{F}$ and that L is also an R-order in $\mathbb{F}$, see [Rei75, 8.7]. But, since R is integrally closed R is a maximal order in $\mathbb{F}$; hence, $L = R$ and $M_2(R) = \mathcal{O}$. Below we prove that every maximal order in $M_2(\mathbb{F})$ is a conjugate of this maximal order, namely $M_2(R)$.

Proposition 2.64. *If $\mathcal{O} \subseteq M_2(\mathbb{F})$ is maximal R-order then $\mathcal{O} \simeq M_2(R)$ via a conjugation.*

Proof. Let x_1, x_2 be an $\mathbb{F}$-basis of V and consider the isomorphism $\phi : \mathrm{End}_{\mathbb{F}}(V) \xrightarrow{\sim} M_2(\mathbb{F})$ induced by this choice of basis. Consider the R-lattice $N := Rx_1 \oplus Rx_2$ of V. Then, ϕ restricts to am isomorphism $\mathrm{End}_{\mathbb{F}}(N) \xrightarrow{\sim} M_2(R)$, which is a maximal order in $M_2(\mathbb{F})$, by the above discussion.

Realise $\mathcal{O}$ as an order in $\mathrm{End}_{\mathbb{F}}(B)$ and consider $M := \{x \in N \colon \mathcal{O}x \subseteq N\}$. Notice that it is an R-order in N (as in Lemma 2.24). By definition we have that $\mathcal{O} \subseteq \mathrm{End}_R(M)$ and since $\mathcal{O}$ is maximal we get that $\mathcal{O} = \mathrm{End}_R(M)$. Now, letting $y_1, y_2 \in M$ an R-basis of M we get that the base change $x_i \mapsto y_i$ induces a conjugation of $\mathcal{O} = \mathrm{End}_R(M)$ to $\mathrm{End}_R(N) \simeq M_2(R)$. □

Ramified case. $B_p = B \otimes \mathbb{Q}_p$ is a division quaternion algebra over $\mathbb{Q}_p$. We may extend the p-adic $v_p : \mathbb{Q}_p \longrightarrow \mathbb{R} \cup \{\infty\}$ to a *discrete valuation* on B_p as follows:

$$w_p : B_p \to \mathbb{R} \cup \{\infty\}; \qquad \alpha \mapsto \frac{v_p(\mathrm{nrd}(\alpha))}{2}.$$

It is clear that w_p is an extension of v_p and the fact that we call it a discrete valuation comes from the following lemma.

Lemma 2.65. *The function $w_p : B_p \to \mathbb{R} \cup \{\infty\}$ is the unique extension of v_p to B_p satisfying the following properties:*

1. *$w_p(\alpha) = \infty$ if and only if $\alpha = 0$;*
2. *$w_p(\alpha\beta) = w_p(\alpha) + w_p(\beta)$, for all $\alpha, \beta \in B_p$;*
3. *$w_p(\alpha + \beta) \geq \min(w_p(\alpha), w_p(\beta))$, for all $\alpha, \beta \in B_p$;*
4. *$w_p(B_p^\times) \subseteq \mathbb{R}$ is discrete.*

Proof. This follows using the properties of v_p, see [Voi21, 13.3.2]. □

We now define the *valuation ring* of B_p as the set

$$\mathcal{O}_p := \{\alpha \in B_p \colon w_p(\alpha) \geq 0\},$$

which is a ring by Lemma 2.65. Note that by Remark 2.25, we have that an element $\alpha \in B_p$ is integral over $\mathbb{Z}_p$ if and only if $\mathrm{trd}(\alpha), \mathrm{nrd}(\alpha) \in \mathbb{Z}_p$. Thus, $\mathcal{O}_p$ can be equivalently defined as the set of integral elements of B_p over $\mathbb{Z}_p$, i.e.

$$\mathcal{O}_p = \{\alpha \in B_p \colon \alpha \text{ is integral over } \mathbb{Z}_p\}.$$

In [Voi21, 13.3.4] it is proved that $\mathcal{O}_p$ is a $\mathbb{Z}_p$-order in B_p. Therefore, again by Remark 2.25, we have that if $\mathcal{O} \subseteq B_p$ is an order then $\mathcal{O} \subseteq \mathcal{O}_p$; hence $\mathcal{O}_p$ is the unique maximal order in B_p.

Class set of a maximal order.

Theorem 2.66. *Let $\mathcal{O}$ be a maximal R-order in a quaternion algebra B. Then, both right and left $\mathcal{O}$-ideals in B is invertible.*

Proof. By Lemma 2.63 and Theorem 2.52 we may assume that R is a DVR and prove that if I is a left $\mathcal{O}$-ideal in B then it is principal. If $B \simeq M_2(\mathbb{F}_p)$ the result follows from [Voi21, 17.2.2]. If B is a division algebra then $\mathcal{O} = \{\alpha \in B \colon w(\alpha) \geq 0\}$ is the valuation ring of B, where $w : B \to \mathbb{R} \cup \{\infty\}$ is the unique extension of the discrete valuation of R to B, see Lemma 2.65. Let now $\beta \in I$ be of minimal valuation such that $w(\beta) > 0$. Then, for every $\alpha \in I \setminus \{0\}$ we have that $w(\alpha\beta^{-1}) = w(\alpha) - w(\beta) \geq 0$; hence $\alpha\beta^{-1} \in \mathcal{O}$ and so $\alpha \in \mathcal{O}\beta$. Therefore, $I = \mathcal{O}\beta$ and I is principal. □

For a more direct proof of Theorem 2.66, without the distinction of the ramified-unramified case see [Voi21, 16.6.15]. The above theorem suggests that in the case of a maximal order $\mathcal{O}$ the right class set of $\mathcal{O}$ consists of isomorphism classes of just right $\mathcal{O}$-ideals, i.e.

$$\mathrm{Cls}_R(\mathcal{O}) = \{[I] \colon I \text{ a right } \mathcal{O}\text{-ideal}\}.$$

We conclude this section by proving an auxiliary lemma for (5.1).

Lemma 2.67. *If $I \subseteq B$ is an invertible R-lattice in B, then, $\mathcal{O}_R(I)$ is maximal if and only if $\mathcal{O}_L(I)$ is maximal.*

Proof. By Lemma 2.63 we can prove this statement locally and so by Theorem 2.52 we may assume that I is principal, i.e. there exists $\alpha \in B^\times$ such that $I = \mathcal{O}_L(I)\alpha$. Suppose, without loss of generality, that $\mathcal{O}_R(I)$ is maximal. We have that $\mathcal{O}_R(I) = \mathcal{O}_R(\mathcal{O}_L(I)\alpha)$ and

$$\beta \in \mathcal{O}_R(\mathcal{O}_L(I)\alpha) \iff \mathcal{O}_L(I)\alpha\beta \subseteq \mathcal{O}_L(I)\alpha \iff \alpha\beta\alpha^{-1} \in \mathcal{O}_L(I)$$

and so $\mathcal{O}_R(I) \subseteq \alpha^{-1}\mathcal{O}_L(I)\alpha$. Note that every conjugate of an order is also an order and so $\mathcal{O}_R(I) = \alpha^{-1}\mathcal{O}_L(I)\alpha$. Therefore, $\mathcal{O}_L(I) = \alpha\mathcal{O}_R(I)\alpha^{-1}$ is maximal, as a conjugate of a maximal order. □

2.7 Eichler Orders

We now define a more general and interesting class of quaternion orders.

Definition 2.68. An R-order $\mathcal{O} \subseteq B$ is called an *Eichler order* if it is the intersection of two maximal R-orders of B.

Note 2.69. By Lemma 2.63, we have that being a maximal order is a local property, which implies that being an Eichler order is also a local property.

Let us characterize first Eichler orders in the split case.

Proposition 2.70 (Hijikata, [Hij74])**.** *Let p be a prime and $\mathcal{O} \subseteq B := M_2(\mathbb{Q}_p)$ be an order. Then, the following are equivalent:*

1. *$\mathcal{O}$ is an Eichler order;*
2. *$\mathcal{O} \simeq \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^e\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$, for some unique $e \in \mathbb{Z}_{\geq 0}$.*

Proof. Let $\mathcal{O}$ be an Eichler order. Then, $\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$, where $\mathcal{O}_1, \mathcal{O}_2 \subseteq M_2(\mathbb{Q}_p)$ are maximal orders. By Proposition 2.64, there exist $\alpha_1, \alpha_2 \in B^\times$ such that $\mathcal{O}_1 = \alpha_1^{-1}M_2(\mathbb{Z}_p)\alpha_1$ and $\mathcal{O}_2 = \alpha_2^{-1}M_2(\mathbb{Z}_p)\alpha_2$. Conjugating $\mathcal{O}$ with α_1, we have that

$$\mathcal{O} \simeq \alpha_1\mathcal{O}\alpha_1^{-1} \simeq M_2(\mathbb{Z}_p) \cap \alpha_1\alpha_2^{-1}M_2(\mathbb{Z}_p)\alpha_2\alpha_1^{-1},$$

Using row operations, we may find $\beta \in M_2(\mathbb{Z}_p)^\times$ and using column operations, we may find $\gamma \in M_2(\mathbb{Z}_p)^\times$ such that $\beta\alpha_1\alpha_2^{-1}\gamma = \begin{pmatrix} 1 & 0 \\ 0 & p^e \end{pmatrix}$, for some $e \in \mathbb{Z}_{\geq 0}$. Therefore,

$$\begin{aligned} \mathcal{O} &\simeq \beta\mathcal{O}\beta^{-1} \simeq \beta M_2(\mathbb{Z}_p)\beta^{-1} \cap \beta\alpha_1\alpha_2^{-1}M_2(\mathbb{Z}_p)\alpha_2\alpha_1^{-1}\beta^{-1} \\ &= M_2(\mathbb{Z}_p) \cap \begin{pmatrix} 1 & 0 \\ 0 & p^e \end{pmatrix} M_2(\mathbb{Z}_p) \begin{pmatrix} 1 & 0 \\ 0 & p^e \end{pmatrix}^{-1} \end{aligned}$$

and thus one can see that $\mathcal{O} \simeq \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^e\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. For more careful calculations of the above we refer to [Voi21, 23.4.3] For the uniqueness, see [Hij74, 2.2]. □

Let now B be a definite quaternion algebra over B with ramified places $\operatorname{Ram} B$. Proposition 2.70 enables us to characterize Eichler orders of quaternion algebras over $\mathbb{Q}$. An *Eichler order of level* $N \in \mathbb{Z}_{\geq 1}$ is an Eichler order in B with the following local characterization (see Theorem 2.29): consider a prime number p.

- If $p \in \operatorname{Ram} B$, then by the previous section(2.6), there exists a unique maximal order in B_p and so $\mathcal{O}_p$ is this unique maximal order, namely the valuation ring of B_p.
- If $p \notin \operatorname{Ram} B$, then $B_p \simeq M_2(\mathbb{Q}_p)$ and $\mathcal{O}_p$ is an Eichler order in B_p. Thus, by Proposition 2.70, we define
$$\mathcal{O}_p \simeq \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^e\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix},$$
where $e := v_p(N)$. We call this order the *standard Eichler order of level* p^e.

Note that Eichler orders are a generalization of maximal orders. In particular, maximal orders are just the Eichler orders of level 1.

3 Elliptic Curves

Let $\mathbb{F}$ be a field and fix an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. For background and further study of the following notions we refer to [Sil09].

3.1 Definitions

Throughout the following sections we will refer to a *curve* to mean a projective variety of dimension 1.

Definition 3.1. An *elliptic curve* over $\mathbb{F}$ is a pair (E, O), where E is a smooth curve of genus 1 over $\mathbb{F}$ and $O \in E(\mathbb{F})$. We write $E/\mathbb{F}$ for an elliptic curve over $\mathbb{F}$.

Remark 3.2.

1. An elliptic curve $E/\mathbb{K}$ is isomorphic to a curve defined by the affine equation

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{14}$$

   with $a_i \in \mathbb{K}$. This is called the *Weierstrass equation* associated to the elliptic curve E. See [Sil09, III.3.1].

2. An elliptic curve (E, O) comes with a compatible group structure, where the point O plays the role of the identity element, [Sil09, III.3.6]. This group operation can also be defined in terms of the coefficients of the Weierstrass equation (14), [Sil09, III.2.3].

Let $E/\mathbb{F}$ be an elliptic curve. Using the associated Weierstrass equation (14) of E one can define a certain invariant on E called the *j-invariant* of E, denoted by $j(E)$. This is a rational function in the coefficients of the Weierstrass equation. To be more precise, if $\mathrm{char}(\mathbb{F}) \neq 2, 3$ (which will be assumed in the following chapters) then E has a *short Weierstrass equation* of the form

$$E: \quad y^2 = x^3 + Ax + B, \tag{15}$$

for some $A, B \in \mathbb{F}$ and j-invariant

$$j(E) := 1728\frac{A^3}{4A^3 + 27B^2} \in \mathbb{F}.$$

The importance of the j-invariant is that it classifies the elliptic curves up to isomorphism as shown in the following theorem.

Theorem 3.3.

1. *Two elliptic curves E, E' are isomorphic over $\overline{\mathbb{F}}$ if and only if $j(E) = j(E')$.*

2. *For every $j \in \mathbb{K}$, there exists an elliptic curve $E/\mathbb{F}$ such that $j(E) = j$.*

Proof. See [Sil09, III.4.1]. □

Definition 3.4. An *isogeny* between two elliptic curves $(E, O), (E', O')$ is a morphism of curves $\phi : E \to E'$ such that $\phi(O) = O'$. The elliptic curves E, E' are called *isogenous* if there exists a non-constant isogeny between them.

Note 3.5. By [Har77, II.6.8.], we have that an isogeny $\phi : E \to E'$ is either a constant or surjective and thus either $\phi(E) = \{O\}$ or $\phi(E) = E'$. Moreover, by [Sil09, III.4.8], ϕ also respects the group structure of E.

By the above note, in the case where $\phi : E \to E'$ is a non-constant isogeny we have an induced injection of function fields

$$\phi^* : \overline{\mathbb{F}}(E') \to \overline{\mathbb{F}}(E)$$

and thus we may define the *degree* of the isogeny ϕ, denoted by $\deg \phi$, as the degree of the finite extension $\overline{\mathbb{F}}(E)/\phi^*\overline{\mathbb{F}}(E')$. If ϕ is the constant isogeny we define $\deg \phi := 0$. An isogeny ϕ is called *separable, inseparable,* and *purely inseparable* if the field extension $\overline{\mathbb{F}}(E)/\phi^*\overline{\mathbb{F}}(E')$ is separable, inseparable, and purely inseparable, respectively. Accordingly we define the *separable* and the *inseparable* degree of ϕ, which we denote by $\deg_s \phi$ and $\deg_i \phi$, respectively. By [Sil09, III.4.10], it holds that $\deg_s \phi = \ker \phi$, and so in the case of a separable isogeny ϕ, the degree can be also defined as above.

Definition 3.6. Let E be an elliptic curve. For an integer $m \in \mathbb{Z}$ we define the *multiplication-by-m isogeny*, as the endomorphism

$$[m] : E \longrightarrow E; \qquad [m]P = \overbrace{P + \cdots + P}^{m \text{ times}}$$

We also define the *m-torsion subgroup* of E as the subgroup

$$E[m] := [m]^{-1}(O) = \{P \in E \colon [m]P = O\}.$$

Note 3.7. Note that since the group structure of E is compatible with its geometric structure of the multiplication-by-m map is indeed an isogeny. Note also that, when $m \neq 0$, the multiplication-by-m map is non-constant, by [Sil09, III.4.2].

Lemma 3.8. *Suppose that* $\mathrm{char}(\mathbb{F}) = p$ *a prime number. Then, for every integer* $m \in \mathbb{Z}_{>0}$ *such that* $p \nmid m$ *it holds that*

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof. Let d be a divisor of m. Since $p \nmid m$, we have that $[d]$ is a separable isogeny by [Sil09, III.5.5] and so $\#E[d] = \deg[d] = d^2$. A finite abelian group of order m^2 with this property is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

Definition 3.9. Let E, E' be elliptic curves and $\phi : E \to E'$ an isogeny. We define the *dual isogeny* of ϕ as the unique isogeny $\hat{\phi} : E' \to E$ such that

$$\hat{\phi} \circ \phi = [\deg \phi] : E \to E \qquad \text{and} \qquad \phi \circ \hat{\phi} = [\deg \phi] : E' \to E'$$

Note 3.10. The dual isogeny is well-defined as for every isogeny $\phi : E \to E'$ there is indeed a unique dual of ϕ by [Sil09, III.6.1].

Definition 3.11. Let E, E' be elliptic curves over $\mathbb{F}$. We define the additive group

$$\mathrm{Hom}_{\mathbb{F}}(E, E') := \{\phi : E \to E' \colon \phi \text{ is an isogeny}\}$$

with addition defined point-wise induced by the group structure of E. We also define the *endomorphism ring* of E as the ring $\mathrm{End}_{\mathbb{F}}(E) := \mathrm{Hom}_{\mathbb{F}}(E, E)$ with multiplication operation the composition, and the *endomorphism algebra* of E as the tensor product $\mathrm{End}_{\mathbb{F}}(E)_{\mathbb{Q}} := \mathrm{End}_{\mathbb{F}}(E) \otimes \mathbb{Q}$.

