CARLETON UNIVERSITY

SCHOOL OF
MATHEMATICS AND STATISTICS

HONOURS PROJECT

TITLE: Algorithms for Computing Matrices of Hecke Operators With Conjectured Connections to Modular Forms

AUTHOR: Spencer Secord

SUPERVISOR: Colin Ingalls and Adam Logan

DATE: January 12, 2021

# Algorithms for Computing Matrices of Hecke Operators With Conjectured Connections to Modular Forms

Spencer Secord

*Supervisors:* Colin Ingalls and Adam Logan

January 11, 2021

**Abstract**

We conjecture formulas and make observations for the Hecke matrices of several genera of non-degenerate lattices of rank 4 with non-trivial discriminant, and present the algorithms used to generate the data on Kneser p-neighbours needed to formulate these conjectures. The algorithms and conjectures found in this paper are a result of an ongoing project/collaboration between Adam Logan, Colin Ingalls, Dan Fretwell, and Spencer Secord. These conjectured formulas are of the same form (relying on the coefficients of a specific modular form) as the formulas for the Hecke matrices of the genus of $E_8 \oplus E_8$ and the genus of the Niemeier lattices proven by Chenevier and Lannes in [4].

This project is inspired by and uses results proven by Chenevier and Lannes in [4], and we cover select basics from [4] alongside the necessary background material. An attempt is made to create a mostly self-contained treatment, with the exception of the use of the Riemann-Roch theorem in the proof of (5.3.4), and the omission of the proof of (3.2.3).

# Contents


**1 Preliminaries** **3**
- 1.1 Basic Quadratic and Bilinear Algebra . . . 3
- 1.2 Morphisms, Kernels, and Quotients . . . 5
- 1.3 Tensor Products And Localization . . . 8
- 1.4 Direct Summands . . . 9
- 1.5 Lagrangians And Hyperbolic Modules (In General) . . . 11
- 1.6 Conditions for the Existence of a Transverse Lagrangian . . . 12

**2 Lattices (Over Dedekind Domains)** **15**
- 2.1 Basic Definitions . . . 15
- 2.2 Discriminant Group (resp. Module) . . . 15
- 2.3 Discriminant of a Lattice . . . 18
- 2.4 Lagrangians (Over Dedekind Domains) . . . 18

**3 Kneser p-Neighbours** **19**
- 3.1 p-Neighbours and Isotropic Elements of $\mathbb{P}(L/pL)$ . . . 19
- 3.2 Kneser's Connected Genus Theorem . . . 22

**4 Algorithms** **24**
- 4.1 From a Vector to a Neighbour . . . 25
- 4.2 Finding and Counting All p-Neighbours . . . 25

**5 Modular Forms** **30**
- 5.1 Fourier Series and Poisson Summation . . . 30
- 5.2 Group Actions on the Complex Half-Plane . . . 32
- 5.3 Introduction to Modular Functions . . . 33
- 5.4 Modular Forms with a Character . . . 34

**6 Observations and Conjectured Formulas** **36**
- 6.1 Results and Inspiration from Chenevier and Lannes . . . 36
- 6.2 Conjectured Formulas For $T_p$ . . . 37
- 6.3 Similarities Across Different Genera . . . 39

# Acknowledgements

Firstly, I would like to thank my supervisors, Adam Logan and Colin Ingalls, for their mentorship, and for all the time and patience they have given to share their knowledge and expertise. I would like to thank John Voight for allowing me to access his computers: without his kindness this project would not have been possible. I would also like to thank Yuly Billig, who has been a mentor to me during my undergraduate experience, and who heavily influenced my decision to pursue mathematics.


# 1 Preliminaries

**(1.0.1).** All rings will be commutative with 1 and will be considered a Dedekind domain for every section *except* section one (this section).

**(1.0.2).** The material in this section can be found in "*A Course in Arithmetic*" by Serre [15], and "*Quadratic Mappings and Clifford Algebras*" by Helmstetter and Micali [8], or "*Automorphic Forms and Unimodular Lattices*" by Chenevier and Lannes [4], among many others.

## 1.1 Basic Quadratic and Bilinear Algebra

**(1.1.1) Definition.** *(Bilinear Functions and Bilinear Forms).* Let $A$ be a ring, and let $M$, $N$, and $T$ be $A$-modules. A *bilinear function* $(-,-) : M \times N \to T$ is a function of that is $A$-linear in both $M$ and $N$, and thus can be interpreted so that its domain is $M \otimes N$. A *bilinear form* is an $A$-bilinear function whose codomain is $A$. We say an $A$-module $M$ is equipped with a bilinear function (resp. form) if there is an associated bilinear function (resp. form) $(-,-) : M \otimes M \to N$. By abuse of terminology we call $N$ the codomain of $M$ and denote it by $\mathrm{codom}(M)$.

We call a bilinear function (resp. form) *symmetric* if $(x, y) = (y, x)$ for every $x, y$. We call a bilinear function (resp. form) *alternating* if $(x, x) = 0$ for every $x$.

**(1.1.2).** If a bilinear form is alternating, then $(x + y, x + y) = 0$, and thus $(x, y) = -(y, x)$ for all $x$ and $y$.

**(1.1.3) Definition.** *(Dual Mappings, Non-Degeneracy, and Unimodularity).* Let $M$ be $A$-module equipped with a bilinear function $(-,-) : M \otimes M \to \mathrm{codom}(M)$. There is natural mapping to the dual space $M^* = \mathrm{Hom}_A(M, \mathrm{codom}(M))$ denoted $\mathcal{B}_M : M \to M^* = \mathrm{Hom}_A(M, \mathrm{codom}(M))$ where $\mathcal{B} : x \mapsto (x, -)$. This is called the right *induced dual mapping*. The left induced dual mapping is similarly defined.

By abuse of terminology, we may say "the induced dual mapping has property $X$" to mean that both the left and right dual mappings have the property $X$.

We call $M$ *non-degenerate* if the induced dual mappings are injective. We call $M$ *unimodular* if the induced dual mappings are isomorphisms of $A$-modules.

**(1.1.4).** Note that for symmetric and alternating bilinear functions, right non-degeneracy is equivalent to left non-degeneracy.

**(1.1.5) Examples.** *(Bilinear Functions and Forms).*

(i) (Euclidean Inner Product). Consider the bilinear function on $\mathbb{R}^n$ which sends $(x, y) \to \sum_i x_i y_i$.

This is called the *euclidean inner product*, and plays an important part in real analysis. It is symmetric and unimodular.

(ii) (Inner Product In Function Spaces). Consider the vector space of continuous functions from $[0,1]$ to $\mathbb{R}$. This space has a natural bilinear form $\langle f, g\rangle \mapsto \int_0^1 f(x)\, g(x)\, dx$. Inner products on spaces of functions are an important tool in functional analysis. This is an especially important perspective to have when considering Fourier series and Fourier transformations.

(iii) (Cross Product). Consider the cross product $\times : \mathbb{R}^3 \otimes \mathbb{R}^3 \to \mathbb{R}^3$ defined in the canonical way. This is an alternating bilinear function. Any Lie bracket is an alternating bilinear form, which is non-degenerate if and only if the center of the Lie algebra is trivial.

(iv) (Hilbert Symbol). Example taken from "*A Course in Arithmetic*" by Serre [15, Chapter 3]. Let $k$ be $\mathbb{R}$ or a p-adic field $\mathbb{Q}_p$. Let $(k^*, \cdot)$ be its multiplicative group of units. Consider the function (not bilinear) from $k^* \times k^* \to \mathbb{F}_2$ defined by

$$(a,b) = \begin{cases} 0 & \text{if } ax^2 + by^2 - z^2 \text{ has a non-zero solution in } k^3 \\ 1 & \text{otherwise} \end{cases}$$

$(a,b)$ is called the Hilbert Symbol of $a$ and $b$. Note that the value of $(a,b)$ does not change when $a$ or $b$ are multiplied by squared numbers. Thus we can define this function on the group $(k^*/k^{*2}, \cdot)$. This is an abelian group, and furthermore is an $\mathbb{F}_2$ vector space by the action $a.g = g^a \ \forall g \in k^*/k^{*2}, a \in \mathbb{F}_2$. The Hilbert Symbol is a non-degenerate symmetric bilinear form on the $\mathbb{F}_2$-vector space $k^*/k^{*2}$, although this is non-trivial (see [15, page 20]).

**(1.1.6) Definition.** *(Quadratic Functions and Forms).* Let $M, N$ be two $A$-modules. We say the mapping (not homomorphism) $q : M \to N$ is *quadratic* if:

(i) $q(ax) = a^2 q(x)$

(ii) The mapping $(-,-) : M \times M \to N$ given by $(x,y) = q(x+y) - q(x) - q(y)$ is bilinear.

If $N = A$ we call $q$ a *quadratic form.* We will call $q$ non-degenerate, unimodular, etc, if the corresponding bilinear form is non-degenerate, unimodular, etc. When we refer to the dual mapping induced by $q$, we mean the dual map induced by the corresponding bilinear form, as defined in (1.1.3).

**(1.1.7) Definition.** *(Isotropic Submodules and Lagrangian Submodules).* Let $M$ be $A$-module equipped with a bilinear function. For any subset $N \subseteq M$ and any submodule $Y \subseteq \mathrm{codom}(M)$, we define

$$N^{\#Y} := \{x \in M \mid (x,z) \in Y \text{ and } (z,x) \in Y \text{ for every } z \in N\}$$

We say that a submodule $I \subseteq M$ is *isotropic* if $I \subseteq I^{\#0}$. We say $I$ is a *Lagrangian* if $I = I^{\#0}$. Two Lagrangians $I$, $J$ are called *transverse* if $I \cap J = \{0\}$.

**(1.1.8) Remark.** The use of the notation # is niche but useful - it improves the readability of many of the proofs given, has categorical importance (1.2.3), and allows for better exemplification of correspondences (1.2.7).