Note 3.12. When there is no confusion we may omit the subscript $\mathbb{F}$ in the notation $\mathrm{Hom}_{\mathbb{F}}(E, E')$.

Remark 3.13. Let E, E' be elliptic curves over $\mathbb{F}$. Note that the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ acts on $E(\overline{\mathbb{F}})$ and on $\mathrm{Hom}_{\overline{\mathbb{F}}}(E, E')$. In general, it holds that E is over $\mathbb{F}$ if and only if the points in $E(\overline{\mathbb{F}})$ are fixed by this action, and similarly $\mathrm{Hom}_{\mathbb{F}}(E, E')$ consists exactly of those isogenies $\phi : E \to E'$ that are fixed by this action, see [Sil09, I.3].

Let E, E' are elliptic curves over $\mathbb{F}$. The $\mathbb{Z}$-module $\mathrm{Hom}(E, E')$ is a torsion-free module and hence free. Indeed, if for $m \in \mathbb{Z}_{\geq 0}$ and $\phi : E \to E'$ an isogeny such that $m\phi = [m] \circ \phi = 0$ then $\deg[m] \circ \deg \phi = 0$. Since, by Note 3.7, $[m]$ is constant if and only if $m = 0$, we get that if $m \neq 0$ then $\deg \phi = 0$ and so ϕ is constant.

The $\mathbb{Q}$-algebra $\mathrm{End}(E)_{\mathbb{Q}}$ is a division algebra since for every non-constant isogeny $\phi : E \to E$ it holds that

$$\phi^{-1} = \frac{1}{\deg \phi}\phi \in \mathrm{End}(E)_{\mathbb{Q}}.$$

By [Sil09, III.6.2], the duality map $\phi \mapsto \hat{\phi}$ defines a standard involution on $\mathrm{End}(E)_{\mathbb{Q}}$ in the sense that it satisfies the properties of Proposition 2.6. Therefore, the reduced norm and trace in $\mathrm{End}(E)_{\mathbb{Q}}$ are defined as the induced maps from the following maps on $\mathrm{End}(E)$:

$$\mathrm{trd}(\phi) = \phi + \hat{\phi} \qquad \text{and} \qquad \mathrm{nrd}(\phi) = \phi\hat{\phi} = \hat{\phi}\phi = [\deg \phi] \in \mathbb{Z}$$

Notice that the standard involution on $\mathrm{End}(E)$ is *positive* in the sense that $\mathrm{Tr}(\phi\hat{\phi}) > 0$ for every $\phi \in \mathrm{End}(E) \setminus \{0\}$, where $\mathrm{Tr} : \mathrm{End}(E)_{\mathbb{Q}} \to \mathbb{R}$ is given by the trace of the left multiplication linear map. Using this fact and Theorem 2.12 we can derive the following:

Proposition 3.14. *The endomorphism algebra* $\mathrm{End}(E)_{\mathbb{Q}}$ *is isomorphic to either* $\mathbb{Q}$*, an imaginary quadratic field* $\mathbb{K}$*, or a definite quaternion algebra over* $\mathbb{Q}$*.*

Proof. By Theorem 2.12, we just have to prove that $\mathrm{End}(E)_{\mathbb{Q}} \otimes \mathbb{R}$ is either isomorphic to $\mathbb{R}, \mathbb{C}$, or $\mathbb{H}$. We will use Lemma 2.11. If $\mathrm{End}(E)_{\mathbb{Q}} \otimes \mathbb{R} \not\simeq \mathbb{C}$ then it is isomorphic to $\mathbb{R} \times \mathbb{R}$, where the standard involution is $(x_1, x_2) \mapsto (x_2, x_1)$ and thus $\mathrm{Tr}(x_1x_2, x_1x_2) = 2x_1x_2$, which is not positive. In the other case, if $\mathrm{End}(E)_{\mathbb{Q}}$ is not definite, then $\mathrm{End}(E)_{\mathbb{Q}} \otimes \mathbb{R} \simeq M_2(\mathbb{R})$, where the standard involution is given by the adjugate map Example 2.10; thus, $\mathrm{Tr}(\det A) = 4\det(A)$, which again is not positive. The result follows. □

The Frobenius isogeny. Suppose that $\mathrm{char}(\mathbb{F}) = p \neq 2, 3$ a prime number, $q := p^r$ for some $r \in \mathbb{Z}_{>0}$, and let $E/\mathbb{F}$ be an elliptic curve given by a short Weierstrass equation of the form (15). Then, the curve with affine equation

$$y^2 = x^3 + A^q x + B^q, \tag{16}$$

defines an elliptic curve over $\mathbb{F}$, denoted by $E^{(q)}$, and there exists an isogeny

$$\pi_q : E \longrightarrow E^{(q)}; \qquad (x, y) \longmapsto (x^q, y^q),$$

which we call the *q-Frobenius isogeny* of E. When $\mathbb{F} = \mathbb{F}_q$ then $E^q = E$ and so $\pi_q \in \mathrm{End}_{\mathbb{F}}(E)$, in which case we call π_q the *q-Frobenius endomorphism*. The Frobenius isogeny is purely inseparable

with degree $\deg \pi_q = q$, by [Sil09, II.2.11]. The characteristic property of the Frobenius isogeny is that every isogeny $\phi : E \to E'$ factors as follows

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ & {\scriptstyle \pi_q} \searrow \quad \nearrow {\scriptstyle \lambda} & \\ & E^{(q)} & \end{array} \tag{17}$$

where $q = \deg_i \phi$ and $\lambda : E^{(q)} \to E'$ is a separable isogeny, see [Sil09, II.2.12].

3.2 The Tate module

Let $E/\mathbb{F}$ be an elliptic curve and ℓ be a prime number. We present here an important construction of a $\mathbb{Z}_\ell$-module that arises naturally from the structure of E and captures many properties of E. This construction will allow us to prove the quaternionic properties of $\mathrm{End}_{\mathbb{F}}(E)$.

Observe that for each $n \geq 1$ the multiplication-by-ℓ map restricts to a well-defined homomorphism

$$[\ell] : E[\ell^{n+1}] \longrightarrow E[\ell^n]. \tag{18}$$

Definition 3.15. We define the *ℓ-adic Tate module* of E as the inverse limit

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

with respect to the system of group homomorphisms (18).

Note 3.16. Since each group $E[\ell^n]$ is naturally a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, we have that $T_\ell(E)$ is naturally a $\mathbb{Z}_\ell$-module.

Lemma 3.17. *Suppose that* $\mathrm{char}(\mathbb{F}) = p$ *for some prime* $p > 0$ *and that* $E[p^n] = \{0\}$ *for every* $n \geq 0$. *Then,* $T_\ell(E) \simeq \mathbb{Z}_\ell^2$, *for* $\ell \neq p$ *prime and* $T_p(E) \simeq \{0\}$.

Proof. This follows directly from Lemma 3.8 and the assumption on the p^n-torsion part of E. □

Suppose that $\ell \neq \mathrm{char}(\mathbb{F})$. Note that the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ on E restricts to an action on $E[\ell^n]$ for every $n \geq 0$ that commutes with the maps (18). Thus, $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ acts also on the Tate module $T_\ell(E)$.

Let now $\phi : E \to E'$ be an isogeny. For every $n \geq 0$, consider the restriction maps $\phi \equiv \phi|_{E[\ell^n]} : E[\ell^n] \to E'[\ell^n]$ and observe that it commutes with the multiplication-by-ℓ map, i.e. we have the following commutative diagram

$$\begin{array}{ccc} E[\ell^n] & \xrightarrow{\phi} & E'[\ell^n] \\ {\scriptstyle [\ell]}\downarrow & & \downarrow{\scriptstyle [\ell]} \\ E[\ell^{n+1}] & \xrightarrow[\phi]{} & E'[\ell^{n+1}] \end{array}$$

Thus, ϕ induces a $\mathbb{Z}_\ell$-linear map $\phi_\ell : T_\ell(E) \to T_\ell(E')$. Note that if ϕ is an isogeny over $\mathbb{F}$, we have that ϕ commutes with the action of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ and so, by compatibility, ϕ_ℓ also commutes with the action of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ on the Tate module. For that reason, we define the group of $\mathrm{Hom}_{\mathbb{F}}(T_\ell(E), T_\ell(E'))$

as the group of $\mathbb{Z}_\ell$-homomorphisms that commute with the action of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$. Thus, the above construction gives us a natural $\mathbb{Z}_\ell$-homomorphism

$$\mathrm{Hom}_{\mathbb{F}}(E, E') \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{F}}(T_\ell(E), T_\ell(E')). \tag{19}$$

This map is always injective, by [Sil09, III.7.4], and so we have the following corollary.

Corollary 3.18. *For every elliptic curves E, E' over $\overline{\mathbb{F}}$, the $\mathbb{Z}$-module $\mathrm{Hom}_{\overline{F}}(E, E')$ is a free $\mathbb{Z}$-module of rank at most 4.*

However, Tate conjectured and proved a major result about the map (19) in the finite field case. We call the following theorem the *Isogeny theorem.*

Theorem 3.19 (Tate, [Tat66])**.** *Suppose that $\mathbb{F} = \mathbb{F}_q$, where $q = p^r$, for some $r \geq 1$, and let $\ell \neq p$ be a prime number. Then, the natural map (19)*

$$\mathrm{Hom}_{\mathbb{F}}(E, E') \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{F}}(T_\ell(E), T_\ell(E'))$$

is an isomorphism.

3.3 Supersingular Elliptic Curves

Recall that by Proposition 3.14, for an elliptic curve E, $\mathrm{End}(E)_{\mathbb{Q}}$ is either isomorphic to $\mathbb{Q}$, a quadratic field, or a quaternion algebra. We are now going to define the class of elliptic curves that corresponds to the third case. By [Sil09, III.5.6], if $\mathrm{char}(\mathbb{F}) = 0$ then $\mathrm{End}(E)_{\mathbb{Q}}$ is a commutative ring and so we suppose that $\mathrm{char}(\mathbb{F}) = p$, where $p \neq 2$ is a prime number. The following theorem provides defining properties for this class.

Theorem 3.20 (Deuring, [Deu41])**.** *Let $E/\mathbb{F}$ be an elliptic curve. The following are equivalent:*

1. $\mathrm{End}(E)_{\mathbb{Q}}$ *is a quaternion algebra;*
2. $E[p^n] = \{0\}$ *for all $n \geq 1$; and*
3. *The multiplication-by-p map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.*

Proof. See [Sil09, V.3.1]. □

Definition 3.21. We say that an elliptic curve E is *supersingular* if one of the conditions in Theorem 3.20 holds. An elliptic curve that is not supersingular is called *ordinary.*

The distinction between ordinary and supersingular elliptic curves leads also to a distinction between isogenies. Essentially, the following lemma states that isogenies are divided in those between ordinary and those between supersingular elliptic curves.

Lemma 3.22. *Let E, E' be isogenous elliptic curves. Then, E is supersingular if and only if E' is supersingular.*

Proof. Suppose that E is supersingular. Let $\phi : E \to E'$ be a non-zero isogeny with $\deg \phi = m$ and consider the $\mathbb{Z}$-linear map

$$\mathrm{End}(E) \longrightarrow \mathrm{End}(E'); \qquad \psi \longmapsto \phi \circ \psi \circ \hat{\phi}.$$

This induces a $\mathbb{Q}$-linear isomorphism $\mathrm{End}(E)_{\mathbb{Q}} \xrightarrow{\sim} \mathrm{End}(E')_{\mathbb{Q}}$, since if $\phi \circ \psi \circ \hat{\phi} = 0$ then multiplying from the left by $\hat{\phi}$ and from the right by ϕ we get that $[m^2]\psi = 0$, where in $\mathrm{End}(E)_{\mathbb{Q}}$ implies that $\psi = 0$. Therefore, $\dim_{\mathbb{Q}} \mathrm{End}(E')_{\mathbb{Q}} = \dim_{\mathbb{Q}} \mathrm{End}(E)_{\mathbb{Q}} = 4$. The result follows from Theorem 3.20 and Proposition 3.14. □

The quaternion algebra $\mathrm{End}(E)_{\mathbb{Q}}$. We are now going to determine the quaternionic properties of $\mathrm{Hom}(E, E')$, $\mathrm{End}(E)$, and $\mathrm{End}(E)_{\mathbb{Q}}$, when E, E' are supersingular elliptic curves.

Let $\mathbb{K} := \mathbb{F}_q$, where $q = p^r$ for some $r \geq 0$, and fix an algebraic closure $\overline{\mathbb{F}_q}$ of it. We begin by examining the Galois action in the finite field case. Let E be an elliptic curve over $\mathbb{K}$. Recall the q-Frobenius endomorphism π_q and notice that it is induced by the q-power map $\phi_q : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, $\phi_q(x) = x^q$. Now, for each $k \geq 0$, we have that $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ is cyclic of order k generated by ϕ_q. Then, for the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ we have the isomorphism

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \varprojlim_{k \geq 0} \mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q) \simeq \hat{\mathbb{Z}},$$

where $1 \in \hat{\mathbb{Z}}$ corresponds to ϕ_q. Thus, ϕ_q topologically generates $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. This proves that the q-Frobenius endomorphism π_q and $(\pi_q)_\ell$ generate the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ into E and on $T_\ell(E)$, respectively. For more details see [Len97, 2.5].

Lemma 3.23. *Let $E/\overline{\mathbb{F}}$ be a supersingular elliptic curve. Then, E is isomorphic to a supersingular elliptic curve defined over a finite field $\mathbb{F}_q$, where the action of the q-Frobenius map π_q is scalar.*

Proof. By Theorem 3.20, we have that $j(E) \in \mathbb{F}_{p^2}$ and so by Theorem 3.3 there exists an elliptic curve E' over $\mathbb{F}_{p^2}$ that is isomorphic to E (over $\overline{\mathbb{F}_p}$). By Corollary 3.18, $\mathrm{End}(E)$ has rank at most 4 as a $\mathbb{Z}$-module and so by taking a $\mathbb{Z}$-basis of $\mathrm{End}(E)$, each of these basis endomorphisms can be defined over a finite subfield of $\overline{\mathbb{F}_p}$; taking the biggest of these, say $\mathbb{F}_q$, we see that $\mathrm{End}(E) = \mathrm{End}_{\mathbb{F}_q}(E)$. This implies that π_q commutes with every $\phi \in \mathrm{End}(E)$ and so $\pi \in Z(\mathrm{End}(E))$. Now, since E is supersingular, $\mathrm{End}(E)_{\mathbb{Q}}$ is a quaternion algebra and so it is central, which means that $Z(\mathrm{End}(E)) = Z(\mathrm{End}(E)_{\mathbb{Q}}) \cap \mathbb{Z} = \mathbb{Z}$. Therefore, $\pi_q \in \mathbb{Z}$ and thus it is indeed scalar. □

Proposition 3.24. *Let E, E' be supersingular elliptic curves over $\overline{\mathbb{F}}$. Then, $\mathrm{Hom}(E, E')$ is a free $\mathbb{Z}$-module of rank 4.*

Proof. We have proved above that $\mathrm{Hom}(E, E')$ is indeed a free $\mathbb{Z}$-module. By Lemma 3.23, we may assume that E, E' are defined over $\mathbb{F}_q$ and that the q-Frobenius map π_q acts as a scalar on $\mathrm{Hom}(E, E')$. Let $\ell \neq p$ be a prime and consider the Tate module $T_\ell(E)$. Since the Frobenius endomorphism generates $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ we get that $\mathrm{Hom}_{\mathbb{F}_q}(E, E') = \mathrm{Hom}(E, E')$ and that $\mathrm{Hom}_{\mathbb{F}_q}(T_\ell(E), T_\ell(E')) = \mathrm{Hom}(T_\ell(E), T_\ell(E'))$. Thus, by Theorem 3.19, we have the following isomorphism

$$\mathrm{Hom}(E, E') \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}(T_\ell(E), T_\ell(E')).$$

Now, by Lemma 3.17 we get that

$$\mathrm{Hom}(T_\ell(E), T_\ell(E')) \simeq \mathrm{Hom}(\mathbb{Z}_\ell^2, \mathbb{Z}_\ell^2) \simeq M_2(\mathbb{Z}_\ell).$$

Hence, $\mathrm{rank}_{\mathbb{Z}} \mathrm{Hom}(E, E') = \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Hom}(E, E') \otimes \mathbb{Z}_\ell = \mathrm{rank}_{\mathbb{Z}_\ell} M_2(\mathbb{Z}_\ell) = 4$. □

Theorem 3.25. *Let E be a supersingular elliptic curve. Then $B := \mathrm{End}(E)_{\mathbb{Q}}$ is a definite quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞ and $\mathcal{O} := \mathrm{End}(E)$ is a maximal order in $\mathrm{End}(E)_{\mathbb{Q}}$.*

Proof. Note first that by Theorem 3.20 and Proposition 3.14, $\mathrm{End}(E)_{\mathbb{Q}}$ is a definite quaternion algebra and that by Proposition 3.24, $\mathrm{End}(E)$ is indeed an order in $\mathrm{End}(E)_{\mathbb{Q}}$. Let $\ell \neq p$ be a prime number. Then, by the proof of Proposition 3.24, we have an isomorphism

$$\mathrm{End}(E) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}(T_\ell(E), T_\ell(E)) \simeq M_2(\mathbb{Z}_\ell). \tag{20}$$

Note that by construction this map is also a ring homomorphism. Therefore, $\mathrm{End}(E)_{\mathbb{Q}} \otimes \mathbb{Q}_\ell \simeq M_2(\mathbb{Q}_\ell)$ as $\mathbb{Q}_\ell$-algebras and so B is split at every $\ell \neq p$. Now, since B is definite, by Theorem 2.39, we have that $B \otimes \mathbb{Q}_p$ is a division algebra and so $\mathrm{Ram}(B) = \{p, \infty\}$.