For reference: in [4], given structures $J \subseteq L$, the module $J^{\#0}$ is written as $J^{\perp}$, $J^{\#pA}$ is written as $M_d(L;J)$, and given $L \subseteq K \otimes L$, the module $L^{\#A}$ is written as $L^{\#}$ (since $A$ is almost always $\mathbb{Z}$

or $\mathbb{Z}_p$ in [4]). In the theory of Lie algebras, $J^{\#0}$ is called the centralizer of $J$, and $J^{\#J}$ is called the normalizer of $J$. In the theory of toric varieties, for an element $u \in \mathbb{R}^n$, $u^{\#0}$ is written as $H_u$, $u^{\#\mathbb{R}_+}$ is written as $H_u^+$, and $u^{\#b+\mathbb{R}_+}$ is written as $H_{u,b}^+$ [6, page xiii].

**(1.1.9) Lemma.** *Let $M$ be $A$-module equipped with a bilinear function with codomain codom$(M)$. Let $L$ and $J$ be subsets of $M$. Let $X$ and $Y$ be submodules of codom$(M)$. Then the following are true*

*(i) For any $f$ in $A$, we have $fL^{\#X} \subseteq L^{\#fX}$.*

*(ii) For any ideal $\alpha$ over $A$, we have $\alpha(L^{\#X}) \subseteq L^{\#\alpha X}$.*

*(iii) If $J$ is contained in $L$, then $L^{\#X}$ is contained in $J^{\#X}$.*

*(iv) If $X$ is contained in $Y$, then $L^{\#X}$ is contained in $L^{\#Y}$.*

*(v) For a family of subsets $L_i$ of $M$, $(\bigcup_{i\in I} L_i)^{\#X} = \bigcap_{i\in I} L_i^{\#X}$*

*(vi) For a family of subsets $X_i$ of $X$, $L^{\#\bigcup_{i\in I} X_i} = \bigcup_{i\in I} L^{\#X_i}$ and $L^{\#\bigcap_{i\in I} X_i} = \bigcap_{i\in I} L^{\#X_i}$*

*Proof.* The proofs follow from definition (1.1.7). ■

## 1.2 Morphisms, Kernels, and Quotients

**(1.2.1) Definition.** *(Morphism).* Let $M, N$ be $A$-modules equipped with bilinear functions. We say $f : M \to N$ is a *morphism* of modules equipped with a bilinear function if $f$ is a morphism of $A$-modules paired with a second morphism of $A$-modules $\tilde{f} : \text{codom}(M) \to \text{codom}(N)$ such that

$$\big(f(x), f(y)\big) = \tilde{f}\big((x, y)\big) \qquad (\forall x, y \in M)$$

If $M$ and $N$ are equipped with bilinear forms, then we say $f$ is a *morphism of bilinear formed modules* if $\tilde{f}$ is identity (ie $f$ preserves the bilinear form)

**(1.2.2) Lemma.** *Let $f : M \to N$ be a morphism of modules equipped with a bilinear function. Let $J \subseteq N$ and $X \subseteq$ codom$(N)$. Then*

$$f^{-1}\big(J^{\#X}\big) \subseteq f^{-1}(J)^{\#\tilde{f}^{-1}(X)}$$

*with equality if $f$ is surjective. Let $I \subseteq M$ and $Y \subseteq$ codom$(M)$. Then*

$$f\big(I^{\#Y}\big) \subseteq f(I)^{\#\tilde{f}(Y)}$$

*with equality if $f$ is surjective and* $\ker \tilde{f} \subseteq Y$.

*Proof.* First, we will show $f^{-1}(J^{\#X}) \subseteq f^{-1}(J)^{\#\tilde{f}^{-1}(X)}$. Let $x \in f^{-1}(J^{\#X})$. Then, $f(x) \in J^{\#X}$ implies $(f(x), J) \subseteq X$ and thus $\tilde{f}^{-1}(f(x), J) \subseteq \tilde{f}^{-1}(X)$. Hence,

$$(x, f^{-1}(J)) \subseteq (f^{-1}(f(x)), f^{-1}(J)) \subseteq \tilde{f}^{-1}(f(x), J) \subseteq \tilde{f}^{-1}(X)$$

From a symmetrical argument, we can get $(f^{-1}(J), x) \subseteq \tilde{f}^{-1}(X)$. Therefore $f^{-1}(J^{\#X}) \subseteq f^{-1}(J)^{\#\tilde{f}^{-1}(X)}$.

We need to prove that $f^{-1}(J^{\#X}) = f^{-1}(J)^{\#\tilde{f}^{-1}(X)}$ when $f$ is surjective. Let $x \in f^{-1}(J)^{\#\tilde{f}^{-1}(X)}$ and assume $f$ is surjective. By definition, $(x, f^{-1}(J)) \subseteq \tilde{f}^{-1}(X)$ and hence $\tilde{f}(x, f^{-1}(J)) \subseteq$

$\tilde{f}(\tilde{f}^{-1}(X))$ which implies $(f(x), f(f^{-1}(J))) \subseteq \tilde{f}(\tilde{f}^{-1}(X))$. Since $f$ is assumed to be surjective, $f(f^{-1}(J)) = J$. Thus $(f(x), J) = (f(x), f(f^{-1}(J))) \subseteq \tilde{f}(\tilde{f}^{-1}(X)) \subseteq X$. By a symmetrical argument, $(J, f(x)) \subseteq X$. Thus, $f$ surjective implies $f^{-1}(J^{\#X}) = f^{-1}(J)^{\#\tilde{f}^{-1}(X)}$.

Next, we will prove $f(I^{\#Y}) \subseteq f(I)^{\#\tilde{f}(Y)}$. Let $x \in f(I^{\#Y})$. This means there is some $y \in f^{-1}(x)$ such that $y \in I^{\#Y}$, which is equivalent to $(y, I) \subseteq Y$. Applying $\tilde{f}$ we get $(x, f(I)) = (f(y), f(I)) = \tilde{f}(y, I) \subseteq \tilde{f}(Y)$. Thus $(x, f(I)) \subseteq \tilde{f}(Y)$. By a symmetric argument, we get $(f(I), x) \subseteq \tilde{f}(Y)$. Therefore $f(I^{\#Y}) \subseteq f(I)^{\#\tilde{f}(Y)}$.

Finally, we need to show that if $f$ is surjective and $\ker \tilde{f} \subseteq Y$, then $f(I^{\#Y}) = f(I)^{\#\tilde{f}(Y)}$. Let $x \in f(I)^{\#\tilde{f}(Y)}$, assume $f$ is surjective and $\ker \tilde{f} \subseteq Y$. Since $f$ is surjective, there is some $y$ such that $x = f(y)$. Thus $(f(y), f(I)) \subseteq \tilde{f}(Y)$, implying $\tilde{f}(y, I) \subseteq \tilde{f}(Y)$. Since $\ker \tilde{f} \subseteq Y$ we know $\tilde{f}^{-1}(\tilde{f}(Y)) = Y$ and hence $(y, I) \subseteq \tilde{f}^{-1}(\tilde{f}(y, I)) \subseteq \tilde{f}^{-1}(\tilde{f}(Y)) = Y$. A symmetric argument yields $(I, y) \subseteq Y$, and thus $y \in I^{\#Y}$ which implies $x = f(y) \in f(I^{\#Y})$. Therefore, if $f$ is surjective and $\ker \tilde{f} \subseteq Y$, then $f(I^{\#Y}) \subseteq f(I)^{\#\tilde{f}(Y)}$. ■

**(1.2.3) Definition.** *(Kernels and Quotients).* Let $f : M \to N$ be any morphism of modules equipped with bilinear functions, as defined in (1.2.1). The kernel of the $A$-module morphism $M \to N$ has a natural bilinear function:

$$(-,-) : \ker f \otimes \ker f \to \ker \tilde{f}$$

We will call this module equipped with this bilinear function the *kernel* of $f$. It can be checked that this satisfies the categorical definition of a kernel in the category with objects being modules equipped with a bilinear function, and morphisms of the category being those given in definition (1.2.1).

The kernel of $f$ has the important property that $M = (\ker f)^{\#\ker \tilde{f}}$. Conversely, given any submodule $J \subseteq M$ with bilinear function $J \otimes J \to \mathrm{codom}(J) \subseteq \mathrm{codom}(M)$ that agrees with the bilinear function on $M$, we can say the bilinear function on $M$ induces a bilinear function $M/J \otimes M/J \to \mathrm{codom}(M)/\mathrm{codom}(J)$ if and only if $M = J^{\#\mathrm{codom}(J)}$. Thus we know that any $J$ with the property $M = J^{\#\mathrm{codom}(J)}$ is a *kernel*, and $M/J$ its *quotient* (with its resulting bilinear function implicitly included). In summary:

$$J \textit{ is a kernel of } M \iff M = J^{\#\mathrm{codom}(J)}$$

where the codomain of $J$ is an implicit part of its definition, and will contain but not necessarily equal its range (ie $\mathrm{codom}(J) \neq (J, J)$ in general).

**(1.2.4).** The specification of codomain in such a sub-object is an important part of its structure. For example, the zero module $(0) \subseteq M$ with codomain $(0)$ is always a kernel since it is the kernel of the identity function (it is the zero object) - but the zero module with codomain equal to the codomain of $M$ can be a kernel if and only if the bilinear function on $M$ is trivial.

**(1.2.5) Remark.** *(Isomorphism Theorems).* The first, second, and third isomorphism theorems hold, *mutatis mutandis*, when using definition (1.2.3). Moreover, it will be proven in (1.2.7) that the corresponding fourth isomorphism theorem (also known as the correspondence theorem) also holds in this setting. This is worth mentioning, as the isomorphism theorems for most commonly used structures are corollaries of the isomorphism theorems formulated in terms of universal algebras [7, §11], and yet the structure of modules equipped with a bilinear form are not types of universal algebras.

**(1.2.6) Examples.** *(Examples of Kernels).*

(i) Consider $\mathbb{Z}^3$ with bilinear form defined by the Gram matrix

$$M = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

We know $Me_3^t = 0$ and thus $xMe_3^t = 0$ for any $x \in \mathbb{Z}^3$. Thus $(\mathbb{Z}e_3)^{\#0} = (\mathbb{Z}e_3)^{\perp} = \mathbb{Z}^3$ and therefore $\mathbb{Z}e_3$ with codomain 0 is a kernel.