Now, isomorphism (20) also means that for every prime $\ell \neq p$, $\mathcal{O}_\ell \simeq M_2(\mathbb{Z}_\ell)$ and so it is maximal in $B_\ell \simeq M_2(\mathbb{Q}_\ell)$, by Proposition 2.64. In light of Lemma 2.63, which states that maximality is a local property, we are left to prove that $\mathcal{O}_p$ is maximal in the division algebra B_p. Recall from (2.6) that the unique maximal order of B_p is its valuation ring $\{\alpha \in B_p \colon w(\alpha) \geq 0\}$, where the valuation $w : B \to \mathbb{R} \cup \{\infty\}$ is defined as $w(\alpha) = \frac{1}{2} v_p(\mathrm{nrd}(\alpha))$, $\alpha \in B$. Therefore, we want to prove that for every $\alpha \in B_p$ with $w(\alpha) \geq 0$ it follows that $\alpha \in \mathcal{O}_p$. By Proposition 2.31, it is enough to prove that $\mathcal{O}_{(p)} = \{\alpha \in B_{(p)} \colon w(\alpha) \geq 0\}$. We begin by making the following claim:

Claim. If $\phi \in \mathcal{O}$ then $v_p(\deg \phi) = v_p(\deg_i \phi)$.

Proof of Claim. If $p \mid \deg \phi$ then either $p \mid \deg_i \phi$, in which case we are done, or $p \mid \deg_s \phi$, in which case $\ker \phi$ contains a subgroup of order p and so, by [Sil09, III.4.11,III.4.12], we have that ϕ factors through an isogeny of degree p. Thus we may assume that $\deg \phi = p$. Then, $[p] = \phi \circ \hat{\phi}$, from where we get that $\deg_i \phi \deg_i \phi = \deg_i [p] = \deg [p] = p^2$, since $[p]$ is purely inseparable, by Theorem 3.20. Now, since $\deg \phi = p$ we have that $\deg_i \phi, \deg_i \hat{\phi} \leq p$; hence $\deg_i \phi = \deg_i \hat{\phi} = p$, which proves the claim.

Now, let $\alpha \in B_{(\mathfrak{p})}$ with $w(\alpha) \geq 0$ and write it as $\alpha = a\phi$, where $a \in \mathbb{Q}$ and $\phi \in \mathcal{O} = \mathrm{End}(E)$ is an isogeny not divided by an integer. Then, it holds that $0 \leq v_p(\deg_i \phi) \leq 1$. Indeed, if $p^2 \mid \deg_i \phi$ then by (17), there exists an isogeny $\psi : E^{(p^2)} \to E$ such that $\phi = \psi \circ \pi_{p^2}$. Note also that as above and again by (17), $[p] = \lambda \circ \pi_{p^2}$ for some isomorphism λ, since by comparing degrees it follows that $\deg \lambda = 1$. Therefore, $\phi = \psi \circ \lambda^{-1} \circ \pi_{p^2}$, a contradiction to the fact that ϕ is not divisible by an integer. From this and the above claim we get that

$$w(\alpha) = \frac{v_p(a\phi)}{2} = v_p(a) + \frac{v_p(\deg \phi)}{2} = v_p(a) + \frac{v_p(\deg_i \phi)}{2}.$$

and that $0 \leq v_p(\deg_i \phi)/2 \leq 1/2$. Therefore, since $w(\alpha) \geq 0$, we get that $v_p(a) \geq -1/2$; hence $a \in \mathbb{Z}_{(p)}$ and $\alpha \in \mathcal{O}_{(p)} = \mathcal{O} \otimes \mathbb{Z}_{(p)}$. Thus, $\mathcal{O}_p$ is a maximal order in B_p, as desired. □

3.4 Kernel ideals

In this section we will make use of the language of group schemes, where we need the results of W. C. Waterhouse [Wat69]. For proofs and further details see also [Voi21, 42.2].

Consider a field $\mathbb{F}$ of positive characteristic $\mathrm{char}\mathbb{F} = p \neq 2$ and fix an algebraic closure $\overline{\mathbb{F}}$ of it. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}$ and set $\mathcal{O} := \mathrm{End}(E)$ and $B := \mathrm{End}(E)_{\mathbb{Q}}$. By the previous section we know that B is a definite quaternion algebra ramified only at the finite prime p and at ∞ and that $\mathcal{O}$ is a maximal order in B.

Let $I \subseteq \mathcal{O}$ be an integral $\mathcal{O}$-ideal in B. We define the scheme-theoretic intersection

$$E[I] := \bigcap_{\alpha \in I} E[\alpha],$$

where $E[\alpha] := \ker \alpha$, where we consider it as a *group-scheme* over $\mathbb{F}$. Note that $E[I]$ is a finite subgroup of E and consider its group-scheme quotient $E_I := E/E[I]$. By [Sil09, III.4.12], there exists an isogeny

$$\phi_I : E \longrightarrow E_I,$$

for which it holds that $\deg(\phi_I) = \mathrm{nrd}(I)$, see [Voi21, 42.2.16]. Note that, by Lemma 3.22, the existence of ϕ_I implies that E_I is also a supersingular elliptic curve. In this section we are going to state some lemmas that will help us in the proof of the Deuring Correspondence in (5.2.2). For proofs see also [Voi21, 42.2].

Lemma 3.26. *If $I, J \subseteq \mathcal{O}$ are integral right $\mathcal{O}$-ideals with $[I] = [J]$ then $E_I \simeq E_J$.*

Lemma 3.27. *Given an integral right $\mathcal{O}$-ideal I, the pullback map induced by $\hat{\phi}_I$*

$$\mathrm{Hom}(E, E_I) \xrightarrow{\hat{\phi}_I^*} I; \qquad \psi \longmapsto \hat{\phi}_I \phi$$

is an isomorphism of right $\mathcal{O}$-modules.

Lemma 3.28. *For every isogeny $\phi : E \to E'$, there exists a right $\mathcal{O}$-ideal I and an isomorphism $\rho_I : E_I \to E'$ such that $\phi = \rho\phi_I$.*

4 Modular Forms

In this section we introduce the theory of modular forms which plays the central role in the proof of the Ramanujan bound for Pizer graphs, see (5.1). We follow [DS05].

4.1 Definitions

Consider the *full modular group*

$$\mathrm{SL}_2(\mathbb{Z}) := \{A \in M_2(\mathbb{Z})\colon \det A = 1\},$$

$\mathrm{SL}_2(\mathbb{Z})$ defines an action on the complex upper half-plane $\mathcal{H} := \{z \in \mathbb{C}\colon \Im z > 0\}$ by *fractional linear transformations* as follows:

$$\gamma \cdot z := \frac{az+b}{cz+d}, \qquad \gamma \in \mathrm{SL}_2(\mathbb{Z}), z \in \mathcal{H}. \tag{21}$$

The denominator of the above fraction is denoted by $j(\gamma, z) := cz + d \in \mathbb{C}^\times$ and is called the *factor of automorphy*. Via direct calculations j satisfies the following relation, called the *cocycle relation*:

$$j(\gamma\gamma'; z) = j(\gamma; \gamma' \cdot z) j(\gamma'; z), \qquad \gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z}), z \in \mathcal{H}. \tag{22}$$

Definition 4.1. Let $N \in \mathbb{Z}_{\geq 1}$. We define the *principal congruence subgroup of level* N as the subgroup of $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma(N) := \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z})\colon \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N\right\}, \tag{23}$$

where the defining congruence for $\Gamma(N)$ is interpreted entry-wise. A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is called a *congruence subgroup* if there exists $N \in \mathbb{Z}_{\geq 1}$ such that $\Gamma(N) \subseteq \Gamma$. The least such N is called the *level* of Γ.

Remark 4.2. Let $N \in \mathbb{Z}_{\geq 1}$. The principal congruence subgroup $\Gamma(N)$ is the kernel of the reduction map

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

which can be shown to be surjective. Thus, $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] \leq \#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. This also shows that every congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is of finite index in $\mathrm{SL}_2(\mathbb{Z})$.

For the purposes of this thesis we need in particular the following congruence subgroup:

$$\Gamma_0(N) := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})\colon c \equiv 0 \pmod N\right\}$$

Note that the subgroup $\Gamma(N)$ is a normal subgroup of $\Gamma_0(N)$ with index $[\Gamma_0(N) : \Gamma(N)] = N$ as the following isomorphism suggests

$$\Gamma(N)/\Gamma_0(N) \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z}; \qquad \Gamma_0(N)A \longmapsto b \pmod N,$$

where b is the upper right entry of A.

In order to study modular forms over arbitrary congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, we attach to $\mathcal{H}$ the *projective line over* $\mathbb{Q}$, $\mathbb{P}^1(\mathbb{Q}) := \mathbb{Q} \cup \{\infty\}$. Set $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ and note that the action (21) of $\mathrm{SL}_2(\mathbb{Z})$ by fractional linear transformations extends to an action on $\mathcal{H}^*$, by the same formula (21), where we interpret the fraction as a limit when needed.

Remark 4.3. Note that the action of $\mathrm{SL}_2(\mathbb{Z})$ to $\mathbb{P}^1(\mathbb{Q})$ is transitive. Indeed, if $t \in \mathbb{Q}$, we write it as $t = \frac{a}{c}$, for some $a, c \in \mathbb{Z}$ coprime. Thus, there exist $b, d \in \mathbb{Z}$ such that $ad - bc = 1$ and the matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ satisfies $\gamma \cdot \infty = t$.

Definition 4.4. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. We define the *cusps of* Γ as the Γ-orbits in $\mathbb{P}^1(\mathbb{Q})$ and we denote them by $\mathrm{Cusp}(\Gamma) := \Gamma \setminus \mathbb{P}^1(\mathbb{Q})$.

Note 4.5. The set of cusps of a congruence subgroup Γ is finite. Indeed, the stabiliser of $\infty \in \mathbb{P}^1(\mathbb{Q})$ under the action of $\mathrm{SL}_2(\mathbb{Z})$ is

$$\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$$

and so we get a bijection

$$\mathrm{SL}_2(\mathbb{Z}) / \mathrm{SL}_2(\mathbb{Z})_\infty \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q}); \qquad \gamma \, \mathrm{SL}_2(\mathbb{Z})_\infty \longmapsto \gamma \cdot \infty.$$

This induces a surjective map

$$\Gamma \setminus \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{Cusp}(\Gamma),$$

which shows the claim as a congruence subgroup is of finite index in $\mathrm{SL}_2(\mathbb{Z})$, by Remark 4.2.

Let now $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function on $\mathcal{H}$ and $k \in \mathbb{Z}_{\geq 0}$. We define the *slash operator of weight* k as the action of $\mathrm{SL}_2(\mathbb{Z})$ on f defined by:

$$(f|_k\gamma)(z) := j(\gamma, z)^{-k} f(\gamma \cdot z)$$

Notice that since the factor of automorphy $j(\gamma, z)$ is never 0 or ∞, the function $f|_k\gamma$ is again holomorphic with the same zeroes as f.

Definition 4.6. Let $k \in \mathbb{Z}_{\geq 0}$ and $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ a congruence subgroup. A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is called *weakly modular of weight* k *for* Γ if it is invariant under the action of the slash operator under Γ, i.e. if for all $\gamma \in \Gamma$ we have that $f|_k\gamma = f$.

Let $k \in \mathbb{Z}_{\geq 0}$ and a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ that is weakly modular of weight k for Γ. Every congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ contains a matrix of the form $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$, for some $h \in \mathbb{Z}_{\geq 1}$, which acts on $\mathcal{H}$ as the translation by h. Let h be the minimal such positive integer. Thus, since f is weakly modular, it is $h\mathbb{Z}$-periodic. Set $q_h := e^{2\pi i z/h}$. The latter implies that f can be written as $f(z) = \tilde{f}(q_h)$, for some meromorphic function $\tilde{f}$ on the punctured disk $\mathbb{D}^* = \{q \in \mathbb{C} \mid 0 < |q| < 1\}$. We say that f is *holomorphic at* ∞ if $\tilde{f}$ can be continued to a holomorphic function on the disk $\mathbb{D} = \{q \in \mathbb{C} \mid |q| < 1\}$, or equivalently if it can be written as a power series

$$\tilde{f}(q_h) = \sum_{n=0}^{\infty} a_n q_h^n, \tag{24}$$

for some $a_n \in \mathbb{C}$ that is convergent on some punctured disk $\{q \in \mathbb{C} \colon 0 < |q| < \epsilon\}$ for some $\epsilon > 0$. We call the expression (24) of f, the *q-expansion of* f *at* ∞. If f is holomorphic at ∞ we also define its *value at infinity* as $f(\infty) := \tilde{f}(0) = a_0$.

In general, we define holomorphy at an arbitrary cusp using the notion of holomorphy at ∞ as follows. Let $c \in \mathrm{Cusp}(\Gamma)$ and let $t \in \mathbb{P}^1(\mathbb{Q})$ be a an element in its Γ-orbit. By Remark 4.3, we know that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$ and so there exists $\gamma_t \in \mathrm{SL}_2(\mathbb{Z})$ such that $t = \gamma_t \cdot \infty$. It can be readily seen that $f|_k\gamma_t$ is again a holomorphic function that is weakly modular of weight k for the congruence subgroup $\gamma_t^{-1}\Gamma\gamma_t \subseteq \mathrm{SL}_2(\mathbb{Z})$. Thus, we may define f to be *holomorphic at the cusp* c if $f|_k\gamma_t$ is holomorphic at ∞ and we define the *value of* f *at the cusp* c as $(f|_k\gamma_t)(\infty)$.

We are finally ready to define the notion of a modular form.

Definition 4.7. Let $k \in \mathbb{Z}_{\geq 0}$, $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ a congruence subgroup and a function $f : \mathcal{H} \to \mathbb{C}$. We say that f is a *modular form of weight* k *for* Γ if

1. f is holomorphic on $\mathcal{H}$;
2. f is weakly modular of weight k for Γ; and
3. f is holomorphic at every cusp $\gamma \in \mathrm{Cusp}(\Gamma)$.

If further f vanishes at every cusp, i.e. the value of f at every cusp is 0, then it is called a *cusp form of weight* k *for* Γ. We denote by $M_k(\Gamma)$ the $\mathbb{C}$-vector space of modular forms of weight k for Γ and by $S_k(\Gamma)$ its subspace of cusp forms.

In studying modular forms we are particularly interested in cusp forms. This is because for $k \geq 2$, we have that $M_k(\Gamma) = S_k(\Gamma) \oplus E_k(\Gamma)$, where $E_k(\Gamma)$ is the space of *Eisenstein series*, which subspace of modular forms is better understood than cusp forms.

4.2 Hecke Operators

One major tool in the study of cusp forms are the *Hecke operators*, which are operators on the space $S_k(\Gamma)$. For the purposes of this thesis we only need to define the Hecke operators over the congruence subgroup $\Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ for $N \in \mathbb{Z}_{\geq 0}$ and for $(n, N) = 1$. In this section we follow [Voi21, 40.5]. Let $N \in \mathbb{Z}_{\geq 1}$ and set $\Gamma := \Gamma_0(N)$.

For every $n \in \mathbb{Z}_{\geq 1}$ with $(n, N) = 1$ we define the set of matrices

$$\Gamma_n := \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \colon N \mid c, \det \alpha = n \right\}.$$

Note that Γ acts on Γ_n by multiplication on the left (and on the right).

Let $k \in \mathbb{Z}_{\geq 0}$ and $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function. We extend the definition of the slash operator on the bigger group $\mathrm{GL}_2^+(\mathbb{Q}) := \{\alpha \in M_2(\mathbb{Q}) \mid \det \alpha > 0\}$, by

$$(f|_k\alpha)(z) := \frac{(\det \alpha)^k}{j(\alpha; z)^k} f(\alpha \cdot z), \qquad \alpha \in \mathrm{GL}_2^+(\mathbb{Q}),\ z \in \mathcal{H},$$

where the factor of automorphy $j(\alpha, z)$ and $\alpha \cdot z$ are defined again as in (21). Note that if f is weakly modular of weight k and $\alpha \in \Gamma_n$ then $f|_k\alpha$ depends only on the class of α in $\Gamma \setminus \Gamma_n$, which can be seen using the cocycle relation (22).

Definition 4.8. For $n \in \mathbb{Z}_{\geq 1}$, $(n, N) = 1$. The *n-Hecke operator* $T_n : M_k(\Gamma) \to M_k(\Gamma)$ is defined as follows: for $f \in M_k(\Gamma)$ let

$$T_n f := \frac{1}{n} \sum_{\Gamma\alpha \in \Gamma\setminus\Gamma_n} f|_k\alpha$$

The operators T_n are well defined. Indeed, if $f \in M_k(\Gamma)$ then $T_n f \in M_k(\Gamma)$ by the fact that f is weakly modular of weight k for Γ and the cocycle relation (22). Also, by applying row operations one can see that a set of representatives of $\Gamma \setminus \Gamma_n$ for $(n, N) = 1$ is

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \colon a > 0, ad = n, 0 \leq b < d \right\}$$

and so the sum defining $T_n f$ is finite. In particular, using the above set of representatives we get a more explicit description of T_n:

$$(T_n f)(z) = n^{k-1} \sum_{\substack{ad=n \\ a>0}} \frac{1}{d^k} \sum_{b=0}^{d-1} f\left(\frac{az+b}{d}\right). \tag{25}$$

The effect of the Hecke operators on the q-expansion of a modular form $f \in M_k(\Gamma)$ can be seen from (25) as follows: let $\tilde{f}(q) = \sum_{n=0}^{\infty} a_n q^n$ be the q-expansion of f at ∞, then

$$a_m(T_n f) = \sum_{\substack{d|(m,n) \\ d>0}} d^{k-1} a_{mn/d^2} \tag{26}$$

Remark 4.9. In particular, we see from (26) that if $a_0 = 0$ then $b_0 = 0$ and by repeating this process for every $f|_k\gamma$, $\gamma \in \Gamma$, we have that T_n restricts to an operator $T_n : S_k(\Gamma) \to S_k(\Gamma)$.

The Hecke operators satisfy a recursive relation, which enables us to compute them only from the operators T_p, $p \nmid N$.

Proposition 4.10. *Let $m, n \in \mathbb{Z}_{\geq 1}$ such that $(m, N) = (n, N) = 1$. Then,*

$$\begin{aligned} T_{mn} &= T_m T_n, && \text{if } (m, n) = 1 \\ T_p T_{p^r} &= T_{p^{r+1}} + p^{k-1} T_{p^{r-1}}, && \text{if } m = p, n = p^r, r \in \mathbb{Z}_{\geq 1}. \end{aligned}$$

Proof. This follows from the formulas (26). □

In order to study the spaces $M_k(\Gamma)$ and $S_k(\Gamma)$ spectrally we need the following notion.

Definition 4.11. We call a non-zero modular form $f \in M_k(\Gamma)$ an *eigenform* for the Hecke operator T_n, $n \geq 1$, if it is an eigenfunction for T_n. An eigenform $f \in M_k(\Gamma)$ is called *normalised* if $a_1(f) = 1$.

Remark 4.12. If $f \in M_k(\Gamma)$ is an eigenform for T_n then there exists an eigenvalue λ_n such that $T_n f = \lambda_n f$. Thus, using (26), we get that

$$a_n(f) = a_1(T_n f) = \lambda_n a_1(f). \tag{27}$$

Therefore, if f is normalised, we have that $\lambda_n = a_n(f)$.

The next main step is to define an inner product on the space of cusp forms $S_k(\Gamma)$.

Definition 4.13. We define the *Petersson inner product* on $S_k(\Gamma)$ as follows:

$$\langle f, g \rangle := \int_{\Gamma z \in \Gamma \setminus \mathcal{H}} f(z)\overline{g(z)}(\Im(z))^k d\mu(z),$$

where $d\mu(z) := \frac{dxdy}{y^2}$, where $z = x + yi \in \mathbb{C}$, is the $\mathrm{SL}_2(\mathbb{Z})$-invariant hyperbolic measure on $\mathcal{H}$.

This inner product is well-defined and it is a positive definite, non-degenerate inner product on the $\mathbb{C}$-vector space $S_k(\Gamma)$, see [DS05, 5.4].

Theorem 4.14. *The Hecke operators $T_n, (n, N) = 1$, form a commuting system of normal operators on $S_k(\Gamma)$ equipped with the Petersson inner product.*

Proof. The commutativity of the operators can be seen directly from (26). For the fact that these operators are normal with respect to the Petersson inner product, see [DS05, 5.5.3]. □

The Spectral theorem from linear algebra states that given a commuting family of normal operators on a finite-dimensional inner product space, the space has an orthogonal basis of simultaneous eigenvectors for the operators. Therefore, we conclude the following.

Corollary 4.15. *The space $S_k(\Gamma)$ admits a basis consisting of simultaneous eigenforms for the Hecke operators T_n, $(n, N) = 1$.*

4.3 Ramanujan-Petersson Conjecture

We follow [Ser73, VII.6.3] and [Kat76]. Let $f \in S_k(\Gamma)$ be a cusp form that is a normalised eigenform for all Hecke operators $T_n, n \geq 1$, and let $f(q) = q + \sum_{n=2}^{\infty} a_n q^n$ be its q-expansion. Then, by [DS05, 5.9.1], f has an associated Dirichlet series, called the *L-function* of f at s defined by

$$L(f, s) := \sum_{n=1}^{\infty} a_n n^{-s},$$

which converges absolutely in a half-plane of s-values. Since f is an eigenform, by [DS05, 5.9.2], the L-function $L(f, s)$ admits an Euler product of the form

$$L(s, f) = \prod_{p:\ \text{prime}} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}} \tag{28}$$

The fact that $L(f, s)$ can be written as the above Euler product is equivalent to the fact that a_n satisfies the recursive relations

(1) $a_{mn} = a_m a_n$, for $(m, n) = 1$,

(2) $a_{p^{n+1}} = a_p a_{p^n} + p^{k-1} a_{p^{n-1}}$. for $n \geq 1$.

These recursive relations are immediate from (26) and Remark 4.12. Let now p be a prime number and consider the polynomial arising from the denominator of the Euler product (28)

$$\Phi_{f,p}(T) := 1 - a_p T + p^{k-1} T^2.$$

We can rewrite this polynomial as $\Phi_{f,p}(T) = (1 - c_p T)(1 - c'_p T)$, where $c_p, c'_p \in \mathbb{C}$ satisfying $c_p + c'_p = a_p$ and $c_p c'_p = p^{k-1}$. The *Ramanujan-Petersson conjecture*, introduced by Petersson in [Pet40], states that c_p, c'_p are complex conjugates. From this, using the triangle inequality we can conclude that

(3) $|a_p| \leq 2p^{(k-1)/2}$, or more generally that $|a_n| \leq \sigma_0(n) p^{(k-1)/2}$,

where the general inequality follows from the special as in [Kob84, II.6.13].

The original Ramanujan Conjecture consists of the parts (1),(2), and (3) for a particular cusp form of weight 12, namely the cusp form

$$\Delta(q) := q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n,$$

where the coefficients $\tau(n)$ is the so-called *Ramanujan tau function*. The first two parts of the original Ramanujan conjecture were proved by Mordell [Mor17], which work also motivated Hecke to define his operators. For the third and most difficult part of the Ramanujan-Petersson conjecture for cusp forms of weight $k \geq 2$, Deligne [Del71] proved that it can be reduced to the Weil conjectures. Deligne [Del73] proved it for weight $k \geq 3$ and Eichler-Shimura [Eic54, Shi58] proved it for weight $k = 2$. Thus, we have the following theorem.

Theorem 4.16. *Let $k \in \mathbb{Z}_{\geq 2}$ and let $n \in \mathbb{Z}_{\geq 1}$ be such that $(n, N) = 1$. Then, every eigenvalue λ of T_n acting on $S_k(\Gamma)$ satisfy the Ramanujan bound*

$$|\lambda| \leq \sigma_0(n)n^{(k-1)/2}.$$

4.4 Theta Series

Theta series are modular forms that arise from quadratic forms. The quadratic forms in this thesis will be integral, in the sense that they are maps $\mathbb{Z}^m \to \mathbb{Z}$, as they will arise from lattices in quaternion algebras over $\mathbb{Q}$. Thus, we need a slight generalization of quadratic forms over PID's. We follow [Lam73] and [Voi21, 9.7,40.4]

Let R be a PID and let $\mathbb{F} := \mathrm{Frac}(R)$ be its field of fractions. A *quadratic form over R* in $m = 2k \in \mathbb{Z}$ variables is map $Q : R^m \to \mathbb{F}$ satisfying

- $Q(rx) = r^2Q(x)$, for all $x \in R^m$ and $r \in R$; and
- the map $T_Q : R^m \times R^m \to \mathbb{F}$ defined by

$$T_Q(x, y) := Q(x + y) - Q(x) - Q(y), \qquad x, y \in R^m$$

  is R-bilinear.

If the image of Q is inside R, we say that Q is *integral*. The map T_Q is called the *associated bilinear form* to Q. Observe that it is symmetric such that $T_Q(x, x) = 2Q(x)$ and so the quadratic map can be recovered by T_Q. Therefore, given a symmetric R-bilinear map $T : R^m \times R^m \to \mathbb{F}$, the map $Q : R^m \to \mathbb{F}$ defined by $Q(x) := \frac{1}{2}T(x, x)$, $x \in R^m$, is a quadratic form over R. If Q is integral then, considering a basis $e_1, \ldots, e_m$ for R^m, we may define the matrix of the bilinear form T_Q as $A_Q := (T_Q(e_i, e_j))_{1\leq i,j\leq m}$, which is a symmetric matrix with even diagonal. Therefore, the quadratic form Q can be written as $Q(x) = \frac{1}{2}x^T A_Q x$, $x \in R^m$.

Note 4.17. A quadratic form behaves well with tensoring. In particular, for every prime ideal $\mathfrak{p}$ in R, the map $Q_\mathfrak{p} := Q \otimes_R R_\mathfrak{p} : R_\mathfrak{p}^m \to \mathbb{F}_\mathfrak{p}$ is again a quadratic form over $R_\mathfrak{p}$.

Definition 4.18. Let $Q : \mathbb{Z}^m \to \mathbb{Z}$ be an integral quadratic form. The *level* of Q is defined as the minimum natural number $N \in \mathbb{Z}_{>0}$ such that $NA_Q^{-1} \in M_2(\mathbb{Z})$ and has even diagonal.

Remark 4.19. Note that since the level a quadratic form $Q : \mathbb{Z}^m \to \mathbb{Z}$ is a positive integer and that quadratic forms behave well with tensor products, it can be computed locally. Note also that the level is stable under base change since if $\tau : \mathbb{Z}^m \to \mathbb{Z}^m$ is a $\mathbb{Z}$-linear isomorphism given by a non-singular matrix $U \in \mathrm{GL}_m(\mathbb{Z})$, then $A_{Q\circ\tau} = U^T A_Q U$, and the level of $A_{Q\circ\tau}$ equals the level of A_Q.

Definition 4.20. Let $Q, Q' : R^m \to \mathbb{F}$ be quadratic forms over a R. An *isometry* between Q, Q' is an R-linear isomorphism $\tau : R^m \to R^m$ such that $Q'(x) = Q(\tau(x))$ for every $x \in R^m$. The quadratic forms Q, Q' are called *isometric* if there exists an isometry between them, in which case we write $Q \sim Q'$. We also say that Q, Q' are *of the same genus* if they are locally isometric, i.e. for every prime ideal $\mathfrak{p} \subseteq R$ we have that $Q_\mathfrak{p} \sim Q'_\mathfrak{p}$.

We now define the *theta series* associated to integral quadratic forms. Let $m = 2k \in 2\mathbb{Z}$ be a natural number and consider an integral quadratic form $Q : \mathbb{Z}^m \to \mathbb{Z}$ that is *positive definite*, i.e. $Q(x) > 0$ for all $x \in \mathbb{Z}^m \setminus \{0\}$.

Definition 4.21. The *theta series* of Q is defined as the function $\theta_Q : \mathcal{H} \to \mathbb{C}$ defined by

$$\theta_Q(z) := \sum_{x\in\mathbb{Z}^m} e^{2\pi i Q(x) z} = \sum_{n=0}^{\infty} r_Q(n) q^n,$$

where $r_Q(n) = \#\{x \in \mathbb{Z}^m \colon Q(x) = n\}$ are the *representation numbers* of the quadratic form Q.

Since Q is assumed to be positive definite, there exists $C > 0$ such that for every $x \in \mathbb{Z}^m$, we have $Q(x) \geq C \sum_{i=1}^m x_i^2$ and so $r_Q(n) \leq Cn^k$; in particular $r_Q(n)$ is finite. Moreover, by [Miy89, 4.3.3] this implies that θ_Q converges absolutely and uniformly to a holomorphic function $\mathcal{H} \to \mathbb{C}$. See also [Ogg69, Chapter 6]. In fact more is true, using the Poisson-summation formula, it can be shown that these theta series turn out to be modular forms for specific congruence subgroups.

Theorem 4.22 (Schoeneberg)**.** *Let $m = 2k \in 2\mathbb{Z}$ be a natural number and let $Q : \mathbb{Z}^m \to \mathbb{Z}$ be a positive definite integral quadratic form of level $N \in \mathbb{Z}_{\geq 1}$. Then, the theta series θ_Q of Q is a modular form of weight k for the congruence subgroup $\Gamma_0(N)$.*

Proof. See [Ogg69, 6.10]. □

We list here also a result due to C. Siegel [Sie35, p. 577], that will help us prove that our theta series defined in (5.1.4) are indeed cusp forms.

Theorem 4.23. *Let $Q, Q' : \mathbb{Z}^m \to \mathbb{Z}$ be quadratic forms of the same genus. Then, the differences of the theta series of Q, Q', respectively, are cusp forms, i.e. $\theta_Q - \theta_{Q'} \in S_k(\Gamma_0(N))$.*

Proof. For a proof see [Wal94]. □

5 Explicit Constructions

5.1 Pizer Construction

In this section, we present Pizer's construction [Piz98] of infinite families of Ramanujan graphs, which arise from Eichler orders in quaternion algebras over $\mathbb{Q}$. In short, Pizer defines his Ramanujan graphs as the graphs $\mathcal{G}_{pN}(n)$ with adjacency matrices the so-called *Brandt matrices* $\mathcal{B}_{pN}(n), (n, pN) = 1$, defined in (5.1) associated to an Eichler order $\mathcal{O}$ of level $N \in \mathbb{Z}_{\geq 1}$ in the quaternion algebra $B_{p,\infty}$ (see (5.1.1)), for some prime number p, under some technical conditions that make these matrices symmetric with even diagonal. The Brandt matrices form a commuting system of normal matrices and satisfy the same recursive relations as the Hecke operators, see Proposition 4.10 and Proposition 5.5. Their order is computed by the Eichler mass formula Corollary 5.11, which uses the *Eichler trace formula* Theorem 5.9. Pizer gives an effective algorithm for computing the Eichler trace formula in his paper [Piz80a]. The proof of the Ramanujan bound for these graphs is attained by the following method: we first construct a space of theta series (4.4) associated to right ideals in $\mathrm{Cls}_R(\mathcal{O})$ via the reduced norm $\mathrm{nrd} : B_{p,\infty} \to B_{p,\infty}$, which defines a quadratic form on $\mathbb{Q}$. After some modifications to these theta series we construct a certain subspace of eigenforms $\Phi \subseteq S_2(\Gamma_0(N))$ for the Hecke operators T_n, such that the action of T_n on Φ has a matrix representation given by the Brandt matrices $\mathcal{B}_{pN}(n)$. Thus, the Ramanujan bound on the graphs $\mathcal{G}_{pN}(n)$ will follow from the Ramanujan-Petersson conjecture Theorem 4.16.

5.1.1 Brandt Matrices

Let $R := \mathbb{Z}$, p be a prime number, and let $B := B_{p,\infty}$ be the unique quaternion algebra ramified exactly at p and ∞, see Theorem 2.39. Let $\mathcal{O}$ be an Eichler order of level $N \in \mathbb{Z}_{\geq 1}$ in B, with N prime to p, and consider the right class set $\mathrm{Cls}(\mathcal{O}) := \mathrm{Cls}_R(\mathcal{O})$ of $\mathcal{O}$. By (2.7), the local description of $\mathcal{O}$ is given as follows:

- $\mathcal{O}_p$ is the unique maximal order in the division algebra B_p;
- For every prime number $q \neq p$ we have an isomorphism, given by a conjugation,

$$\mathcal{O}_q \simeq \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^e\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$$

  where $e = v_p(N)$.

By Remark 2.61, we know that the class number $h := h(\mathcal{O})$ of $\mathcal{O}$ is finite. Let $I_1, \ldots, I_h$ be representative of the classes of invertible right $\mathcal{O}$-ideals in $\mathrm{Cls}(\mathcal{O})$. Let also $\mathcal{O}_i := \mathcal{O}_L(I_i)$ denote the left order of I_i for each $i = 1, \ldots, h$, and note that each $\mathcal{O}_i^\times$ is a finite group, by [Voi21, 17.5.6]. Set $e_i := \#\mathcal{O}_i^\times$.

We define the central object of this thesis. It was first defined by Brandt [Bra43].

Definition 5.1. For a non-zero $n \in \mathbb{Z}$ we define the *n-Brandt matrix* associated to the order $\mathcal{O}$ in $B_{p,\infty}$, denoted by $\mathcal{B}_{pN}(n)$, as the $h \times h$ matrix with entries

$$\mathcal{B}_{pN}(n)_{i,j} := \#\left\{ J \subseteq I_j : \begin{array}{c} J \text{ invertible right } \mathcal{O}\text{-ideal}, \\ \mathrm{nrd}(J) = n\,\mathrm{nrd}(I_j), \\ \text{and } \ [J] = [I_i] \end{array} \right\} \tag{29}$$

for $i, j = 1, \dots, h$.

Note that essentially the n-Brandt matrix $\mathcal{B}_{pN}(n)$ counts the number of invertible right $\mathcal{O}$-ideals with respect to the their class in $\mathrm{Cls}(\mathcal{O})$. From now on, we will omit that J is a right invertible $\mathcal{O}$-ideal in the definition of $\mathcal{B}_{pN}(n)$, which will be apparent by the condition $[J] = [I_i]$.