(ii) Consider $\mathbb{Z}^4$ equipped with a bilinear function to $\mathbb{Q}$ defined by the Gram matrix

$$M = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 1 \\ 0 & 0 & 1 & \frac{1}{3} \end{pmatrix}$$

Consider the submodule $L = 2\mathbb{Z}e_1 + 2\mathbb{Z}e_2 + 3\mathbb{Z}e_3 + 3\mathbb{Z}e_4$ with codomain $\mathbb{Z}$. This is a kernel whose quotient space $\mathbb{Z}^4/L$ will be a module isomorphic (as a regular module) to $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^3$ with bilinear function to $\mathbb{Q}/\mathbb{Z}$ given by the Gram matrix

$$\begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & \frac{1}{3} \end{pmatrix}$$

with values in $\mathbb{Q}/\mathbb{Z}$.

(iii) Let $R$ be a *(commutative) ring*. Consider $R$ as an $R$-module equipped with the bilinear form corresponding to the ring multiplication. Let $I \lhd R$ be an ideal of $R$ and consider $I$ as a subobject of $R$ where $\mathrm{codom}(I) = I$. Then $I$ is a kernel of $R$, and the resulting quotient $R/I$ is isomorphic (as an $R$-module equipped with a bilinear function) to the quotient ring $R/I$ with the bilinear function being multiplication in $R/I$. The same is true for ideals in *Lie algebras*.

(iv) Let $M = \mathbb{Z}^{2n+1}$ be a $\mathbb{Z}$-module equipped with the symmetric bilinear form

$$(\bar{x}, \bar{y}) = \sum_{m=1}^{2n+1} \Big(\sum_{\substack{i=1 \\ i \neq m}}^{2n+1} x_i\Big)\Big(\sum_{\substack{i=1 \\ i \neq m}}^{2n+1} y_i\Big)$$

Consider the submodule $J$ of $M$, whose elements are those with all entries even, or all entries odd. Consider $J$ with codomain the even numbers (i.e. $2\mathbb{Z}$), this is a kernel of $M$. The quotient space $M/J$ is a bilinear formed $\mathbb{F}_2$-vector space. This $\mathbb{F}_2$-bilinear form is equivalent to the Euclidean inner product minus the product of the $L^1$-norms of both input vectors.

**(1.2.7) Lemma.** *(Correspondence Theorem / Fourth Isomorphism Theorem) Let $M$ be a module equipped with a bilinear function, and let $J \subseteq M$ be a kernel as defined in* (1.2.3)*. Then there is a one-to-one correspondence between kernels in $M/J$ and kernels $I \subseteq M$ such that $J \subseteq I$ and $\mathrm{codom}(J) \subseteq \mathrm{codom}(I)$. Furthermore, there is a correspondence between isotropic submodules in $M/J$ and submodules in $M$ that contain $J$ and have the same codomain as $J$.*

*Proof.* Let $\phi : M \to M/J$ be the canonical morphism as described in (1.2.1). Given a module $I$ where $J \leq I$ and $\text{codom}(J) \leq \text{codom}(I)$, by (1.2.2) if $I^{\#\text{codom}(I)} = M$ then $M/J = \phi(M) = \phi(I^{\#\text{codom}(I)}) \subseteq f(I)^{\#\text{codom}(\tilde{f}(I))}$. Thus $f(I)^{\#\text{codom}(\tilde{f}(I))} = M/J$ and thus the image of $I$ must be a kernel.

If $I/J$ is a kernel in $M/J$, then by (1.2.2), $M = f^{-1}(M/J) = f^{-1}\big((I/J)^{\#\text{codom}(I/J)}\big) \subseteq f^{-1}(I/J)^{\#\tilde{f}^{-1}(\text{codom}(I/J))}$. Thus the module $f^{-1}(I/J)$ with codomain $\tilde{f}^{-1}(\text{codom}(I/J))$ must be a kernel since $M = f^{-1}(I/J)^{\#\tilde{f}^{-1}(\text{codom}(I/J))}$. ■

## 1.3 Tensor Products And Localization

**(1.3.1).** The tensor product of modules in the category of modules equipped with bilinear functions behaves exactly as one would expect. Given $M$ and $N$, you tensor the modules and for the codomain, you tensor the codomains of $M$ and $N$.

**(1.3.2) Definition.** *(Tensor Product).* Let $N$ and $M$ be $A$-modules, both equipped with bilinear functions (resp. forms). Then the tensor product $M \otimes N$ inherits a bilinear function (resp. form) $(M \otimes N) \otimes (M \otimes N) \to \text{codom}(M) \otimes \text{codom}(N)$ given by $((x_1 \otimes y_1),\ (x_2 \otimes y_2)) = (x_1, x_2)_M \otimes (y_1, y_2)_N$.

**(1.3.3).** Although not used here, it is a useful exercise to confirm that the universal property that defines tensor products in the category of modules also works for tensor products in the category of $A$-modules equipped with a bilinear function or the category of $A$-modules equipped with a bilinear function.

**(1.3.4) Definition.** *(Localization).* Let $M$ be an $A$-module equipped with a bilinear function. The localization of $M$ by $S$, denoted $S^{-1}M$, is equipped with an $S^{-1}A$-bilinear form

$$(-,-) : S^{-1}M \otimes S^{-1}M \to S^{-1}\text{codom}(M)$$

Moreover, $S^{-1}M$ is canonically isomorphic to $(S^{-1}A) \otimes M$ as $S^{-1}A$-modules with $S^{-1}A$-bilinear functions (resp. $S^{-1}A$-bilinear forms).

**(1.3.5) Definition.** *(Local Property).* For a prime ideal $\mathfrak{p}$ of $A$, the localization of $A$ at $\mathfrak{p}$ is the ring $(A \setminus \mathfrak{p})^{-1}A$. A property $P$ is called a *local property* if, for every $M$, the object $M$ has property $P$ if and only if the localization of $M$ by $\mathfrak{p}$ has property $P$ for every prime ideal $\mathfrak{p}$.

**(1.3.6) Lemma.** *Let $A$ be any ring, let $M$ be an $A$-module equipped with a bilinear function, let $N$ and $H$ be submodules of $M$, and let $Y \subseteq codom(M)$. Then, $N = H^{\#Y} \iff$ the following sequence is exact:*

$$N \hookrightarrow M \xrightarrow{\rho_R \oplus \rho_L} \text{Hom}_A(H, codom(M)/Y) \oplus \text{Hom}_A(H, codom(M)/Y)$$

*Where $\rho_R$ (resp. $\rho_L$) is the composition of the morphism $M \to \text{Hom}(M, codom(M)/Y)$ given by $x \mapsto (x,-)+Y$ (resp. $x \mapsto (-,x)+Y$), and $i^* : \text{Hom}(M, codom(M)/Y) \to \text{Hom}(H, codom(M)/Y)$ which is the image of the inclusion $i : H \to M$ under the contravariant functor $\text{Hom}_A(-, codom(M)/Y)$.*

*Proof.* The kernel of $i^*$ is the set of functions from $M$ to $\text{codom}(M)/Y$ that are zero on $H$. The only elements whose image under both $x \mapsto (x,-)+Y$ and $x \mapsto (-,x)+Y$ are zero when restricted to $N$ are precisely the elements of $H^{\#Y}$. This implies $ker(\rho_R \oplus \rho_L) = H^{\#Y}$. The image of the inclusion $N \to M$ is $N$, and hence the diagram is exact if and only if $H^{\#Y} = N$. ■

**(1.3.6.1) Corollary.** *(Stated in the proof of [4, Proposition 2.1.2]). Let $A$ be any ring, let $M$ be an $A$-module equipped with a symmetric or alternating bilinear function, and let $N$ be any submodule of $M$. Then, $N$ is Lagrangian $\iff$ the following sequence is exact:*

$$N \xrightarrow{\ i\ } M \xrightarrow{\ \rho\ } \mathrm{Hom}_A(N, \mathit{codom}(M))$$

*$\rho$ is the composition of the morphism $M \to M^*$ given by $x \mapsto (x, -)$, and $i^* : M^* \to N^*$ which is the image of $i$ under the contravariant functor $\mathrm{Hom}_A(-, \mathit{codom}(M))$.*

*Proof.* Follows from (1.3.6). ■

**(1.3.6.2) Corollary.** *Let $N$ be a submodule of $M$, let $Y$ be a submodule of $\mathit{codom}(M)$, and let $S$ be a multiplicatively closed subset of $A$. Then,*

$$S^{-1}(N^{\#X}) = (S^{-1}N)^{\#S^{-1}X}$$

*Proof.* Follows from (1.3.6) and the fact that exactness of a diagram is a local property. ■

**(1.3.6.3) Corollary.** *The following are true:*

*(i) If $N$ is a submodule of $M$, then the property that "$N$ is a Lagrangian of $M$" is a local property.*

*(ii) Non-degeneracy is a local property.*

*(iii) Unimodularity is a local property.*

*Proof.* $(i)$ and $(ii)$ follow from (1.3.6). $(iii)$ follows from the fact that $M$ is unimodular if and only if both $0 \to M \xrightarrow{\mathcal{B}_R} \mathrm{Hom}(M, \mathrm{codom}(M)) \to 0$ and $0 \to M \xrightarrow{\mathcal{B}_L} \mathrm{Hom}(M, \mathrm{codom}(M)) \to 0$ are exact, where $\mathcal{B}_R$ and $\mathcal{B}_L$ are the right and left dual mappings (1.1.3). ■

## 1.4 Direct Summands

**(1.4.1).** Let $S$ be any $A$-module. Here we will restrict our focus to the (sub)category containing $A$-modules with a bilinear function whose codomain is $S$. This will allow for more specific and useful results.