Note 5.2. As the notation suggests, the Brandt matrix $\mathcal{B}_{pN}(n)$ is independent (up to a permutation matrix) of the particular Eichler order of level N and of the choice of representatives of the right $\mathcal{O}$-ideals in $\mathrm{Cls}(\mathcal{O})$. This is not hard to see and we refer to the proof of [Piz80a, 1.21,2.18] or [Piz80b, 4.2,4.3]. Note that while Pizer uses an adelic argument to prove the independence from the particular order, the argument can be replaced by a simpler one using a *connecting ideal* for the two different Eichler orders of level N, see [Voi21, 17.4].

Remark 5.3. We can derive an equivalent description of the n-Brandt matrix $\mathcal{B}_{pN}(n)$ which is

$$\mathcal{B}_{pN}(n)_{i,j} = \#\left\{ J \subseteq O_j \colon \begin{array}{c} \mathrm{nrd}(J) = n \\ \text{and } [JI_j] = [I_i] \end{array} \right\} \tag{30}$$

This follows from the fact that the map $J \longmapsto JI_j^{-1}$ establishes a bijection between the defining sets of (29) and (30). Indeed, if $J \subseteq I_j$ is in the defining set of $\mathcal{B}_{pN}(n)_{i,j}$ then $JI_j^{-1} \subseteq I_j I_j^{-1} = \mathcal{O}_j$ and the product JI_j^{-1} is compatible since $\mathcal{O}_R(J) = \mathcal{O} = \mathcal{O}_R(I_j)$. Thus, by Lemma 2.54, we get that $\mathrm{nrd}(JI_j^{-1}) = \mathrm{nrd}(J)\,\mathrm{nrd}(I_j)^{-1} = n$.

A more useful description of $\mathcal{B}_{pN}(n)$ is given by the following lemma:

Lemma 5.4. *Let $n \in \mathbb{Z}$ be a non-zero integer. Then,*

$$\mathcal{B}_{pN}(n)_{i,j} = \frac{1}{e_i} \# \left\{ \alpha \in I_j I_i^{-1} \colon \mathrm{nrd}(\alpha) = \pm n \frac{\mathrm{nrd}(I_j)}{\mathrm{nrd}(I_i)} \right\}. \tag{31}$$

Proof. We show that there is a bijection

$$\left\{ J \subseteq I_j \colon \begin{array}{c} \mathrm{nrd}(J) = n\,\mathrm{nrd}(I_j) \\ \text{and } [J] = [I_i] \end{array} \right\} \longrightarrow \left\{ \alpha \in I_j I_i^{-1} \colon \mathrm{nrd}(\alpha) = n \frac{\mathrm{nrd}(I_j)}{\mathrm{nrd}(I_i)} \right\} \Big/ \mathcal{O}_i^\times.$$

Let $J \subseteq I_j$ be an invertible right $\mathcal{O}$-ideal such that $\mathrm{nrd}(J) = n\,\mathrm{nrd}(I_j)$ and $[J] = [I_i]$. By the latter, we know that $J = \alpha I_i$ for some $\alpha \in JI_i^{-1} \subseteq I_j I_i^{-1}$. Thus, by Lemma 2.54, we have $\mathrm{nrd}(J) = \mathrm{nrd}(\alpha)\,\mathrm{nrd}(I_i)$ and so

$$\mathrm{nrd}(\alpha) = \frac{\mathrm{nrd}(J)}{\mathrm{nrd}(I_i)} = \pm n \frac{\mathrm{nrd}(I_j)}{\mathrm{nrd}(I_i)}.$$

To conclude note that $JI_i^{-1} = \alpha I_i I_i^{-1} = \alpha \mathcal{O}_i$, which shows that α is unique modulo multiplication by $\mathcal{O}_i^\times$ from the right. □

The Brandt matrices satisfy the same recursive relations as the Hecke operators, see Proposition 4.10. This fact will be further justified in (5.1.4), where we prove that the action of these two operators coincides in a particular subspace of $S_k(\Gamma_0(N))$.

Proposition 5.5. *The Brandt matrices $\mathcal{B}_{pN}(n)$, $(n, pN) = 1$, form a commuting system of normal matrices and satisfy the recursive relations*

$$\begin{aligned} \mathcal{B}_{pN}(n)\mathcal{B}_{pN}(m) &= \mathcal{B}_{pN}(mn), && \text{for } (m,n) = 1 \\ \mathcal{B}_{pN}(q)\mathcal{B}_{pN}(q^r) &= B_{pN}(q^{r+1}) + qB_{pN}(q^{r-1}), && \text{for } r \in \mathbb{Z}_{\geq 1}, \end{aligned}$$

where q, m, n are assumed coprime to pN.

Proof. See [Voi21, 41.3.1,41.3.6,41.4.10] or [Eic73, II.Theorem 2]. □

5.1.2 Eichler Trace Formula

In this section we present the Eichler trace formula, which will enable us to compute the class number $h(\mathcal{O})$ of an Eichler order $\mathcal{O}$. In turn, this will help us understand when the Brandt matrix $\mathcal{B}_{pN}(n)$ is symmetric with even diagonal, in order for it to define a graph, see Remark 1.4. In order to derive this formula we need the theory of optimal embeddings of quadratic orders into quaternion orders.

We begin by presenting some preliminaries for the quadratic orders. We follow [Lem21] for the theory of quadratic number fields. An integer $d \in \mathbb{Z} \setminus \{0, 1\}$ is called a *discriminant* if $d \equiv 0, 1 \pmod 4$ and a *fundamental discriminant* if it is the discriminant of an (imaginary) quadratic number field, or equivalently if $d \equiv 1 \pmod 4$ or $d = 4d'$, where $d' \equiv 2, 3 \pmod 4$. So let $d < 0$ be a fundamental discriminant and let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be the imaginary quadratic field with discriminant d. Let $\mathcal{O}_{\mathbb{K}}$ be the ring of integers of the number field $\mathbb{K}$. Then, $\mathcal{O}_{\mathbb{K}}$ is the unique maximal order in $\mathbb{K}$ and we can write $\mathcal{O}_{\mathbb{K}}$ as

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \tfrac{d+\sqrt{d}}{2}\mathbb{Z}.$$

We define the *class group* of $\mathcal{O}_{\mathbb{K}}$, denoted by $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$, as the group of invertible fractional ideals in $\mathcal{O}_{\mathbb{K}}$ modulo the equivalence relation $\sim$, where $I \sim J$ if and only if $J = \alpha I$ for some $\alpha \in \mathbb{K}^\times$. The *class number* of $\mathcal{O}_{\mathbb{K}}$, denoted by h_d, is the cardinality of $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$. Let also w_d denote the cardinality of the unit group of $\mathcal{O}_{\mathbb{K}}$, or equivalently its number of roots of unity, by *Dirichlet's Unit Theorem*.

Now, let $d < 0$ be a discriminant and let S be an order in $\mathbb{K}$ of discriminant d. If S is not a maximal order in $\mathbb{K}$ then

$$S = \mathbb{Z} + f\mathcal{O}_{\mathbb{K}},$$

for some unique $f \in \mathbb{Z}_{>1}$, called the *conductor* of S. It further holds that $d = d_{\mathbb{K}} f^2$, where $d_{\mathbb{K}} \in \mathbb{Z}$ is the fundamental discriminant of $\mathbb{K}$, i.e. the discriminant of the maximal order $\mathcal{O}_{\mathbb{K}}$.

For the following results we refer to [Dav80, Chapter 6]. Let $d < 0$ be a fundamental discriminant. The number w_d equals

$$w_d = \begin{cases} 2, & \text{if } d < -4 \\ 4, & \text{if } d = -4 \\ 6, & \text{if } d = -3 \end{cases}$$

For $d < 0$ the class number of $\mathcal{O}$ can be computed by *Dirichlet's Class Number Formula*, as follows

$$h_d = -\frac{w_d}{2|d|} \sum_{m=1}^{|d|} m \left(\frac{d}{m}\right), \tag{32}$$

where $\left(\frac{d}{m}\right)$ is the Kronecker symbol.

We now introduce the notion of optimal embeddings. Let B be a quaternion algebra over $\mathbb{Q}$, let $\mathcal{O} \subseteq B$ be an order, and let S be a quadratic order in a quadratic number field $\mathbb{K}$. Note that a $\mathbb{Z}$-algebra embedding $\phi : S \hookrightarrow \mathcal{O}$ induces an embedding $\phi : \mathbb{K} \hookrightarrow B$ be extending the scalars, which we denote also by ϕ.

Definition 5.6. We call a $\mathbb{Z}$-algebra embedding $\phi : S \hookrightarrow \mathcal{O}$ *optimal* if $\phi(\mathbb{K}) \cap \mathcal{O} = \phi(S)$. We denote by $E(S, \mathcal{O})$ the set of optimal embeddings $S \hookrightarrow \mathcal{O}$.

Note that $\mathcal{O}^\times$ acts on $E(S, \mathcal{O})$ on the right by conjugation. Indeed, if $\beta \in \mathcal{O}^\times$ and $\phi : S \hookrightarrow \mathcal{O}$ is an optimal embedding then the embedding $\psi : S \hookrightarrow \mathcal{O}$ defined by $\psi(\alpha) = \beta^{-1}\phi(\alpha)\beta$, $\alpha \in S$, is again optimal. This follows from the fact that $\psi(\mathbb{K}) \cap \mathcal{O} = \beta^{-1}\phi(\mathbb{K})\beta \cap \beta^{-1}\mathcal{O}\beta = \beta^{-1}(\phi(\mathbb{K}) \cap \mathcal{O})\beta = \beta^{-1}\phi(S)\beta = \psi(S)$. We denote by $m(S, \mathcal{O})$ the number of $\mathcal{O}^\times$-conjugacy classes of optimal embeddings $S \hookrightarrow \mathcal{O}$.

Note 5.7. For the computation of the numbers $m(S, \mathcal{O})$ in the local case when $\mathcal{O}$ is a maximal order see [Voi21, 30.5] and more generally when $\mathcal{O}$ is an Eichler order see [Voi21, 30.6].

Let the notation be as (5.1.1). We define the *mass* of the order $\mathcal{O}$ as the quantity

$$\operatorname{mass}(\mathcal{O}) := \sum_{i=1}^{h} \frac{2}{e_i}. \tag{33}$$

Below we provide a neat formula for $\operatorname{mass}(\mathcal{O})$.

Theorem 5.8 (Eichler Mass Formula)**.** *The mass of the Eichler order $\mathcal{O}$ is given by the formula*

$$\operatorname{mass}(\mathcal{O}) = \frac{p-1}{12}\phi(N),$$

where $\phi(N) := N \prod_{q|N} \left(1 - \frac{1}{q}\right)$ is the Euler totient function.

Proof. See [Voi21, 30.1.4]. □

Theorem 5.9 (Eichler Trace Formula)**.** *The trace of the n-Brandt matrix $\mathcal{B}_{pN}(n)$ with respect to the Eichler order $\mathcal{O}$ is given by the formula*

$$\operatorname{tr} \mathcal{B}_{pN}(n) = \sum_{\substack{t \in \mathbb{Z}: \\ t^2 < 4n}} h_N(t^2 - 4n) + \begin{cases} \operatorname{mass}(\mathcal{O}), & \text{if } n \text{ is a square} \\ 0, & \text{otherwise} \end{cases}$$

where

$$h_N(d) = \frac{2h_d}{w_d} \prod_{q|pN} m((\mathcal{O}_\mathbb{K})_q, \mathcal{O}_q),$$

$h_d := \#\operatorname{Cl}(\mathcal{O}_\mathbb{K})$, $w_d := \mathcal{O}_\mathbb{K}^\times$, and $\mathcal{O}_\mathbb{K}$ is the ring of integers of $\mathbb{K} := \mathbb{Q}(\sqrt{d})$, when $d < 0$ is a fundamental discriminant. When $d < 0$ is an arbitrary discriminant we define $h_N(d) := h_N(d/f^2)$, where f is the conductor of the the order of discriminant d in $\mathbb{K}$.

Proof. See [Voi21, 41.5.2] and [Piz98, 4.9]. □

Note 5.10. When $\mathcal{O}$ is a maximal order we may compute $h_N(d)$ in the following more direct way

$$h_N(d) = \frac{2h_d}{w_d}\left(1 - \left(\frac{d}{p}\right)\right)\prod_{q|N}\left(1 + \left(\frac{d}{q}\right)\right),$$

where $\left(\frac{d}{q}\right)$ the Legendre symbol. See [Voi21, 30.7.4].

Using the Eichler mass formula Theorem 5.8 and the Eichler Trace formula Theorem 5.9 we derive the following formula for the class number of $\mathcal{O}$.

Corollary 5.11 (Class Number Formula)**.** *The class number of $\mathcal{O}$ is given by the formula*

$$h(\mathcal{O}) = \#\operatorname{Cls}\mathcal{O} = \frac{p-1}{12}\phi(N) + h_N(-4) + h_N(-3),$$

where

$$h_N(-4) = \begin{cases} \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right)\prod_{q|N}\left(1 + \left(\frac{-4}{q}\right)\right), & \text{if } 4 \nmid N \\ 0, & \text{if } 4 \mid N \end{cases} \tag{34}$$

$$h_N(-3) = \begin{cases} \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right)\prod_{q|N}\left(1 + \left(\frac{-3}{q}\right)\right), & \text{if } 9 \nmid N \\ 0, & \text{if } 9 \mid N \end{cases} \tag{35}$$

Proof. Consider the 1-Brandt matrix $\mathcal{B}_{pN}(1)$. We claim that for every $i = 1, \ldots, h$, $\mathcal{B}_{pN}(1)_{i,i} = 1$. Indeed, we have that

$$\mathcal{B}_{pN}(1)_{i,i} = \frac{1}{e_i}\#\{\alpha \in \mathcal{O}_i \colon \operatorname{nrd}(\alpha) = \pm 1\} = 1,$$

since $\operatorname{nrd}(\alpha) \in \mathbb{Q}^\times$ if and only if $\alpha \in B^\times$. Therefore,

$$\operatorname{tr}\mathcal{B}_{pN}(1) = \sum_{i=1}^{h}\mathcal{B}_{pN}(1)_{i,i} = h = h(\mathcal{O}).$$

The result follows from Theorem 5.8 and Theorem 5.9, since $t^2 < 4$ if and only if $t = 0, 1$, where the computation of $h_N(-4)$ and $h_N(-3)$ can be found in [Voi21, 30.7.7].

□

5.1.3 Brandt Graphs

Let again the notation be as in (5.1.1). We are now able to construct the Ramanujan graphs associated to the n-Brandt matrix $\mathcal{B}_{pN}(n)$ for $(n, pN) = 1$. Recall that $\operatorname{Ram} B = \{p, \infty\}$ and that $\mathcal{O}$ is of level N. Fix a natural number n coprime to pN. We start by proving the following lemma:

Lemma 5.12. *For every $i, j = 1, \ldots, h$ it holds that*

$$e_i \cdot \mathcal{B}_{pN}(n)_{i,j} = e_j \cdot \mathcal{B}_{pN}(n)_{j,i}.$$

Proof. By Lemma 5.4, it suffices to prove that the map

$$\left\{\alpha \in I_j I_i^{-1} \colon \operatorname{nrd}(\alpha) = \pm n\frac{\operatorname{nrd}(I_j)}{\operatorname{nrd}(I_i)}\right\} \longrightarrow \left\{\alpha \in I_i I_j^{-1} \colon \operatorname{nrd}(\alpha) = \pm n\frac{\operatorname{nrd}(I_i)}{\operatorname{nrd}(I_j)}\right\}$$
$$\alpha \longmapsto \frac{\operatorname{nrd}(I_i)}{\operatorname{nrd}(I_j)}\overline{\alpha}$$

is a bijection. If this map is well defined, then it has an inverse, namely $\alpha \mapsto \frac{\mathrm{nrd}(I_j)}{\mathrm{nrd}(I_i)}\overline{\alpha}$ and so it is a bijection. To prove that it is well-defined, let $\alpha \in I_j I_i^{-1}$ be such that $\mathrm{nrd}(\alpha) = \pm n\frac{\mathrm{nrd}(I_j)}{\mathrm{nrd}(I_i)}$. Then, by Lemma 2.57 we get that

$$\overline{\alpha} \in \overline{I_j I_i^{-1}} = \overline{I_i^{-1}}\,\overline{I_j} = (\mathrm{nrd}(I_i)^{-1} I_i)(\mathrm{nrd}(I_j) I_j^{-1}) = \frac{\mathrm{nrd}(I_j)}{\mathrm{nrd}(I_i)} I_i I_j^{-1}$$

and so indeed, $\frac{\mathrm{nrd}(I_i)}{\mathrm{nrd}(I_j)}\overline{\alpha} \in I_i I_j^{-1}$. Now,

$$\mathrm{nrd}\left(\frac{\mathrm{nrd}(I_i)}{\mathrm{nrd}(I_j)}\overline{\alpha}\right) = \frac{\mathrm{nrd}(I_i)^2}{\mathrm{nrd}(I_j)^2}\,\mathrm{nrd}(\alpha) = n\frac{\mathrm{nrd}(I_i)}{\mathrm{nrd}(I_j)}$$

and we are done. □

By Lemma 5.12 we see that the Brandt matrix $\mathcal{B}_{pN}(n)$ is symmetric if and only if $e_i = e_j$ for every $i, j = 1, \ldots, h$. Corollary 5.11 gives us a sufficient condition for $\mathcal{B}_{pN}(n)$ to be symmetric as follows.

Corollary 5.13. *The Brandt matrix $\mathcal{B}_{pN}(n)$ is symmetric if $h_N(-4) = h_N(-3) = 0$. In particular, $B_{pN}(n)$ is symmetric if $p \equiv 1 \pmod{12}$ or if $N \equiv 0 \pmod{36}$. In this case it also holds that $e_i = 2$ for every $i = 1, \ldots, h$.*

Proof. Since ± 1 are units in every $\mathcal{O}_i$ we have that $e_i \geq 2$ for every $i = 1, \ldots, h$. Therefore, by the definition (33) of the mass of $\mathcal{O}$, it follows that $\mathrm{mass}(\mathcal{O}) \leq h(\mathcal{O})$, where the equality holds if and only if $e_i = 2$ for every $i = 1, \ldots, h$. By Corollary 5.11, we have equality if and only if $h_N(-4) = h_N(-3) = 0$. The fact that $B_{pN}(n)$ is symmetric in this case follows from Lemma 5.12.

Now, if $p \equiv 1 \pmod{12}$ then $\left(\frac{-4}{p}\right) = \left(\frac{-3}{p}\right) = -1$ and so from (34) we see that $h_N(-4) = h_N(-3) = 0$. □

Definition 5.14. Suppose that $\mathcal{B}_{pN}(n)$ has even diagonal and that $h_N(-4) = h_N(-3) = 0$. We define the *n-Brandt graph* as the multi-graph $\mathcal{G}_{pN}(n)$ with adjacency matrix $\mathcal{B}_{pN}(n)$.

Note 5.15. The above assumptions assures us that the matrix $B_{pN}(n)$ is symmetric (Corollary 5.13) with even diagonal. Thus, $\mathcal{G}_{pN}(n)$ is well defined. See Remark 1.4.

Proposition 5.16. *Assume that $h_N(-4) = h_N(-3) = 0$. The n-Brandt graph $\mathcal{G}_{pN}(n)$ is a $\sigma_1(n)$-regular multigraph, i.e. for every $j = 1, \ldots, h$*

$$\sum_{i=1}^{h} \mathcal{B}_{pN}(n)_{i,j} = \sigma_1(n),$$

where $\sigma_1(n) := \sum_{d|n} d$.

Proof. We will use the description (30) of the Brandt matrix $\mathcal{B}_{pN}(n)$. We have that

$$\sum_{i=1}^{h} \mathcal{B}_{pN}(n)_{i,j} = \#\left\{J \subseteq \mathcal{O}_j \colon J \text{ invertible right } \mathcal{O}_j\text{-ideal and } \mathrm{nrd}(J) = n\right\}$$

Let $b_j(n)$ be this quantity. By [Voi21, 26.3.9], $b_j(n)$ is multiplicative in n and so we may compute the values $b_j(\ell^s)$, for $\ell \mid n$ a prime number and $s \in \mathbb{Z}_{\geq 0}$. Let $\ell \mid n$ and note that then $\ell \notin \operatorname{Ram} B$, which implies that $B_\ell \simeq M_2(\mathbb{Q}_\ell)$ and $\mathcal{O}_\ell \simeq M_2(\mathbb{Z}_\ell)$ is maximal. Thus, by Lemma 2.67 we have also that $(\mathcal{O}_j)_\ell \simeq M_2(\mathbb{Z}_\ell)$ is maximal. Thus, from Theorem 2.29 we get

$$b_j(\ell^s) = \#\left\{J_\ell \subseteq (\mathcal{O}_j)_\ell \colon J_\ell \text{ invertible right } (\mathcal{O}_j)_\ell\text{-ideal and } \operatorname{nrd}(J_\ell) = \ell^s\right\}$$

since for every $q \neq \ell$ we have that $\operatorname{nrd}(J_q) = 1$, which is equivalent to $J_q = (\mathcal{O}_j)_q$, by Corollary 2.53. So consider an invertible right $M_2(\mathbb{Q}_\ell)$-ideal $J \subseteq M_2(\mathbb{Z}_\ell)$ with $\operatorname{nrd}(J) = \ell^s$. Since J is invertible it is locally principal by Theorem 2.52. and so we have that $J = \alpha M_2(\mathbb{Z}_\ell)$, for some $\alpha \in M_2(\mathbb{Z}_\ell)$. Now, by this description of J, α is unique up to multiplication on the right by elements of $M_2(\mathbb{Z}_\ell)$, or equivalently up to application of column operations. Therefore, we may first write α_ℓ in the form $\alpha = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$, where $a = a'\ell^u$ and $b = b'\ell^v$, for some unique $u, v \in \mathbb{Z}_{\geq 0}$ and $a', b' \in \mathbb{Z}_\ell^\times$ and then we may further write

$$\alpha = \begin{pmatrix} \ell^u & 0 \\ c & \ell^v \end{pmatrix},$$

where c is unique modulo $\mathbb{Z}/\ell^v\mathbb{Z}$. Since, $\operatorname{nrd}(\alpha) = \operatorname{nrd}(J) = \ell^s$ we have that $s = u + v$. We conclude that $b_j(\ell^s) = \sum_{i=1}^{s} \ell^i$ and thus, by writing n as a product of prime numbers, we find that $b_j(n) = \sigma_1(n) = \sum_{d \mid n} d$, since $b_j(n)$ is multiplicative on n. □

5.1.4 The Ramanujan Bound

Let the notation be as in (5.1.1) and assume further that $h_N(-3) = h_N(-4) = 0$ and that $\mathcal{B}_{pN}(n)$ has even diagonal. Then the n-Brandt graph $\mathcal{G}_{pN}(n)$ is defined. Set $\mathcal{B}(n) := \mathcal{B}_{pN}(n)$ and $\mathcal{G}(n) := \mathcal{G}_{pN}(n)$. By Lemma 5.12, $\mathcal{G}(n)$ is a $\sigma_1(n)$-regular graph. We conclude this section by proving that for q a prime number, $\mathcal{G}(q)$ is a connected Ramanujan graph, i.e. that the eigenvalue $\sigma_1(q) = q+1$ appears with multiplicity 1 (see Proposition 1.14) and that every other eigenvalue $\lambda \neq q+1$ of $\mathcal{G}(q)$ satisfies the Ramanujan bound

$$|\lambda| \leq 2\sqrt{q}.$$

We will do so by showing that the the Brandt matrices $B_{pN}(q)$ arise from the action of the Hecke operators T_q on a space of theta series of weight 2 and then Ramanujan-Petersson conjecture will give us the Ramanujan bound.

We start by defining this particular space of theta series. Observe first that the map $T : B \to \mathbb{Q}$ defined by

$$T(x, y) := \frac{1}{2}\operatorname{trd}(x\overline{y}) = \frac{1}{2}\left(x\overline{y} + y\overline{x}\right) \qquad x, y \in B$$

is a symmetric bilinear map and so the reduced norm $\operatorname{nrd}(x) = T(x, x)$ defines a quadratic form over $\mathbb{Q}$. Let I be an invertible right $\mathcal{O}$-ideal. Then, the quadratic form $\operatorname{nrd} : B \to \mathbb{Q}$ restricts to a quadratic form $\operatorname{nrd}|_I : I \simeq \mathbb{Z}^4 \to \mathbb{Q}$. In order to make $\operatorname{nrd}|_I$ an integral quadratic form in the sense of the definition in (4.4), we fix a $\mathbb{Z}$-basis $e_1, e_2, e_3, e_4 \in I$ of I and then normalise it by $\operatorname{nrd}(I)$, which then gives an integral quadratic form

$$Q_I : \mathbb{Z}^4 \to \mathbb{Z}; \qquad Q_I(x_1, x_2, x_3, x_4) = \operatorname{nrd}(x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4)/\operatorname{nrd}(I).$$

Note that indeed for every $x \in \mathbb{Z}^4$ we have that $Q_I(x) \in \mathbb{Z}$, since for every $\alpha \in I$, it holds by definition that $\operatorname{nrd}(I) \mid \operatorname{nrd}(\alpha)$. Note also that Q_I depends on the choice of the basis only up to

isometry and that the level of Q_I does not depend on it, since any other $\mathbb{Z}$-basis of I is obtained by a matrix $U \in \mathrm{GL}_2(\mathbb{Z})$; hence claim follows from Remark 4.19.

Proposition 5.17. *Let I be an invertible right $\mathcal{O}$-ideal. Then, the quadratic form $Q_I : \mathbb{Z}^4 \to \mathbb{Z}$ is a positive definite quadratic form of level N.*

Proof. To see that Q_I is indeed positive definite we tensor by $\mathbb{R}$ and we get the map $Q_I \otimes \mathbb{R} : \mathbb{R}^4 \to \mathbb{R}$, which is given by the reduced norm on $B_\infty \simeq \mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, since B is ramified at ∞. Since the reduced norm on $\mathbb{H}$ is positive-definite, Q_I is also positive-definite.

By Remark 4.19, we may compute the level locally, so let ℓ be a prime number. Assume first that $\ell \neq p$. Then, since $\ell \notin \mathrm{Ram}(B)$, we have $B_\ell \simeq M_2(\mathbb{Z}_\ell)$ and since $\mathcal{O}$ is an Eichler order of level N, there exists $\alpha \in B_\ell^\times$

$$\mathcal{O}_\ell = \alpha \begin{pmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ N\mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix} a^{-1}$$

Since I is invertible, I_ℓ is principal and so there exists $\beta \in B_\ell^\times$ such that $I_\ell = \beta\mathcal{O}_\ell$. From the latter we get that $\mathrm{nrd}(\beta)\mathbb{Z}_\ell = \mathrm{nrd}(I_\ell)$. We now find a $\mathbb{Z}$-basis of I_ℓ. Let

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ e_3 = \begin{pmatrix} 0 & 0 \\ N & 0 \end{pmatrix},\ e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then, the elements $f_i := \beta\alpha e_i \alpha^{-1}, i = 1, \dots, 4$, form a $\mathbb{Z}_\ell$-basis of I_ℓ. Computing then the matrix $M_{Q_I \otimes \mathbb{Z}_\ell}$ of the quadratic form $Q_I \otimes \mathbb{Z}_\ell$ with respect to that basis we find that

$$M_{Q_I \otimes \mathbb{Z}_\ell} = (\mathrm{trd}(f_i f_j)/\,\mathrm{nrd}(\beta))_{1 \leq i,j \leq 4} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -N & 0 \\ 0 & -N & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

which has level N in $\mathbb{Z}_\ell$. (For the exact calculation of $M_{Q_I \otimes \mathbb{Z}_\ell}$, see [Piz80a, 2.11].) In the case where $\ell = p$, we have that B_p is a division algebra and $\mathcal{O}_p$ its unique maximal order. By [Voi21, 13.3.4] and [Piz80a, Section 1] we have that

$$B_p \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in L \right\} \quad \text{and} \quad \mathcal{O}_p \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in S \right\},$$

where L is the unique unramified quadratic field extension of $\mathbb{Q}_p$, S its ring of integers, and σ the conjugation of the field extension $\mathbb{Q}_p/L$. Calculating the matrix of the quadratic form as above we find that its level is 1, as it should be, since $p \nmid N$. That concludes the proof. □

Recall from Lemma 5.4 that for every $i, j = 1, \dots, h$, the (i,j)-th entry of the Brandt matrix $\mathcal{B}(n)$ is given by

$$\mathcal{B}(n)_{i,j} = \frac{1}{2} \# \left\{ \alpha \in I_j I_i^{-1} \colon \mathrm{nrd}(\alpha) = \pm n \frac{\mathrm{nrd}(I_j)}{\mathrm{nrd}(I_i)} \right\}$$

Note that $e_i = 2$ for each i, by our assumptions and Corollary 5.13. For each such i, j, consider the quadratic form $Q_{i,j} := Q_{I_j I_i^{-1}}$ (w.r.t. to a basis) and let the $\theta_{i,j}$ be the theta series of $Q_{i,j}$, i.e.

$$\theta_{i,j}(z) := \frac{1}{2}\theta_{Q_{i,j}}(z) = \sum_{m=0}^{\infty} B_{pN}(m)_{i,j} q^m.$$

Corollary 5.18. *For each $i, j = 1, \dots, h$, we have that $\theta_{i,j} \in M_2(\Gamma_0(N))$.*

Proof. Immediate from Proposition 5.17 and Theorem 4.22. □

In order to apply the Ramanujan-Petersson conjecture we need cusp forms. However, none of the $\theta_{i,j}$ are cusp forms as for example at the cusp ∞ we have that $a_0(\theta_{i,j}) = 1/2$. Since all $\theta_{i,j}$ have the same behaviour at the cusp ∞, their difference is holomorphic at ∞. Using Theorem 4.23, we prove that this is the case at all cusps.

Proposition 5.19. *For every $1 \leq i, j, k \leq h$, we have that $\theta_{i,j} - \theta_{k,j} \in S_2(\Gamma_0(N))$.*

Proof. Let $1 \leq i, k \leq h$. We claim that for every $1 \leq j \leq h$, $Q_{i,j}$ and $Q_{k,j}$ are of the same genus. Let ℓ be a prime number. Since I_i, I_k are invertible, there exists $\beta, \gamma \in B_\ell^\times$ such that $(I_i)_\ell = \beta \mathcal{O}_l$ and $(I_k)_\ell = \gamma \mathcal{O}_\ell$. Thus, setting $\alpha := \beta\gamma^{-1}$ we have that $(I_i)_\ell = \alpha(I_k)_\ell$ and so $\operatorname{nrd}(\alpha) = \operatorname{nrd}((I_i)_\ell)/\operatorname{nrd}((I_j)_\ell)$ and $(I_j I_i^{-1})_\ell \alpha = (I_j I_k^{-1})_\ell$. Thus, the $\mathbb{Z}$-linear map $f : x \mapsto x\alpha$ fits into the commutative diagram

$$\begin{array}{ccc} (I_j I_i^{-1})_\ell & \xrightarrow{f} & (I_j I_k^{-1})_\ell \\ {\scriptstyle Q_{i,j}\otimes\mathbb{Z}_\ell}\downarrow & & \downarrow{\scriptstyle Q_{k,j}\otimes_{\mathbb{Z}_\ell}} \\ \mathbb{Z} & \xrightarrow{\mathrm{id}} & \mathbb{Z} \end{array}$$

which shows that f defines an isometry $Q_{i,j} \otimes \mathbb{Z}_\ell \to Q_{k,j} \otimes \mathbb{Z}_\ell$. Hence, indeed $Q_{i.j}, Q_{k,j}$ are of the same genus. Therefore, Theorem 4.23 implies that $\theta_{i,j} - \theta_{k,j} \in S_2(\Gamma_0(N))$. □

We are now going to express these theta series differences using the Brandt matrix $\mathcal{B}(n)$. Consider the matrix $A \in \mathrm{GL}_h(\mathbb{Z})$ with $A_{i,1} = A_{1,i} = 1$ for all $i = 1, \dots, h$, $A_{i,i} = -1$, for $i = 2, \dots, h$ and $A_{i,j} = 0$ for $2 \leq i \neq j \leq h$. Then, using Proposition 5.16 and the commutativity of Brandt matrices, one can show that

$$A\mathcal{B}(n)A^{-1} = \begin{pmatrix} \sigma_1(n) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathcal{B}'(n) & \\ 0 & & & \end{pmatrix} =: \mathcal{C}(n), \tag{36}$$

where $\mathcal{B}'(n)_{i,j} := \mathcal{B}(n)_{i+1,j+1} - \mathcal{B}(n)_{1,j+1}$, $1 \leq i, j \leq h-1$. For the exact explicit matrix multiplication (36) see [Piz80a, 2.19]. We call the matrix $\mathcal{B}'(n) \in M_{h-1}(\mathbb{Z})$ the *modified n-Brandt matrix*.

Remark 5.20. Observe that the modified Brandt matrix $\mathcal{B}'(n)$ and the Brandt matrix $\mathcal{B}(n)$ share the same spectrum, where the multiplicity of the eigenvalue $\sigma_1(n)$ in $\mathcal{B}'(n)$ is 1 less than its multiplicity in $\mathcal{B}(n)$.

For each $i, j = 2, \dots, h$, consider now the *modified theta series*

$$\theta'_{i,j}(q) := \sum_{m=1}^{\infty} \mathcal{B}'(n)_{i-1,j-1} q^m = \theta_{i-1,j-1}(q) - \theta_{1,j-1}(q) \in S_2(\Gamma_0(N)),$$

where the second equality follows from the definition of the modified Brandt matrix $\mathcal{B}'(n)$.