**(1.4.2) Definition.** *(Direct Sum).* Let $\{M_i\}_{i\in I}$ be a family of $A$-modules equipped with bilinear function with codomain $S$. Define the *direct sum* $\bigoplus_{i\in I} M_i$ to be the module $\bigoplus_{i\in I} M_i$ equipped with the bilinear function to $S$ given by

$$\left(\bigoplus_{i\in I} x_i\,,\, \bigoplus_{i\in I} y_i\right) = \sum_{i\in I}(x_i, y_i) \in S$$

**(1.4.3) Remark.** It can be checked that the definition (1.4.2) satisfies the categorical definition of the direct sum in the category with the objects being *$A$-modules with a bilinear function which has codomain $S$*, and morphisms being those that preserve the bilinear functions. This is not true in the larger category of modules with a bilinear function (with morphisms as defined in (1.2.1)). The reason we are looking at the direct summation defined only in this subcategory is that it offers some convenient decompositions that will become useful later.

**(1.4.4) Proposition.** *(Structure Theorem For Finitely Generated Torsion Modules Over a Dedekind Domain With a Bilinear Function). Let $A$ be a Dedekind domain, and let $M$ any finitely generated torsion $A$-module. Let $\alpha$ be the annihilator of $M$, and let $\alpha = \prod_{i=1}^{s} \mathfrak{p}_i^{n_i}$ be its canonical decomposition. Let $M_{\mathfrak{p}_i}$ be the submodule of $M$ defined by $M_{\mathfrak{p}_i} := \{x \in M \ ; \ \mathfrak{p}_i^r x = 0 \text{ for some } r\}$, and equipped them with the bilinear form inherited from $M$. Then,*

$$M \cong \bigoplus_{i=1}^{s} M_{\mathfrak{p}_i}$$

*Where the isomorphism is canonical and preserves the bilinear function with codomain $S$.*

*Proof.* The structure theorem for finitely generated modules over a Dedekind domain gives us the isomorphism of modules $M \cong \bigoplus_{j=1}^{s} M_{\mathfrak{p}_i}$. Now, we need only prove that this conserves the bilinear function. Specifically, we need to show that if $i \neq j$ then $(M_{\mathfrak{p}_i}, M_{\mathfrak{p}_j}) = 0$. Let $x \in M_{\mathfrak{p}_i}$ and let $y \in M_{\mathfrak{p}_j}$, then there is a $n$ such that $\mathfrak{p}_i^n x = 0$ and $\mathfrak{p}_j^n y = 0$. Note that $A$ is a Dedekind domain, and thus of Krull dimension at most one. Thus $\mathfrak{p}_i + \mathfrak{p}_j = A$, and hence $A = (\mathfrak{p}_i + \mathfrak{p}_j)^{2n} = \mathfrak{p}_i^n\big(\sum_{k=0}^{n} \binom{2n}{k} \mathfrak{p}_i^k \mathfrak{p}_j^{n-k}\big) + \mathfrak{p}_j^n\big(\sum_{k=0}^{n} \binom{2n}{k} \mathfrak{p}_j^k \mathfrak{p}_i^{n-k}\big) \subseteq \mathfrak{p}_i^n + \mathfrak{p}_j^n \subseteq A$. Hence $A = \mathfrak{p}_i^n + \mathfrak{p}_j^n$, and thus:

$$A \cdot (x, y) = (\mathfrak{p}_i^n + \mathfrak{p}_j^n) \cdot (x, y) = (\mathfrak{p}_i^n x, y) + (x, \mathfrak{p}_j^n y) = 0$$

But $A \cdot (x, y) = 0$ implies that $(x, y) = 0$, which is what was needed. ■

**(1.4.4.1) Corollary.** *Let $A$ be a Dedekind domain, and let $M$ any (torsion) $A$-module (not necessarily finitely generated) with non-trivial annihilator. Let $\alpha$ be the annihilator of $M$, and let $\alpha = \prod_{i=1}^{s} \mathfrak{p}_i^{n_i}$ be its canonical decomposition. Let $M_{\mathfrak{p}_i}$ be the submodule of $M$ defined by $M_{\mathfrak{p}_i} := \{x \in M \ ; \ \mathfrak{p}_i^r x = 0 \text{ for some } r\}$, and equipped them with the bilinear form inherited from $M$. Then,*

$$M \cong \bigoplus_{i=1}^{s} M_{\mathfrak{p}_i}$$

*Where the isomorphism is canonical and preserves the bilinear function with codomain $S$.*

*Proof.* Note that $M$ is equal to the union of all its finitely generated submodules. Since the annihilator of a submodule of $M$ will contain the annihilator of $M$, the annihilator of any submodule of $M$ can only have powers of the prime ideals $\{\mathfrak{p}_i\}_{i=1}^{s}$ in its canonical decomposition. Note that $M_{\mathfrak{p}_i} = \bigcup_N N_{\mathfrak{p}_i}$ where $N$ is taken over all finitely generated submodules. The proof then follows from applying (1.4.4) to each finitely generated submodule of $M$. ■

**(1.4.5) Lemma.** *Let $\{M_i\}$ be a family of modules equipped with bilinear functions, all of which share a codomain $S$. Let $M = \bigoplus_i M_i$. Then the following are true:*

*(i) $\bigoplus_i M_i$ is non-degenerate if and only if each $M_i$ is non-degenerate.*

*(ii) $\bigoplus_i M_i$ is unimodular if and only if each $M_i$ is unimodular.*

*(iii) $L$ is a Lagrangian for $\bigoplus_i M_i$ if and only if $L \cap M_i$ is a Lagrangian for each $M_i$. In particular, a Lagrangian for $\bigoplus_i M_i$ can be viewed as a direct summand of Lagrangians $L_i$ for each $M_i$.*

*Proof.* (i) comes from the fact that for any $x_i \in M_i$, we have $(y, x_i) = (\pi_i(y), x_i)$ and $(x_i, y) = (x_i, \pi_i(y))$. (ii) follows from the fact that $(\bigoplus_i x_i, \bigoplus_i M_i) = \bigoplus_i (x_i, M_i)$ and $(\bigoplus_i M_i, \bigoplus_i x_i) = \bigoplus_i (M_i, x_i)$. (iii) is a result of (ii) and the fact that $\mathrm{Hom}(\bigoplus_i M_i, S) = \bigoplus_i \mathrm{Hom}(M_i, S)$. For (iv), note that $L = L^{\#0} = \bigoplus_i \pi_i(L)^{\#0}$ and hence $L = \bigoplus_i (L \cap M_i)$, which implies $\bigoplus_i (L \cap M_i)^{\#0} = L^{\#0} = L = \bigoplus_i (L \cap M_i)$. Thus $L^{\#0} = L$ if and only if $(L \cap M_i)^{\#0} = L \cap M_i$ for each $i$. ■

## 1.5 Lagrangians And Hyperbolic Modules (In General)

Lagrangians are a special kind of isotropic submodule (see definition (1.1.7)). They arise naturally and have many interesting properties. Our main motivation for looking at hyperbolic modules is their connections to Lagrangians - hyperbolic modules are always the direct summand of two Lagrangians. Later in this section, we will find that the converse is also true: if a module with a unimodular bilinear form is the direct summand of two of its Lagrangians, then it must be isomorphic to a hyperbolic module. In fact, in most situations we consider here, it is enough to show a lattice has one Lagrangian to show it is isomorphic to a hyperbolic module.

**(1.5.1) Definition.** (Hyperbolic Modules). Let $M$ and $N$ be an $A$-modules. Define $H(M) := M \oplus \mathrm{Hom}_A(M, N)$ to be the hyperbolic module, which is equipped with one of two bilinear forms:

(i) (Symmetric). $\big((x_1 \oplus x_2), (y_1 \oplus y_2)\big) \mapsto (x_2 \circ y_1) + (y_2 \circ x_1)$ in which case we call $H(M)$ the *symmetric hyperbolic module* and denote it $H_+(M)$ when this choice is not obvious.

(ii) (Alternating). $\big((x_1 \oplus x_2), (y_1 \oplus y_2)\big) \mapsto (x_2 \circ y_1) - (y_2 \circ x_1)$ in which case we call $H(M)$ the *alternating hyperbolic module* and denote it $H_-(M)$ when this choice distinction is not obvious.

**(1.5.2).** We consider mainly hyperbolic modules with codomain $A$, or codomain $Frac(A)/A$ (i.e., the quotient of the field of fractions of $A$ by the Dedekind domain $A$, as $A$-modules). Also, $H(M) := M \oplus \mathrm{Hom}_A(M, N)$ will be non-degenerate if and only if $\mathrm{Hom}_A(\mathrm{Hom}_A(M, N), N)$ is isomorphic to $M$ via the canonical $A$-module morphism. If the hyperbolic module has a bilinear form (ie $N = A$) then modules in which $\mathrm{Hom}_A(\mathrm{Hom}_A(M, N, N)) \cong M$ (via the canonical morphism) are called reflexive. Every vector space, projective module, or self-dual $A$-module is reflexive.

**(1.5.3) Example.** Here are some examples of Lagrangians:

(i) Let $V$ be the $\mathbb{R}$-vector space of continuous functions $f : [-1, 1] \to \mathbb{R}$ and equip $V$ with the symmetric bilinear form

$$(f, g) = \int_{-1}^{1} x\, g(x)\, f(x)\, dx$$

This is a degenerate bilinear form, and moreover, it can be shown (using some basic real analysis) that both the subspace consisting of even functions, and the subspace consisting of odd functions, are Lagrangians. Thus $V$ is the sum of two transverse Lagrangians.

(ii) (Taken from [4, page 23]). Consider the $\mathbb{F}_2$-vector space $W := \mathbb{F}_2 \oplus \mathbb{F}_2$ with bilinear form given by $(x, y) \mapsto x^t \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} y$. Here, $\mathbb{F}_2 \oplus 0$ will be a Lagrangian of $W$. Note that $W$ is non-degenerate, and yet $\mathbb{F}_2 \oplus 0$ has no transverse Lagrangian. This serves as the main reason for our restriction of case $(i)$ of (1.6.2) to fields *not* of characteristic 2.

(iii) Let $M$ be a free $A$-module, and $K$ the fraction field of $A$. Let $H(M)$ be any hyperbolic module. Then $M \oplus 0$ and $0 \oplus \mathrm{Hom}(M, K)$ will be transverse Lagrangians of $H(M)$ [4].