We now prove one of the most important facts about the Brandt matrices. Their action on the space of the theta series defined above coincides with the action of the Hecke operators into this space. More precisely we have the following:

Theorem 5.21. *Let $n \in \mathbb{Z}_{\geq 0}$ be such that $(n, pN) = 1$. Then,*

$$(T_n \theta_{i,j})(q) = \sum_{m=0}^{\infty} \left(\left(\mathcal{B}(n)\mathcal{B}(m)\right)_{i,j} q^m \right) \tag{37}$$

Proof. Since T_n and $\mathcal{B}(n)$ satisfy the same recursive relations, by Proposition 5.5 and Proposition 4.10, it suffices to prove the statement for ℓ a prime number such that $(\ell, pN) = 1$. By (26), we have that

$$(T_\ell \theta_{i,j})(q) = \sum_{m=0}^{\infty} b_m q^m, \qquad \text{where } b_m = \mathcal{B}(\ell m)_{i,j} + \begin{cases} q\mathcal{B}(m/\ell)_{i,j}, & \text{if } q \mid m \\ 0, & \text{if } q \nmid m \end{cases}$$

If $(m, pN) = 1$ then by Proposition 4.10, we have that $b_m = (\mathcal{B}(\ell)\mathcal{B}(m))_{i,j}$, as desired. In the case where $(m, pN) > 1$, the result follows from [Eic73, p. 138]. □

Remark 5.22. We can express the action in (37) in a more clear and useful way as follows: consider $g_k : \mathbb{C}^h \to S_2(\Gamma_0(N))$ to be the linear map that sends the standard basis element $e_i \in \mathbb{C}^h$ into $g(e_i) := \theta_{i,k}$, where $k = 1, \ldots, h$. Then, for every $n \in \mathbb{Z}_{\geq 1}$ such that $(n, pN) = 1$ the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}^h & \xrightarrow{\mathcal{B}(n)} & \mathbb{C}^h \\ {\scriptstyle g_k}\downarrow & & \downarrow{\scriptstyle g_k} \\ S_2(\Gamma_0(N))) & \xrightarrow[T_n]{} & S_2(\Gamma_0(N))) \end{array} \tag{38}$$

This is indeed the case since if we take the basis element $e_i = (\delta_{i,j})_{j=1}^h \in \mathbb{C}^h$[2] then $\mathcal{B}(n)e_i = (\mathcal{B}(n)_{j,i})_{j=1}^h = (\mathcal{B}(n)_{i,j})_{j=1}^h$, as $\mathcal{B}(n)$ is a symmetric matrix, by Corollary 5.13. Thus,

$$g(\mathcal{B}(n)e_i)(q) = \sum_{j=1}^{h} \mathcal{B}(n)_{i,j}\theta_{j,k}(q) = \sum_{j=1}^{h} \mathcal{B}(n)_{i,j} \sum_{m=0}^{\infty} \mathcal{B}(m)_{j,k} q^m = \sum_{m=0}^{\infty} \left(\sum_{j=1}^{h} \mathcal{B}(n)_{i,j}\mathcal{B}(m)_{j,k} \right) q^m$$
$$= \sum_{m=0}^{\infty} (\mathcal{B}(n)\mathcal{B}(m))_{i,k} q^m = (T_n \theta_{i,k})(q).$$

where the last equality holds by (37).

Continuing with the construction of the eigenforms, by Proposition 5.5 and the spectral theorem we have that there exists a matrix $C \in \mathrm{GL}_h(\mathbb{C})$ such that all the matrices $C\mathcal{B}(n)C^{-1}$, $(n, pN) = 1$, are simultaneously diagonal. Combining C with the matrix A defined above in (36), we find a matrix $C_0 \in \mathrm{GL}_{h-1}(\mathbb{C})$ such that all matrices $\mathcal{D}'(n) := C_0\mathcal{B}'(n)C_0^{-1}$, $(n, pN) = 1$, are simultaneously diagonal. For every $i = 2, \ldots, h$, define the cusp form

$$\Phi_i(q) = \sum_{m=0}^{\infty} \mathcal{D}'(m)_{i-1,i-1} q^m.$$

Note that each Φ_i is indeed a cusp form as it is a linear combination of the $\theta'_{i,j}$, $i, j = 2, \ldots, h$.

[2] $\delta_{i,j}$ denotes the *Kronecker delta*.

Corollary 5.23. *For every $i = 2, \dots, h$, $\Phi_i \in S_2(\Gamma_0(N))$ are eigenforms for the Hecke operators T_n, $(n, pN) = 1$, with eigenvalues the diagonal entries of $\mathcal{D}'(n)$.*

Proof. Since the matrices $\mathcal{D}'(n) = C_0 \mathcal{B}'(n) C_0^{-1}$, $(n, pN) = 1$, are all diagonal, it is enough to show that the action of the Hecke operators $T(n)$ into Φ_i is given as in Theorem 5.21, but by the matrix $D'(n)$ instead of $\mathcal{B}(n)$. But, this follows from the definition of $D'(n)$, and by composing from above to the commutative diagram (38), the commutative diagrams

$$\begin{array}{ccccccc} \mathbb{C}^{h-1} & \xrightarrow{C_0^{-1}} & \mathbb{C}^{h-1} & \hookrightarrow & \mathbb{C}^{h} & \xrightarrow{A^{-1}} & \mathbb{C}^{h} \\ {\scriptstyle \mathcal{D}'(n)}\uparrow & & {\scriptstyle \mathcal{B}'(n)}\uparrow & & {\scriptstyle \mathcal{C}(n)}\uparrow & & {\scriptstyle \mathcal{B}(n)}\uparrow \\ \mathbb{C}^{h-1} & \xrightarrow[C_0^{-1}]{} & \mathbb{C}^{h-1} & \hookrightarrow & \mathbb{C}^{h} & \xrightarrow[A^{-1}]{} & \mathbb{C}^{h} \end{array}$$

where the inclusion arrow just puts a zero in the first coordinate. The commutativity of the diagrams follows by the above analysis and (36). □

We are finally able to conclude that the graphs $\mathcal{G}_{pN}(q)$, with $(q, pN) = 1$ are Ramanujan.

Theorem 5.24. *Let $n \in \mathbb{Z}_{\geq 1}$ such that $(n, pN) = 1$. Then the graph $\mathcal{B}_{pN}(n)$ is a $\sigma_1(n)$-regular connected graph with maximum eigenvalue $\lambda_1 = \sigma_1(n)$ and all other eigenvalues λ satisfy the Ramanujan bound*

$$|\lambda| \leq \sigma_0(n)\sqrt{n}.$$

In particular, if q is a prime number such that $(q, pN) = 1$ then the graph $\mathcal{G}_{pN}(q)$ is a $(q+1)$-regular connected Ramanujan graph.

Proof. By Proposition 5.16 and Proposition 1.14 we have that $\mathcal{G}_{pN}(n)$ is a $\sigma_1(n)$-regular graph. By Remark 5.20, we have that

$$\operatorname{spec}(\mathcal{B}'_{pN}(n)) = \operatorname{spec}(\mathcal{B}_{pN}(n)) \setminus \{\sigma_1(n)\},$$

where, as usual, we view the spectrum as a multiset. Since $\mathcal{D}'_{pN}(n) = C_0 \mathcal{B}'_{pN}(n) C_0^{-1}$, the diagonal entries of $\mathcal{D}'_{pN}(n)$ coincides with $\operatorname{spec}(\mathcal{B}'_{pN}(n))$; therefore, by Corollary 5.23 and the Ramanujan-Petersson conjecture Theorem 4.16, we get that for all $\lambda \in \operatorname{spec}(\mathcal{B}'_{pN}(n))$

$$|\lambda| \leq \sigma_0(n)\sqrt{n}.$$

This shows that $\sigma_1(n)$ is an eigenvalue of multiplicity 1, which by Proposition 1.14, implies that $\mathcal{G}_{pN}(n)$ is connected, and that $\lambda(\mathcal{G}_{pN}(n)) \leq \sigma_0(n)\sqrt{n}$. The second claim is immediate from the first since $\sigma_1(p) = p + 1$ and $\sigma_0(p) = 2$. □

Remark 5.25. It is worth mentioning that Theorem 5.24, in the case where n is not necessarily a prime, gives an interesting family of expander graphs as the bound $|\lambda| \leq \sigma_0(n)\sqrt{n}$ is non-trivial. See Corollary 1.23.

5.2 Supersingular Isogeny Graphs

In this section we describe a second construction of Ramanujan graphs using supersingular elliptic curves and their isogenies, which remarkably turns out to be equivalent to Pizer's construction for Eichler orders of level 1, or equivalently for maximal orders.

5.2.1 ℓ-Isogeny Graphs

Let $p \neq 2$ be a prime number, consider the finite field $\mathbb{F}_p$, and fix an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. Let also $\ell \neq p$ be another prime. We will refer to an isogeny of degree ℓ an *ℓ-isogeny*.

Let E, E' be elliptic curves over $\overline{\mathbb{F}_p}$. Two isogenies $\phi, \psi : E \to E'$ are said *equivalent* if there exists a non-zero isogeny $\alpha \in \mathrm{Aut}(E')$ such that $\psi = \alpha \circ \phi$. Clearly this defines an equivalence relation on $\mathrm{Hom}(E, E')$.

Definition 5.26. We define the *ℓ-isogeny graph* (over $\overline{\mathbb{F}_p}$), which we denote by $\mathcal{G}_p(\ell)$, as the graph with vertices the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ and arrows between two supersingular elliptic curves E and E' as the equivalence classes of isogenies $E \to E'$.

First note that by Theorem 3.20 and Theorem 3.3, we can represent each vertex $[E]$ of $\mathcal{G}_p(\ell)$ by its j-invariant $j(E)$ in $\mathbb{F}_{p^2}$. This also shows that $\mathcal{G}_p(\ell)$ is a finite graph.

This is by definition a directed graph whereas in the context of this thesis we study undirected graphs. Fortunately, the only possible vertices that can cause the directness of the graph $\mathcal{G}_p(\ell)$ are represented by the j-invariants $j = 0, 1728$. This is because for every elliptic curve E with $j(E) \neq 0, 1728$ we have that $\#\,\mathrm{Aut}(E) = 2$, whereas for elliptic curves E with $j(E) \in \{0, 1728\}$ we have $\#\,\mathrm{Aut}(E) > 2$, see [Sil09, III.10.1]. The numbers $j = 0, 1728$ appear as vertices in $\mathcal{G}_p(\ell)$, i.e. they are the j-invariants of a supersingular elliptic curve, exactly in the following cases:

- $j(E) = 0$ for some supersingular elliptic curve $E/\overline{\mathbb{F}_p}$ if and only if $p \equiv 2 \pmod 3$; and
- $j(E) = 1728$ for some supersingular elliptic curve $E/\overline{\mathbb{F}_p}$ if and only if $p \equiv 3 \pmod 4$,

according to [ACNL+19, 2.2]. Thus if we restrict p to be $p \equiv 1 \pmod{12}$, the graphs $\mathcal{G}_p(\ell)$ becomes undirected in the sense of Definition 1.1. Moreover, where we require $p \equiv 1 \pmod{12}$, the graph $\mathcal{G}_p(\ell)$ is also $(\ell+1)$-regular. Indeed, if $\phi : E \to E'$ is an ℓ-isogeny then it is separable and thus it corresponds bijectively to the subgroups of E of order $\#\ker\phi = \deg\phi = \ell$, by [Sil09, III.4.12]. But note that $\ker\phi \subseteq E[\ell]$, since if $P \in \ker\phi$ then $\phi(P) = 0$ and by applying $\hat{\phi}$ we get that $[\ell](P) = 0$. Now, by Lemma 3.8 we have that $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, which has exactly $\ell + 1$ subgroups of order ℓ.

The order of the graph $\mathcal{G}_p(\ell)$ is computed according to the congruence of p modulo 12 as follows: if $p \geq 5$ then

$$\#V(\mathcal{G}_p(\ell)) = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0, & p \equiv 1 \pmod{12} \\ 1, & p \equiv 5, 7 \pmod{12} \\ 2, & p \equiv 11 \pmod{12} \end{cases}$$

according to [Sil09, V.4.1]. Thus, again if we assume $p \equiv 1 \pmod{12}$ we get that the order of the graph is exactly $\frac{p-1}{12}$.

The most important property of the ℓ-isogeny graph $\mathcal{G}_p(\ell)$ is that it is a Ramanujan graph. This follows from the fact that $\mathcal{G}_p(\ell)$ is isomorphic to the ℓ-Brandt graph associated to a maximal order in the quaternion algebra $B_{p,\infty}$. Note that from this isomorphism will also follow the statements about the order and the regularity of $\mathcal{G}_p(\ell)$ described above, as they were proved in (5.1). We give this isomorphism in the following section.

5.2.2 The Deuring Correspondence.

Let $p \equiv 1 \pmod{12}$ be a prime number and $\ell \neq p$ a prime number. To define the isomorphism we fix a base supersingular elliptic curve E_0 over $\overline{\mathbb{F}_p}$. Let $\mathcal{O}_0 := \mathrm{End}(E_0)$ and $B_0 := \mathrm{End}(E_0)_{\mathbb{Q}}$.

By Theorem 3.25, we have that B is a quaternion algebra isomorphic to B_0 and $\mathcal{O}_0$ is a maximal order in B_0. The isomorphism presented in this section is essentially the so-called *Deuring Correspondence* due to M. Deuring [Deu41]. In (5.1.1), we proved that the ℓ-Brandt graph $\mathcal{G}_p(\ell)$ associated to the maximal order $\mathcal{O}_0$ in B_0 is an $(\ell+1)$-regular multigraph (Proposition 5.16) of order $h(\mathcal{O}_0) = \mathrm{mass}(\mathcal{O}_0) = \frac{p-1}{12}$ (Corollary 5.11) with vertex set $V(\mathcal{G}_p(\ell)) = \mathrm{Cls}_R(\mathcal{O}_0)$, where an edge exists between two vertices $[I], [J] \in \mathrm{Cls}_R(\mathcal{O}_0)$ for every $\alpha \in JI^{-1}$ such that $\mathrm{nrd}(\alpha) = \ell \frac{\mathrm{nrd}(J)}{\mathrm{nrd}(I)}$.

Remark 5.27. Let E be a supersingular elliptic curve. Then, $\mathrm{Hom}(E_0, E)$ is a $\mathbb{Z}$-module with a right action from $\mathcal{O}_0 = \mathrm{End}(E_0)$ and thus defines a right $\mathcal{O}_0$-module. Therefore, the association $E \longmapsto \mathrm{Hom}(E_0, E)$ defines a functor between the category of elliptic curves with isogenies and right $\mathcal{O}_0$-modules with right $\mathcal{O}_0$-module homomorphisms.

In order to define this isomorphism recall (3.4).

Theorem 5.28. *The association between integral right $\mathcal{O}_0$-ideals and supersingular elliptic curves*

$$I \longmapsto E_{0,I} \longmapsto [E_{0,I}]^{(3)} \tag{39}$$

induces an isomorphism between the ℓ-Brandt graph $\mathcal{G}_p(\ell)$ and the ℓ-isogeny graph $\mathcal{G}_p(\ell)$.

Proof. Note first that (39) induces a well-defined map on $V(\mathcal{G}_p(\ell))$. This follows as by Lemma 2.18, each isomorphism class $[I] \in \mathrm{Cls}_R(\mathcal{O}_0)$ contains an integral right $\mathcal{O}_0$-idea and thus the claim follows from Lemma 3.26. Therefore we get an induced map

$$V(\mathcal{G}_p(\ell)) \longrightarrow V(\mathcal{G}_p(\ell)); \qquad [I] \longmapsto [E_{0,I}], \tag{40}$$

where $E_{0,I}$ is defined with a possible scaling of I in order for it to be integral.

We next prove that the map (40) is injective. Let I, J be integral right $\mathcal{O}_0$-ideals in B_0 such that $[E_{0,I}] = [E_{0,J}]$, i.e. such that there exists an isomorphism $\phi : E_{0,I} \xrightarrow{\sim} E_{0,J}$. By Remark 5.27, $\mathrm{Hom}(E_0, -)$ is functorial and so the pullback map $\phi^* : \mathrm{Hom}(E_0, E_{0,I}) \xrightarrow{\sim} \mathrm{Hom}(E_0, E_{0,J})$ is an isomorphism of right $\mathcal{O}_0$-modules. Now, from Lemma 3.27, we get a composition of isomorphisms of right $\mathcal{O}_0$-modules

$$I \xrightarrow{\sim} \mathrm{Hom}(E_0, E_{0,I}) \xrightarrow{\sim} \mathrm{Hom}(E_0, E_{0,J}) \xrightarrow{\sim} J$$

and thus from Lemma 2.59, we have that $[I] = [J]$. Hence, the map (40) is injective.

To prove surjectivity, let E be a supersingular elliptic curve. By Proposition 3.24, we have that $\mathrm{Hom}(E_0, E)$ is of rank 4 and in particular it is non-empty, thus from Lemma 3.28, there exists an integral right $\mathcal{O}_0$-module I and an isomorphism $\rho_I : E_{0,I} \xrightarrow{\sim} E$, which proves surjectivity.

To conclude that (40) defines an isomorphism of graphs in the sense of Definition 1.2, we are left to prove that it induces compatible with (40) local bijections on the edges of the graphs, i.e. for every integral $\mathcal{O}_0$-ideals I, J we have a bijection

$$E_{\mathcal{G}_p(\ell)}([I], [J]) \xrightarrow{\sim} E_{\mathcal{G}_p(\ell)}([E_{0,I}], [E_{0,J}]).$$

[(3)] Here we use the notation $E_{0,I}$ in the place of $(E_0)_I$.