**(1.5.4) Lemma.** *Let $L$ and $J$ be two Lagrangians of $M$. Then:*

$$(L + J)^{\#0} = L \cap J$$

*More generally, given any family of submodules $\{L\}_i$ and a submodule $X \subseteq codom(M)$, if $L_i^{\#X} = L_i$ for every $i$, then, $(\sum_i L_i)^{\#X} = \bigcap_i L_i$.*

*Proof.* Since $X$ is a submodule, for any $x \in M$, $(x, \sum_i L_i)$ and $(\sum_i L_i, X)$ are contained in $X$ if and only if $(x, L_i)$ and $(L_i, x)$ are contained in $X$ for each $i$. Thus $(\sum_i L_i)^{\#X} = (\bigcup_i L_i)^{\#X}$. By (1.1.9), we have $(\bigcup_i L_i)^{\#X} = \bigcap_i L_i^{\#X}$. Since $L_i = L_i^{\#X}$ for all $i$, we can conclude $(\bigcup_i L_i)^{\#X} = \bigcap_i L_i$ and therefore $(\sum_i L_i)^{\#X} = \bigcap_i L_i$. ■

**(1.5.5) Lemma.** *[4, Proposition 2.1.2]. Let $A$ be a ring and $M$ be an $A$-module with a unimodular symmetric (resp alternating, quadratic) bilinear function. Suppose $M$ has two transverse Lagrangians $L$ and $J$ such that $M = L + J$. Then, $M$ is isomorphic to the symmetric (resp alternating, quadratic) hyperbolic module $H(L) = L \oplus \mathrm{Hom}(L, codom(M))$ with isomorphism preserving the bilinear function.*

*Proof.* Let $N = \mathrm{codom}(M)$. Clearly, $J \cap L = \{0\}$ and $M = L + J$ implies $M \cong L \oplus J$. Let $\mathcal{B}_M : M \to \mathrm{Hom}(M, N)$ be the morphism induced by the bilinear form. By unimodularity of the bilinear form, this will be an isomorphism. Let $i : L \to M$ be the inclusion mapping. $Hom(M, N) \cong \mathrm{Hom}(L \oplus J, N) \cong \mathrm{Hom}(L, N) \oplus \mathrm{Hom}(J, N)$ and thus by unimodularity we know $i^*\mathcal{B}_M : M \to \mathrm{Hom}(L, N)$ must be surjective.

Let $\phi = (i^*\mathcal{B}_M)$. By (1.3.6.1) we know $L \subseteq ker\phi$. If $x \in J \cap ker\phi$ then $\phi(x) = \mathcal{B}_M(x)|_L = 0$. This implies $(x, L) = 0$, and thus, by definition of a Lagrangian, we have that $x \in L$. Hence $x \in L \cap J$, implying $x = 0$ since $L$ and $J$ are transverse. Thus $J \cap ker\phi = \{0\}$ and hence $ker\phi = L$. Hence $(i^*\mathcal{B}_M)_{|J} : J \to \mathrm{Hom}(L, N)$ is an isomorphism, and thus $(id_L \oplus (i^*\mathcal{B}_M)_{|J}) : L \oplus J \to L \oplus \mathrm{Hom}(L, N)$. It is straightforward to check that this preserves the bilinear function structure for the symmetric case, alternating case, and quadratic case. ■

## 1.6 Conditions for the Existence of a Transverse Lagrangian

**(1.6.1).** This subsection is dedicated to providing proofs for [4, Proposition 2.1.2] and for a result used implicitly in the proof of [4, Theorem 3.1.12]. The proof of [4, Proposition 2.1.2] presented here differs from the original in order to be more accessible to an undergraduate audience - relying only on basic linear and homological algebra.

**(1.6.2) Lemma.** *(Weak version of [4, Proposition 2.1.2]). Let $k$ be a field and $V$ be a finite-dimensional $k$-vector space with a non-degenerate bilinear form. Let $L \leq V$ be a Lagrangian of $V$. Then, the following are true (with the isomorphisms below preserving the bilinear form)*

*(i) If $V$ is symmetric and $char(k) \neq 2$, then $V \cong H_+(L)$.*

*(ii) If $V$ is quadratic, then $V \cong H_+(L)$.*

*(iii) If $V$ is alternating, then $V \cong H_-(L)$.*

*Proof.* Note that since $V$ is a non-degenerate finite-dimensional vector space, $V$ must be unimodular (2.2.5). Before we present the main argument of this proof, we need to show that for each case $(i)$, $(ii)$ and $(iii)$, $V$ has the following property:

> *$(*)$ For any subspace $W \subsetneq V$ with $W \cap L = 0$, if $x \in V$ and $x \notin W + L$, then, there is some $y \in V$ such that $(y, y) = 0$, $y \notin W + L$, and $(x - y, W + L) = 0$.*

If $(x,x)=0$ then setting $y$ to equal $x$ works. Assume $(x,x)\neq 0$. Let $\{e_i\}$ be a basis for $V$ with $e_1=x$ such that $\{e_i\}$ contains a subset which is a basis for $W$ and $L$. Let $\rho: V\to k$ be the linear transformation defined by $\rho(\sum_i a_i e_i)=a_1$. $V$ unimodular, and thus there is some $z\in V$ such that $(z,-)=\rho$. By choice of basis $\{e_i\}$ that defines $\rho$, we know $0=\rho(L)=(z,L)$. Therefore, by definition of a Lagrangian, $z\in L$.

If case $(i)$ holds, then 2 is invertible and thus $-\frac{(x,x)}{2}\in k$. Choosing $y=x-\frac{(x,x)}{2}z$ we get that $(y,y)=0$ and thus:

$$(x-y,W)=\left(x-(x-\frac{(x,x)}{2}z),\ W\right)=\frac{(x,x)}{2}(z,W)=0$$

Finally, since $y-x=-\frac{(x,x)}{2}z\in L$ we know:

$$x\notin W+L \iff x+L\notin {}^{W}\!/_{L} \iff x+(y-x+L)\notin {}^{W}\!/_{L} \iff y+L\notin {}^{W}\!/_{L} \iff y\notin W+L$$

Hence $y$ has all the properties needed, concluding case $(i)$.

If case $(ii)$ holds and $char(k)\neq 2$, then this is a special case of $(i)$ and were done. Assume $char(k)=2$. Then $(x,x)=q(2x)-q(x)-q(x)=4q(x)-2q(x)=0$ and thus setting $y=x$ works. If case $(iii)$ holds, then $(x,x)=0$ by definition of an alternating bilinear form. Hence setting $y=x$ works for case $(iii)$. Therefore, condition $(*)$ must hold for all cases given.

Let $Q\leq V$ be a subspace of the largest dimension such that $Q$ is isotropic (ie $Q\subseteq Q^{\#0}$) and $Q\cap L=0$. Such subspaces exist since 0 satisfies these two conditions, and there are finitely many values $\dim(Q)$ can take (since $\dim(V)<\infty$), and thus, largest such subspaces must exist.

Since $Q\cap L=0$, we know $V=Q+L$ implies $V\cong Q\oplus L$, with isomorphism as vector spaces. Lets show $V=Q+L$ implies $Q$ must be a Lagrangian. Indeed, for any $z\in Q+L=V$ there is some $x\in Q$ and $y\in L$ such that $z=x+y$. If $0=(z,Q)$ then $0=((x+y),Q)=(x,Q)$. $L$ is a Lagrangian, thus $(x,L)=0$, and hence $0=(x,L)+(x,Q)=(x,Q+L)=(x,V)$. By non-degeneracy, $x=0$ and hence $z=0+y\in Q$.

By the above argument, if $V=Q+L$ then $Q$ is a Lagrangian, which, by choice of $Q$, must be transverse to $L$. By (1.5.5), we need only show that $V=Q+L$ to finish the proof.

With intent to contradict, assume $x\in V$ such that $x\notin Q+L$. If $\dim({}^{Q}\!/_{x^{\#0}})=0$ then we can choose $x$ such that $(x,x)=0$ since $V$ has the property $(*)$. The subspace $Q'=Q+kx$ will have the properties $(Q',Q')=0$ and $Q'\cap L=0$. This is a contradiction by maximality of $Q$. Thus we can assume $\dim({}^{Q}\!/_{x^{\#0}})\neq 0$ for each $x$. By the rank nullity theorem applied to the linear morphism $(x,-):Q\to k$, we know ${}^{Q}\!/_{x^{\#0}}$ must be of dimension at most one, and therefore $\dim({}^{Q}\!/_{x^{\#0}})=1$.

Let $e_1\in Q$ such that $e_1\notin x^{\#0}$. Extend $e_1$ to a basis $T=\{e_i\}$ of $V$ such that $T$ contains, as subsets, a basis for $L$ and a basis for $Q$. Let $\rho: V\to k$ where $\rho:\sum_{t\in T}a_t t\mapsto -\frac{a_1}{(x,e_1)}$. By unimodularity, there is some $z\in V$ such that $(z,-)=\rho$. Additionally, $(z,L)=\rho(L)=0$ implies $z\in L$ by definition of a Lagrangian. Since $e_1\notin x^{\#0}$, we know $x^{\#0}\cap Q\subseteq (x+z)^{\#0}\cap Q$. Moreover, $z\in L$ and $x\notin Q+L$ implies $x+z+L=x+L\notin {}^{Q}\!/_{L}$ and hence $x+z\notin Q+L$. So $x+z\in V$, $x+z\notin Q+L$ and $\dim({}^{Q}\!/_{(x+z)^{\#0}})<\dim({}^{Q}\!/_{x^{\#0}})=1$. This contradicts our assumption that $\dim({}^{Q}\!/_{x^{\#0}})\neq 0$ for all $x\notin Q+L$. Therefore $V=Q+L$, which finishes the proof. ■

**(1.6.3) Proposition.** *[4, Proposition 2.1.2]. Let $A$ be a domain. Let $M$ be a projective module over $A$ of finite rank, equipped with a non-degenerate bilinear form. Let $L\leq M$ be a Lagrangian of $M$. Then, if any of the following conditions hold*

*(i) $M$ is symmetric and $char(A) \neq 2$,*

*(ii) $M$ is quadratic, or*

*(iii) $M$ is alternating,*

*then there will exist a Lagrangian $J$ transverse to $L$ such that $L + J = M$.*

*Proof.* Let $k$ be the fraction field of $A$. $A$ is a domain and thus (0) is a prime ideal. Hence by (1.3.4) and (1.3.6.3), $k \otimes L$ must be a Lagrangian in the $k$-vector space $k \otimes M$ with respect to the induced $k$-bilinear form.

Note that $char(k) = char(A)$ and the $k$-bilinear form on $k \otimes M$ induced by the $A$-bilinear form on $M$ will inherit the symmetric, quadratic, or alternating structure of the bilinear form on $M$ respectively. Thus, we can apply (1.6.2) to $k \otimes M$. Namely, there must exist a Lagrangian $J$ in $k \otimes M$ transverse to the Lagrangian $k \otimes L$ such that $J + k \otimes L = k \otimes M$. The canonical $\pi : M \to k \otimes M$ must respect the bilinear form on $M$ (ie $(x, y) = (\pi(x), \pi(y))$ ). Since $M$ is projective it must be torsion-free, and hence $\pi$ must also be injective. From these two facts about $\pi$ it follows that $I := \pi^{-1}(J)$ must be a Lagrangian. Moreover, since $(k \otimes L) \cap J = 0$ and $\pi$ injective, we know $0 = \pi^{-1}(0) = \pi^{-1}((k \otimes L) \cap J) = \pi^{-1}(k \otimes L) \cap \pi^{-1}(J) = L \cap I$. Finally, since $M = \pi^{-1}(k \otimes M) = \pi^{-1}((k \otimes L) + J) = \pi^{-1}(k \otimes L) + \pi^{-1}(J)$ we can concude that $I, J$ are transverse Lagrangians of $M$ who sum to $M$. By (1.5.5) we are finished. ■

**(1.6.3.1) Corollary.** *Let $A$ be a domain. Let $M$ be a projective module over $A$, equipped with a unimodular bilinear form. Let $L \leq M$ be a Lagrangian of $M$. Then, the following are true (with the isomorphisms below preserving the bilinear form)*

*(i) If $M$ is symmetric and $char(A) \neq 2$, then $M \cong H_+(L)$.*

*(ii) If $M$ is quadratic, then $M \cong H_+(L)$.*

*(iii) If $M$ is alternating, then $M \cong H_-(L)$.*

*Proof.* Let $k$ be the fraction field of $A$. By (1.3.6.3), $k \otimes M$ must be unimodular since $M$ is unimodular. By (2.2.5), we know $k \otimes M$ must be finite-dimensional. Thus $M$ must have finite rank. By (1.6.3), $M$ must contain a Lagrangian $J$ such that $L \cap J = 0$ and $M = L + J$. By (1.5.5), we are done. ■

**(1.6.4) Lemma.** *(Used implicitly in the proof of [4, Theorem 3.1.12]). Suppose $M$ is equipped with a symmetric or alternating function which is unimodular, and suppose $codom(M)$ is injective as an $A$-module. If $L$ and $J$ are transverse Lagrangians in $M$, then $M = L + J$.*

*Proof.* We need $M$ to be symmetric or alternating to guarantee that $x \in L$ if and only if $(x, L) = 0$, and $x \in J$ if and only if $(x, J) = 0$.

Since $J$ and $L$ are transverse (ie $L \cap J = 0$), $L + J \cong L \oplus J$ with isomorphism as modules. Since $\mathrm{codom}(M)$ is injective, the contravariant functor $\mathrm{Hom}(-, \mathrm{codom}(M))$ is exact [3, page 28]. Applying this functor to the natural injection $i : L + J \cong L \oplus J \to M$ gives a surjective mapping $i^* : \mathrm{Hom}(M, \mathrm{codom}(M)) \to \mathrm{Hom}(L \oplus J, \mathrm{codom}(M))$. Let $\rho = i^* \mathcal{B}_M$. The kernel of $\rho$ must equal $(L + J)^{\#0}$ which by (1.5.4) equals $L \cap J$ which is zero since $L$ and $J$ are transverse. There is a natural isomorphism, $\mathrm{Hom}(L \oplus J, \mathrm{codom}(M)) \cong \mathrm{Hom}(L, \mathrm{codom}(M)) \oplus \mathrm{Hom}(J, \mathrm{codom}(M))$. The inverse of $\mathrm{Hom}(L, \mathrm{codom}(M)) \oplus 0$ will be $J$, and the inverse of $0 \oplus \mathrm{Hom}(J, \mathrm{codom}(M))$ will be $L$. It follows that $L + J = \rho^{-1}(\mathrm{Hom}(L \oplus J, \mathrm{codom}(M))) = M$, which finishes the proof. ■

# 2 Lattices (Over Dedekind Domains)

**(2.0.1).** From this point forward, we will consider $A$ to be a Dedekind domain, and $K$ its field of fractions unless stated otherwise.

## 2.1 Basic Definitions

**(2.1.1) Definition.** *(Lattice).* Let $A$ be a Dedekind domain. $L$ is called an $A$-lattice if it is a finitely generated projective $A$-module equipped with a non-degenerate bilinear form that is symmetric or alternating.

**(2.1.2) Remark.** The majority of proofs that use the fact that $L$ is symmetric or alternating require only the condition that $(x, N) = (N, x)$ for any submodule $N \subseteq L$ and element $x \in L$. In particular, most proofs would hold true in the case that there is some unit $u \in A$ such that $(x, y) = u(y, x)$, for every $x$ and $y$ in $L$. For lattices over the integers, the only such bilinear forms are alternating ones and symmetric ones.

**(2.1.3) Lemma.** *Let $J$ be a submodule of an $A$-lattice $L$. If $L/J$ is a torsion module is an $A$-lattice.*

*Proof.* A hereditary ring is a ring in which every submodule of a projective module is projective. Dedekind domains are hereditary rings [3, page 134]. Every Dedekind domain is Noetherian. A module over a Noetherian ring is a Noetherian module if and only if it is finitely generated. Any submodule of a Noetherian module is Noetherian. Thus every submodule of a finitely generated module over a Dedekind domain is finitely generated. Non-degeneracy of $J$ follows from the fact that $A$ is a domain and $L/J$ is a torsion module. ■

**(2.1.4) Lemma.** *If $A$ is a principal ideal domain, then $L$ is an $A$-lattice if and only if it is a finitely generated free module equipped with a non-degenerate bilinear form. In particular, if $A$ is a Dedekind domain and $M$ an $A$-lattice, then $M_{\mathfrak{p}}$ is a finitely generated free $A_{\mathfrak{p}}$-module equipped with a non-degenerate bilinear form.*

*Proof.* The if the direction is trivial, and the only if direction follows from the fact that finitely generated projective modules over principal ideal domains are free [3, page 13]. The case of $M_{\mathfrak{p}}$ follows from (1.3.6.3 and the above argument.) ■

**(2.1.5).** The condition that for any $x, y$ in $L$ we have $(x, y) \in A$ is not always included in the definition of a lattice. When writers do not include this in the definition, lattices with this property are called *integral lattices*. Thus, we will consider every lattice used here to be integral.

**(2.1.6) Example.** *(Standard Lattice).* Consider $\mathbb{R}^n$ under the euclidean norm. Here, $\mathbb{Z}^n$ will be a lattice in $\mathbb{R}^n$. In fact, the name "lattice" comes from the shape that $\mathbb{Z}$-lattices have in $\mathbb{R}^n$.

## 2.2 Discriminant Group (resp. Module)

**(2.2.1).** The material in this subsection can be found in [8] and [4], among others.

**(2.2.2).** We will consider $A$ to be a Dedekind domain, and $K$ its fraction field.

**(2.2.3) Definition.** *(discriminant module).* Let $L$ be an $A$-lattice. Consider the module $L^{\#A} \subseteq K \otimes L$ where $L$ is viewed as a subobject of $K \otimes L$. The quotient $L^{\#A}/L$ is equipped with a bilinear function to $K/A$ given by

$$(x + L, y + L) + A = (x, y) + A$$

We call $L^{\#A}/L$, equipped with this bilinear function, the *discriminant module* (or discriminant group when $A = \mathbb{Z}$) and denote it $\mathrm{res}(L)$.

**(2.2.4) Remark.** One can think of $L^{\#A}$ as the largest subobject of $K \otimes L$ in which $L$ is a kernel (see (1.2.3)). Indeed, this is a natural and common practice: For a sub-algebra $\mathfrak{h}$ of a Lie algebra $\mathfrak{g}$, the largest subalgebra of $\mathfrak{g}$ in which $\mathfrak{h}$ is an ideal is called the *normalizer subalgebra* of $\mathfrak{h}$, and is denoted $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$. For a subgroup $H$ of a group $G$, the *normalizer* of $H$ is the largest subgroup of $G$ for which $H$ is normal. For a prime ideal $\mathfrak{p}$ of a domain $D$, the largest sub-domain of $Frac(D)$ for which $\mathfrak{p}$ generates a prime ideal, is called the *localization* of $D$ by $\mathfrak{p}$.