By definition of the graphs $\mathcal{G}_p(\ell)$ and $\mathcal{G}_p(\ell)$ we want to prove that there is a bijection

$$\{\phi \in \mathrm{Hom}(E_{0,I}, E_{0,J})\colon \deg\phi = \ell\} \xrightarrow{\sim} \left\{\alpha \in JI^{-1}\colon \mathrm{nrd}(\alpha) = \ell\frac{\mathrm{nrd}(J)}{\mathrm{nrd}(I)}\right\} \tag{41}$$

So, let $I, J \subseteq \mathcal{O}_0$ be integral $\mathcal{O}_0$-ideals and consider the isogenies $\phi_I : E_0 \to E_{0,I}$ and $\phi_J : E_0 \to E_{0,J}$. Recall that $\deg(\phi_I) = \mathrm{nrd}(I)$ and that $\deg(\phi_J) = \mathrm{nrd}(J)$. We claim that the map

$$\left(E_{0,I} \xrightarrow{\phi} E_{0,J}\right) \longmapsto \left(E_0 \xrightarrow{\hat{\phi_I}^{-1}} E_{0,I} \xrightarrow{\phi} E_{0,J} \xrightarrow{\hat{\phi_J}} E_0\right) \tag{42}$$

serves as our desired bijection. Notice first that this map is clearly a bijection into its image and that if $\phi : E_{0,I} \to E_{0,J}$ is an ℓ-isogeny then

$$\mathrm{nrd}\left(\hat{\phi_J}\phi\hat{\phi_I}^{-1}\right) = \deg\left(\hat{\phi_J}\phi\hat{\phi_I}^{-1}\right) = \deg(\phi)\frac{\deg(\hat{\phi_J})}{\deg(\hat{\phi_J})} = \ell\frac{\mathrm{nrd}(J)}{\mathrm{nrd}(I)}.$$

Thus, if we prove that the map (42) maps $\mathrm{Hom}(E_{0,I}, E_{0,J})$ onto JI^{-1} then it will restrict to the bijection (41).

Claim: The following equality holds

$$\mathrm{Hom}(E_0, E_{0,J}) = \mathrm{Hom}(E_{0,I}, E_{0,J})\,\mathrm{Hom}(E_0, E_{0,I}) \tag{43}$$

Proof of Claim: By Lemma 2.57, we have that $m := \deg(\phi_I) = \mathrm{nrd}(I) \in \widehat{I}I$ and, by Lemma 3.27, we have that $\hat{\phi_I}\,\mathrm{Hom}(E_0, E_{0,I}) = I$. Therefore, there exist $\alpha_i, \beta_i \in \mathrm{Hom}(E_0, E_{0,I})$, $i = 1, \ldots, k$, such that

$$[m] = \sum_{i=1}^{k} \widehat{\hat{\phi_I}\alpha_i}\hat{\phi_I}\beta_i = \sum_{i=1}^{k} \hat{\alpha}_i\phi_I\hat{\phi_I}\beta_i = \sum_{i=1}^{k} \hat{\alpha}_i[m]\beta_i$$

and so $\sum_{i=1}^{k} \hat{\alpha}_i\beta_i = [1]$, since $[m]$ is surjective. Therefore, for every $\psi \in \mathrm{Hom}(E_0, E_{0,J})$ we have

$$\psi = \sum_{i=1}^{k}(\psi\hat{\alpha}_i)\beta_i \in \mathrm{Hom}(E_{0,I}, E_{0,J})\,\mathrm{Hom}(E_0, E_{0,I})$$

The other inclusion is obvious and so we get the equality (43).

Now, again by Lemma 3.27, we have also that $\hat{\phi_J}\,\mathrm{Hom}(E_0, E_{0,J}) = J$ and so by (43) we get that

$$\hat{\phi_J}^{-1}J = \mathrm{Hom}(E_{0,I}, E_{0,J})\hat{\phi_I}^{-1}I$$

which in turn implies that $\hat{\phi_J}\,\mathrm{Hom}(E_{0,I}, E_{0,J})\hat{\phi_I}^{-1} = JI^{-1}$. Therefore, we get that the map (42) restricts with the bijection (41). □

Corollary 5.29. *For every prime $p \equiv 1 \pmod{12}$ and $\ell \neq p$ a prime number, the graph $\mathcal{G}_p(\ell)$ is a connected $(\ell+1)$-regular Ramanujan graph.*

Proof. Immediate from Theorem 5.24 and Theorem 5.28. □

Note 5.30. Following Remark 5.25, it is worth mentioning that we can exhibit a similar isomorphism as in Theorem 5.28 for the case of an arbitrary Eichler order of level $N \in \mathbb{Z}_{\geq 1}$. In particular, we endow elliptic curves with a *level-N structure*, by considering pairs (E, G), where E is a supersingular elliptic curve and $G \subseteq E[N]$ is a cyclic group of order N. We define a *leveled isogeny* $\phi : (E, G) \to (E', G')$ between two such pairs as an isogeny $\phi : E \to E'$ such that $\phi(G) \subseteq G'$. Then, it holds that $\mathrm{End}(E, G)$ is isomorphic to an Eichler order of level N.

By a variation of Theorem 5.28, we have an isomorphism of the graphs defined by the level-N supersingular elliptic curves together with leveled isogenies to the graphs $\mathcal{G}_{pN}$ defined in (5.1.3) over an Eichler order N. Thus, by Remark 5.25, we have that these leveled isogeny graphs are good expanders.

For the analysis of leveled isogenies and the proof of this variational Deuring correspondence we refer to [Arp22].

References

[AC88] N. Alon and F.R.K. Chung. Explicit construction of linear sized tolerant networks. *Discrete Mathematics*, 72(1):15–19, 1988.

[ACNL+19] Sarah Arpin, Catalina Camacho-Navarro, Kristin E. Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland. *Experimental Mathematics*, 32:241 – 268, 2019.

[AKS83] Miklós Ajtai, John Komlos, and Endre Szemerédi. An 0(n log n) sorting network. *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, 1983.

[AKS87] M. Ajtai, J. Komlos, and E. Szemeredi. Deterministic simulation in logspace. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, page 132–140, New York, NY, USA, 1987. Association for Computing Machinery.

[Alo86] Noga Alon. Eigenvalues and expanders. *Combinatorica*, 6:83–96, 1986.

[ALW01] Noga Alon, Alexander Lubotzky, and Avi Wigderson. Semi-direct product in groups and zig-zag product in graphs: connections and applications. *Proceedings 2001 IEEE International Conference on Cluster Computing*, pages 630–637, 2001.

[AM69] Michael Francis Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley-Longman, 1969.

[AM85] Noga Alon and V. D. Milman. lambda1, Isoperimetric inequalities for graphs, and superconcentrators. *J. Comb. Theory, Ser. B*, 38:73–88, 1985.

[Arp22] Sarah Arpin. Adding level structure to supersingular elliptic curve isogeny graphs. https://arxiv.org/abs/2203.03531, 2022.

[AS98] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of np. *J. ACM*, 45(1):70–122, jan 1998.

[BKS16] Khodakhast Bibak, Bruce M. Kapron, and Venkatesh Srinivasan. The Cayley Graphs Associated With Some Quasi-Perfect Lee Codes Are Ramanujan Graphs. *IEEE Transactions on Information Theory*, 62:6355–6358, 2016.

[BKV+81] Manuel Blum, Richard M. Karp, Oliver Vornberger, Christos H. Papadimitriou, and Mihalis Yannakakis. The complexity of testing whether a graph is a superconcentrator. *Inf. Process. Lett.*, 13:164–167, 1981.

[BL06] Yonatan Bilu and Nathan Linial. Lifts, discrepancy and nearly optimal spectral gap. *Combinatorica*, 26:495–519, 2006.

[Bra43] Heinrich Brandt. Zur zahlentheorie der quaternionen. *Jahresbericht Der Deutschen Mathematiker-vereinigung*, 53:23–57, 1943.

[BST09] Eiichi Bannai, Osamu Shimabukuro, and Hajime Tanaka. Finite Euclidean graphs and Ramanujan graphs. *Discret. Math.*, 309:6126–6134, 2009.

[Bus82] Peter Buser. A note on the isoperimetric constant. *Annales Scientifiques De l' École normale supérieure*, 15:213–230, 1982.

[Car72] P. Cartier. Fonctions harmoniques sur un arbre. In *Symposia Mathematica MT Summit IX*, number 1 in IX (Convegno di Calcolo delle Probabilità, INDAM, Rome, 1971)„ page 203–270 (French), London, 1972.

[Che71] Jeff Cheeger. *A Lower Bound for the Smallest Eigenvalue of the Laplacian*, pages 195–200. Princeton University Press, Princeton, 1971.

[Chi92] Patrick Chiu. Cubic Ramanujan graphs. *Combinatorica*, 12:275–285, 1992.

[Chu89] Fan R. K. Chung. Diameters and eigenvalues. *Journal of the American Mathematical Society*, 2:187–196, 1989.

[Dav80] Harold Davenport. *Multiplicative Number Theory.*, volume 74 of *2nd ed. Rev. by Hugh L. Montgomery.* Springer, Cham, 1980.

[Del71] Pierre Deligne. Modular forms and ℓ-adic representations. Sémin. Bourbaki 1968/69, No. 355, Lect. Notes Math. 179, 139-172 (1971)., 1971.

[Del73] Pierre Deligne. La conjecture de Weil. I. *Publ. Math., Inst. Hautes Étud. Sci.*, 43:273–307, 1973.

[Deu41] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14:197–272, 1941.

[Din07] Irit Dinur. The pcp theorem by gap amplification. *J. ACM*, 54(3):12–es, jun 2007.

[Dod84] Józef Dodziuk. Difference equations, isoperimetric inequality and transience of certain random walks. *Transactions of the American Mathematical Society*, 284:787–794, 1984.

[dR97] Juan Arias de Reyna. Finite fields and Ramanujan graphs. *J. Comb. Theory, Ser. B*, 70:259–264, 1997.

[Dri88] V. G. Drinfel'd. The proof of Peterson's conjecture for GL(2) over a global field of characteristic p. *Functional Analysis and its Applications*, 22:28–43, 1988.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228 of *Grad. Texts Math.* Berlin: Springer, 2005.

[Eic54] Martin Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954.

[Eic73] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. Modular Functions of one Variable I, Proc. internat. Summer School, Univ. Antwerp 1972, Lect. Notes Math. 320, 75-151 (1973)., 1973.

[ES63] Paul Erdős and Horst Sachs. Regular graphs with given girth and minimal number of knots. *Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg, Math.-Naturwiss. Reihe*, 12:251–258, 1963.

[Fri91] Joel Friedman. The spectra of infinite hypertrees. *SIAM J. Comput.*, 20:951–961, 1991.

[Fri03] Joel Friedman. A Proof of Alon's Second Eigenvalue Conjecture. In *Symposium on the Theory of Computing*, 2003.

[GG81] Ofer Gabber and Zvi Galil. Explicit constructions of linear-sized superconcentrators. *J. Comput. Syst. Sci.*, 22:407–420, 1981.

[Gro09] Mikhail Gromov. Singularities, expanders and topology of maps. I: Homology versus volume in the spaces of cycles. *Geom. Funct. Anal.*, 19(3):743–841, 2009.

[Gun05] Paul E. Gunnells. Some elementary Ramanujan graphs. *Geometriae Dedicata*, 112:51–63, 2005.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[Hij74] Hiroaki Hijikata. Explicit formula of the traces of hecke operators for $\gamma\_\{0\}(n)$. *Journal of the Mathematical Society of Japan*, 26:56–82, 1974.

[HLL19] Jong Yoon Hyun, Jungyun Lee, and Yoonjin Lee. Ramanujan graphs and expander families constructed from p-ary bent functions. *Designs, Codes and Cryptography*, 88:453 – 470, 2019.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Widgerson. Expander graphs and their application. *Bulletin (New Series) of the American Mathematical Society*, 43, 10 2006.

[JL97] Bruce W. Jordan and Ron Livne. Ramanujan local systems on graphs. *Topology*, 36:1007–1024, 1997.

[JY18] Hyungrok Jo and Yoshinori Yamasaki. LPS-type Ramanujan graphs. In *2018 International Symposium on Information Theory and Its Applications (ISITA)*, pages 399–403, 2018.

[Kap69] Irving Kaplansky. Submodules of quaternion algebras. *Proceedings of the London Mathematical Society*, pages 219–232, 1969.

[Kat76] Nicholas M. Katz. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. *Proceedings of Symposia in Pure Mathematics*, 1976.

[Kaz67] D. A. Kazhdan. Connection of the dual space of a group with the structure of its closed subgroups. *Funct. Anal. Appl.*, 1:63–65, 1967.

[Kob84] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*, volume 97 of *Grad. Texts Math.* Springer, Cham, 1984.

[Lam73] T. Y. Lam. *The Algebraic Theory of Quadratic Forms*. Math. Lect. Note Ser. The Benjamin/Cummings Publishing Company, Reading, MA, 1973.

[Lem21] F. Lemmermeyer. *Quadratic Number Fields*. Springer Undergraduate Mathematics Series. Springer International Publishing, 2021.

[Len97] H. W. Lenstra. Galois theory for schemes. https://websites.math.leidenuniv.nl/algebra/GSchemes.pdf, 1997.

[LPS88] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[Lub94] Alexander Lubotzky. *Discrete Groups, Expanding Graphs and Invariant Measures.* Princeton University Press, 1994.

[Mar73] G. A. Margulis. Explicit construction of a concentrator. *Probl. Peredachi Inf.*, 9(4):71–80, 1973.

[Mar88] G. A. Margulis. Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):51–60 (in Russian), 1988. English translation in *Problems of Information Transmission*, 24, 39–46, 1988.

[Mil13] James S. Milne. Class field theory. https://www.jmilne.org/math/CourseNotes/cft.html, 2013.

[Miy89] Toshitsune Miyake. *Modular Forms.* Berlin etc.: Springer-Verlag, 1989.

[ML98] Saunders Mac Lane. *Categories for the Working Mathematician.*, volume 5 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed edition, 1998.

[Mor17] L. J. Mordell. On Mr. Ramanujan's empirical expansions of modular functions. *Proc. Camb. Philos. Soc.*, 19:117–124, 1917.

[Mor94] Moshe Morgenstern. Existence and explicit constructions of q + 1 regular Ramanujan graphs for every prime power q. *J. Comb. Theory, Ser. B*, 62:44–62, 1994.

[MS18] Marvin Minei and Howard Skogman. Ramanujan graphs arising as weighted Galois covering graphs. *Electron. J. Graph Theory Appl.*, 6:123–137, 2018.

[MSS15] Adam W. Marcus, Daniel A. Spielman, and Nikhil Srivastava. Interlacing families. I: Bipartite Ramanujan graphs of all degrees. *Ann. Math. (2)*, 182(1):307–325, 2015.

[Nil91] Alon Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91:207–210, 1991.

[Ogg69] A. Ogg. Modular forms and Dirichlet series. New York - Amsterdam: W. A. Benjamin, Inc. XVI, 173 p (1969)., 1969.

[Pet40] Hans Petersson. Über eine metrisierung der automorphen formen und die theorie der poincaréschen reihen. *Mathematische Annalen*, 117:453–537, 1940.

[Pin73] M. Pinsker. On the complexity of a concentrator. *7th Annual Teletraffic Conference*, pages 318/1–318/4, 1973.

[Piz80a] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64:340–390, 1980.

[Piz80b] Arnold Pizer. Theta series and modular forms of level p^2M. *Compos. Math.*, 40:177–241, 1980.

[Piz90] Arnold Pizer. Ramanujan graphs and Hecke operators. *Bull. Am. Math. Soc., New Ser.*, 23(1):127–137, 1990.

[Piz98] Arnold Pizer. Ramanujan graphs. In *Computational perspectives on number theory. Proceedings of a conference in honor of A. O. L. Atkin, Chicago, IL, USA, September 1995*, pages 159–178. Providence, RI: American Mathematical Society, 1998.

[Rei75] Irving Reiner. *Maximal Orders*, volume 5 of *Lond. Math. Soc. Monogr.* Academic Press, London, 1975.

[Rei08] Omer Reingold. Undirected connectivity in log-space. *J. ACM*, 55(4), sep 2008.

[RVW02] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Ann. Math. (2)*, 155(1):157–187, 2002.

[Sel65] Atle Selberg. On the estimation of Fourier coefficients of modular forms. Proc. Sympos. Pure Math. 8, 1-15 (1965)., 1965.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*, volume 7 of *Grad. Texts Math.* Springer, Cham, 1973.

[Ser94] Jean-Pierre Serre. *Trees*. Springer Berlin, Heidelberg, Berlin–Heidelberg–New York, 1994.

[Ser97] Jean-Pierre Serre. Répartition asymptotique des valeurs propres de l'opérateur de Hecke _. *Journal of the American Mathematical Society*, 10:75–102, 1997.

[Shi58] Goro Shimura. Correspondances modulaires et les fonctions ζ de courbes algebriques. *Journal of the Mathematical Society of Japan*, 10:1–28, 1958.

[Sie35] C. L. Siegel. Über die analytische Theorie der quadratischen Formen. *Ann. Math. (2)*, 36:527–606, 1935.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[Sta15] Richard P. Stanley. *Catalan Numbers*. Cambridge University Press, 2015.

[Tat66] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2:134–144, 1966.

[Val02] Alain Valette. *Introduction to the Baum-Connes conjecture. With notes taken by Indira Chatterji. With an appendix by Guido Mislin*. Basel: Birkhäuser, 2002.

[Voi21] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer International Publishing, 2021.

[Wal94] Lynne Walling. A remark on differences of theta series. *Journal of Number Theory*, 48:243–251, 1994.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Annales Scientifiques de l' École normale supérieure*, 2:521–560, 1969.