**(2.2.5) Lemma.** *Any finite-dimensional vector space equipped with a non-degenerate bilinear form is unimodular. Specifically, for any $A$-lattice $L$, the vector space $K \otimes L$ is unimodular.*

*Proof.* Since $L$ has a non-degenerate bilinear function to $A$, $K \otimes L$ has a bilinear function to $K \cong K \otimes A$. Let $V$ be any finite-dimensional vector space with a non-degenerate bilinear form. Since $V$ is finite-dimensional, we know $V$ is isomorphic as a vector space to its dual $\mathrm{Hom}(V, K)$. Moreover, by non-degeneracy, the image of any basis of $V$ under the canonical right dual mapping (see definition (1.1.3)) will be a linearly independent set of Cardinality equal to the dimension of $V$, which is equal to the dimension of the dual of $V$ since they are isomorphic. Hence the image of a basis of $V$ under the right dual mapping must be a basis for the dual of $V$. Via a symmetrical argument, the same can be said for the left dual mapping. Thus the dual mappings are isomorphisms, and therefore $V$ is unimodular by the definition of unimodularity (1.1.3). ■

**(2.2.6) Lemma.** *Let $L$ be an $A$-lattice that is symmetric or alternating. Then,*

*(i) $\mathrm{res}(L)$ is a torsion module.*

*(ii) $L^{\#A}$ and $\mathrm{res}(L)$ are finitely generated $A$-modules, and $L^{\#A}$ is projective as an $A$-module.*

*(iii) $(L^{\#A})^{\#A} = L$.*

*(iv) $\mathrm{res}(L)$ is unimodular.*

*Proof.* (i) Follows from the fact $L$ is generated (as an $A$-module) by an $K$-basis for $K \otimes L$.

(ii): Note that $L$ is finitely generated and if $L^{\#A}$ is finitely generated then so will $\mathrm{res}(L) = L^{\#A}/L$, and thus it is enough to show that $L^{\#A}$ is finitely generated. Since $L$ is projective and finitely generated as an $A$-module, there will be some module $Q$ such that $L \oplus Q$ is a finitely generated free $A$-module [3, page 6]. A finitely generated free $A$-module is isomorphic to its dual, and thus $\mathrm{Hom}_A(L \oplus Q, A)$ will be finitely generated and free. $\mathrm{Hom}(L \oplus Q, A) \cong \mathrm{Hom}(L, A) \oplus \mathrm{Hom}(Q, A)$, and thus, by [3, page 6], $\mathrm{Hom}(L, A)$ must be projective. Moreover, $A$ is assumed to be a Dedekind domain, and therefore a Noetherian ring, and thus any finitely generated module over $A$ will be Noetherian, and therefore finitely generated. Hence $\mathrm{Hom}(L, A)$ is finitely generated and projective. Moreover, by (2.2.5), $L^{\#A}$ is isomorphic to $\mathrm{Hom}(L, A)$ as $A$-modules. Thus $L^{\#A}$ is finitely generated and projective.

(iii): By (1.3.6.2) for any prime ideal $\mathfrak{p}$,

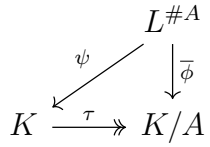
$$\left((L^{\#A})^{\#A}\right)_{\mathfrak{p}} = (L_{\mathfrak{p}}^{\#A_{\mathfrak{p}}})^{\#A_{\mathfrak{p}}}$$

We know that $L =$ if and only if $L_{\mathfrak{p}} = \left((L^{\#A})^{\#A}\right)_{\mathfrak{p}} = (L_{\mathfrak{p}}^{\#A_{\mathfrak{p}}})^{\#A_{\mathfrak{p}}}$ for each prime ideal $\mathfrak{p}$. Hence by (2.1.4), it is enough to prove this when $A$ is a principal ideal domain.

Clearly $L \subseteq (L^{\#A})^{\#A}$. Assume $A$ is a principal ideal domain and $L$ an $A$-lattice. Suppose $x \in (L^{\#A})^{\#A}$, we will show $x \in L$. $L \subseteq L^{\#A}$ and thus $(L^{\#A})^{\#A} \subseteq L^{\#A}$, which implies $x \in L^{\#A}$. By (2.1.4), $L$ is a finitely generated free module. Thus $L^{\#A}$ must be a free module canonically isomorphic to $L$. Let $\{e_i\}$ and $\{v_i\}$ be the bases for $L$ and $L^{\#A}$ such that $v_i$ is the canonical dual of $e_i$ in the basis $\{e_i\}$. Note that $\{e_i\}$ is also a basis of $K \otimes L$ and $x \in L^{\#A} \subseteq K \otimes L$, which implies $x = \sum_i b_i e_i$ for some $b_i \in K$. By definition of $v_i$ we have that $(v_i, x) = \sum_j b_j (v_i, e_j) = b_j$. Yet $v_i \in L^{\#A}$ and $(x, L^{\#A}) \subseteq A$, thus $b_j \in A$ and thus $x = \sum_i b_i e_i \in L$.

(iv): Now to show it is non-degenerate. Since $L^{\#A}$ will be alternating or symmetric, it is enough to show that the maps $(x, -) + A$ and $(y, -) + A$ are equal if and only if $x - y \in L$. Suppose the maps are equal, then $(x - y, L^{\#A}) \subseteq A$. By $(iii)$ we know that $x - y \in L$ and thus we are done.

Finally, we need to show that for any morphism of $A$-modules $\phi : \mathrm{res}(L) \to K/A$ there is an element $x \in \mathrm{res}(L)$ such that $\phi = (x, -)$. First note that the canonical $\pi : L^{\#A} \to L^{\#A}/L \cong \mathrm{res}(L)$ can be used to yield a morphism $\overline{\phi} : L^{\#A} \to K/A$ such that $\overline{\phi} = \phi\pi$. By (ii), we know $L^{\#A}$ must be projective. The canonical map $\tau : K \to K/A$ is surjective, and thus by projectivity, there is a $\psi : L^{\#A} \to K$ such that the following diagram commutes:




Yet $L$ finitely generated and non-degenerate implies that $K \otimes L$ is a non-degenerate and finite-dimensional vector space, and therefore unimodular by (2.2.5). Thus there is a $x \in K \otimes L$ such that $(x, -) = \psi$. But since $\overline{\phi}(L) = 0 + A$, we know that $(x, L) = \psi(L) \subseteq A$ and thus $x \in L^{\#A}$. Hence $(\pi(x), -) = \phi$ and thus the right dual mapping for $\mathrm{res}(L)$ is an isomorphism. By a symmetric arguement, the left dual mapping for $\mathrm{res}(L)$ is an isomorphism, and therefore $\mathrm{res}(L)$ is unimodular. ■

**(2.2.7) Lemma.** *[4, Proposition 2.1.1].*
*Let $L$ be an $A$-lattice. Then the following are true:*

*(i) $L$ is unimodular if and only if its discriminant module res$(L)$ is trivial.*

*(ii) There is a correspondence between isotropic submodules of res$(L)$ and $A$-lattices in $L^{\#A}$ that contain $L$.*

*Proof.* Clearly, unimodularity implies a trivial discriminant module, since $L^{\#A} = L$. Suppose $L$ is not unimodular. Then there is a morphism $\phi : L \to A$. By (2.2.5) there is a $x \in K \otimes L$ such that $\mathcal{B}_{K \otimes L}(x)|_L = \phi$, since $\phi$ naturally extends to $K \otimes L$. Thus $x$ will be in $L^{\#A}$ but not in $L$, which implies that $x + L$ will be nonzero in $\mathrm{res}(L)$. Therefore $L$ is unimodular if and only if its discriminant module $\mathrm{res}(L)$ is trivial.

Let $\pi : L^{\#A} \to \mathrm{res}(L)$ be the canonical projection. $\pi$ is a morphism (1.2.1), and by (1.2.7), there is a correspondence between isotropics in $\mathrm{res}(L)$ and submodules of $L^{\#0}$ that contain $L$ and whose

codomain (and therefore image under the bilinear function) must be contained in $A$. Applying (**??**) proves $(ii)$.

■

## 2.3 Discriminant of a Lattice

**(2.3.1).** The material in this section can be found in [8], or [4], among others.

**(2.3.2) Definition.** Define the *discriminant* of $L$ to be the annihilator of $\mathrm{res}(L)$. By definition of $\mathrm{res}(L)$, the discriminant of $L$ can be equivalently defined as the ideal $(L : L^{\#A})$. In the case where $A$ is a PID, then we will say that an element $d$ of $A$ is the discriminant of $L$ if it generates the annihilator of $\mathrm{res}(L)$.

**(2.3.3) Lemma.** *The discriminant of $L$ is the unit ideal if and only if $L$ is unimodular. (where the unit ideal is the ideal generated by 1)*

*Proof.* Follows from (2.2.7). ■

**(2.3.4) Lemma.** *Let $A$ be a PID, let $L$ be a finitely generated non-degenerate $A$-lattice, let $d$ be the discriminant of $L$, and let $f$ be a prime element of $A$. Then,*

$$f \text{ and } d \text{ are coprime} \iff L/fL \text{ is non-degenerate.}$$

*Proof.* First the forward direction. Since $f$ divides $d$, there is a $h \in A$ such that $f\,h = d$. Let $H = h \cdot \mathrm{res}(L) \subseteq \mathrm{res}(L)$. Note that the annihilator of $H$ must be $fA$. Since $d \notin hA$, $H \neq 0$. By definition of $H$, $H \subseteq (\frac{1}{f}L)/L$, and thus there is some non-zero $x \in L$ such that $0 \neq \frac{1}{f}x + L \in H \subseteq \mathrm{res}(L)$. By definition of res, $\frac{1}{f}x + L \in \mathrm{res}(L)$ implies $(\frac{1}{f}x, L) \subseteq A$ and thus $(x, L) \subseteq fA$. In particular, $(x, x) = 0$. Furthermore, $0 \neq \frac{1}{f}x + L$ implies $x \notin f\,L$. Thus, $x + L$ is an isotropic element of $L$.

For the backwards direction, consider the submodule $F \subseteq \mathrm{res}(L)$ defined by $f := \{y \in \mathrm{res}(L) | f\,y = 0\}$. The module $F$ is also a $A/fA$-vector space (since $fA$ is a maximal ideal). $d.F \subseteq d.\mathrm{res}(L) = 0$, and thus $(d + fA).F = 0$. Since $0 \neq \frac{x}{f} + L \in F \subseteq \mathrm{res}(L)$ we know $F$ is a non-zero $A/fA$-vector space annihilated by $d + fA$, and thus $fA = d + fA$ implying $d \in fA$. ■

## 2.4 Lagrangians (Over Dedekind Domains)

**(2.4.1).** The material here can be found in [4].

The main reason we consider Lagrangians here is that there is a one-to-one correspondence between the Lagrangians in $\mathrm{res}(L)$ and unimodular lattices in $K \otimes L$ that contain $L$.

**(2.4.2) Lemma.** *(Taken from [4]). Let $L$ be any lattice of $V$. The Lagrangians of res$(L)$ will be in one-to-one correspondence with unimodular integral lattices in $V$ containing $L$.*

*Proof.* Let $J$ be a lattice in $K \otimes L$ which contains $L$. By (1.1.9), $J^{\#A} \subseteq L^{\#A}$. Note that the canonical $\pi : L^{\#A} \to \mathrm{res}(L) = L^{\#A}/L$ is surjective, with $A = \ker \tilde{\pi}$, where $\tilde{\pi} : K \to K/A$ is as defined in (1.2.1). By (1.2.2), $\pi(J^{\#A}) = \pi(J)^{\#0}$. By (2.2.7), we know $J$ is unimodular if and only if $J^{\#A} = J$. If $J$ is unimodular, then $\pi(J) = \pi(J^{\#A}) = \pi(J)^{\#0}$, implying that $\pi(J)$ is a Lagrangian.

Let $I \subseteq \mathrm{res}(L)$ be any Lagrangian. By (2.2.7),$\pi^{-1}(I)$ is an $A$-lattice. By (1.2.2), $\pi$ and $A = \ker \tilde{\pi}$ implies that $\pi^{-1}(I^{\#0}) = \pi^{-1}(I)^{\#A}$. Since $I^{\#0} = I$, we get $\pi^{-1}(I) = \pi^{-1}(I)^{\#A}$, implying that $\pi^{-1}(I)$ is an unimodular lattice by (2.2.7). ■

# 3 Kneser p-Neighbours

**(3.0.1).** In this section, we will follow a series of proofs, observations, and definitions found in [4].

One core mathematical concept is that of closeness and proximity: mathematically rigorous ways in which we can say that two mathematical objects are "close" to each other. When we say two lattices are "*p-neighbours*" we are describing how close together these two lattices are, and we do this by looking at their intersection.

**(3.0.2).** For this section, we will always consider $A$ to be a principal ideal domain (PID) of characteristic other than 2, and $K$ to be the field of fractions of $A$.

**(3.0.3) Definition.** ($p$-Neighbour). Let $V$ be an non-degenerate $K$-vector space equipped with a bilinear form, and let $M$ be a torsion $A$-module. Then two lattices $L_1$ and $L_2$ in $V$ are called $M$-neighbours if

$$L_1/L_1 \cap L_2 \cong M \cong L_2/L_1 \cap L_2$$

with isomorphism as $A$-modules.

For an element $d \in A$ (resp. ideal $\alpha \lhd A$), we say that $L_1$ and $L_2$ are $d$-neighbours (resp. $\alpha$-neighbours) if they are neighbours with respect to the $A$-module $A/dA$ (resp. $A/\alpha$).

**(3.0.4) Lemma.** *Let $L$ and $J$ be unimodular $A$-lattices such that $L/(L \cap J)$ is a torsion module. Then $L$ and $J$ are neighbours (ie $L/(L \cap J)$-neighbours) if and only if the images of $L$ and $J$ are transverse Lagrangians in res$(L \cap J)$.*

*Proof.* First the forward direction: By (2.4.2), we know that the images of both $L$ and $J$ will be Lagrangians in $\mathrm{res}(L \cap J)$. Moreover, they must be transverse, since the image of $L \cap J$ in $\mathrm{res}(L \cap J)$ is zero.

Now for the other direction. Assume images of $L$ and $J$ are transverse Lagrangians in $\mathrm{res}(L \cap J)$. By (2.2.6), $\mathrm{res}(L \cap J)$ is unimodular. By (1.5.5), $\mathrm{res}(L \cap J)$ must be isomorphic (with isomorphism preserving bilinear function) to the hyperbolic module $L/L \cap J \oplus \mathrm{Hom}_A(L/L \cap J, K/A)$ with isomorphism taking $L/L \cap J \in \mathrm{res}(L \cap J) \mapsto L/L \cap J \oplus 0$ and $J/L \cap J \mapsto 0 \oplus \mathrm{Hom}_A(L/L \cap J, K/A)$. Since $\mathrm{res}(L \cap J)$ is unimodular, the dual mapping $\mathcal{B}_{\mathrm{res}(L \cap J)}$ must be an isomorphism. By definition of a hyperbolic module, we know $\mathcal{B}_{\mathrm{res}(L \cap J)}$ must take $L/L \cap J \oplus 0$ to $0 \oplus \mathrm{Hom}_A(L/L \cap J, K/A)$. Therefore, $J/L \cap J \cong 0 \oplus \mathrm{Hom}_A(L/L \cap J, K/A) \cong L/L \cap J \oplus 0 \cong L/L \cap J$ and thus $L/L \cap J \cong L/L \cap J$ which implies $L$ and $J$ are $L/L \cap J$-neighbours. ∎

**(3.0.5) Lemma.** *Let $A$ be a Dedekind domain. If $J$ is a $M$-neighbour of $L$ if and only if $J_\mathfrak{p}$ is a $M_\mathfrak{p}$-neighbour (resp $\mathfrak{p}A_\mathfrak{p}$-neighbour) of $L_\mathfrak{p}$ as $A_\mathfrak{p}$-lattices for every prime ideal $\mathfrak{p}$ in $A$.*

*Proof.* From (1.3.6.2) it follows that $\mathrm{res}(L)_\mathfrak{p} \cong \mathrm{res}(L_\mathfrak{p})$ with isomorphism natural and preserving the bilinear function. By (3.0.4), $J$ is a $M$-neighbour of $L$ if and only if their images in $\mathrm{res}(L)$ are transverse Lagrangians which sum to all of $\mathrm{res}(L \cap J)$. Applying (1.3.6.3) finishes the proof. ∎

## 3.1 p-Neighbours and Isotropic Elements of $\mathbb{P}(L/pL)$

**(3.1.1).** The material in this subsection is well known to specialists, and we follow a series of proofs for the specific case of $A = \mathbb{Z}$ found in [4].

**(3.1.2).** The most important tool we will use to find p-neighbours is the following correspondence (found in [4]), which we will prove in this section. This correspondence can be visualized by the following diagram:

$$\begin{array}{ccc} \left(\begin{smallmatrix}\text{Isotropic Elements of}\\ \mathbb{P}(L/pL)\end{smallmatrix}\right) & \xrightarrow{\ orbits\ } & \left(\begin{smallmatrix}\text{Isotropic Elements of}\\ Aut(L)\backslash\mathbb{P}\big(L/pL\big)\end{smallmatrix}\right) \\ \Big(A\frac{1}{p}\,v+v^{\#pA}\Big)\Big\downarrow & & \Big\downarrow\Big(A\frac{1}{p}\,v+v^{\#pA}\Big)_{/\cong} \\ p\text{-Neighbours of } L & \xrightarrow[\text{iso. classes}]{} & \text{Genus of } L \end{array}$$

Let us clarify what it means for an element of $\mathbb{P}(L/pL)$ to be isotropic. $L/pL$ is an $A/pA$ vector space and naturally inherits an $(A/pA)$-bilinear form from the bilinear form on $L$. In this way, we say an element of $\mathbb{P}(L/pL)$ is isotropic if it is isotropic as a subset of $L/pL$. When looking at the arrow

$$\left(\begin{smallmatrix}\text{Isotropic Elements of}\\ \mathbb{P}(L/pL)\end{smallmatrix}\right) \xrightarrow[\Big(A\frac{1}{p}\,v+v^{\#pA}\Big)]{} p\text{-Neighbours of } L$$

We are referring to the process (in 3.1.6) of taking an appropriate representative $v \in L$ of an isotropic element of $\mathbb{P}(L/pL)$, and using $v$ to create a lattice $A\frac{1}{p}\,v + v^{\#pA}$. We will prove that the resulting lattice is independent of the representative $v$ chosen in $\mathbb{P}(L/pL)$, and we will show that this lattice will be a p-neighbour of $L$.

**(3.1.3) Lemma.** *Suppose $p$ does not divide the discriminant of $L$. Let $v \in L$ be an element such that $v \notin pL$ and $(v,v) \equiv 0 \ (mod\ p^2)$. Then the lattice defined by $L_v := A\frac{1}{p}\,v + v^{\#pA}$ is a p-neighbour of $L$.*

*Proof.* Since $v \notin pL$ we know $\frac{1}{p}v \notin L$ and thus $L_v \cap L = Av + v^{\#pA}$. Thus $L_v/(L_v \cap L) = (A\frac{1}{p}v)/(Av) \cong A/pA$. We need only show that $L/(L_v \cap L) \cong A/pA$. Note that $pL \subseteq v^{\#pA} \subseteq Av + v^{\#pA} = L_v \cap L$, and $L/pL$ naturally inherits a bilinear form, thus ${}^{L}\!/_{(L_v \cap L)}$ is isomorphic to ${}^{(L/pL)}\!/_{(v+pL)^{\#0}}$ as an $A$-module (and equivalently, as an $A/pA$-module).

$A$ is a PID, hence every prime ideal is maximal and thus $A/pA$ is a field. Therefore, it is enough to show that ${}^{(L/pL)}\!/_{(v+pL)^{\#0}}$ is a 1 dimensional $A/pA$ vector space, since this will imply that ${}^{L}\!/_{(L_v \cap L)}$ is isomorphic as a $A$-module to $A/pA$. We know ${}^{(L/pL)}\!/_{(v+pL)^{\#0}}$ is not trivial by (2.3.4). Let $x, y \in L/pL$ such that $x, y \notin (v+pL)^{\#0}$. Then $(x,(v+pL))$ and $(y,(v+pL))$ must be units in $A/pA$. Thus there is an $a \in (A/pA)^*$ such that $a(x,(v+pL)) = (y,(v+pL))$, implying $(ax-y,(v+pL)) = 0$ and therefore $ax - y \in (v+pL)^{\#0}$. Hence ${}^{L}\!/_{(L_v \cap L)}$ is a one-dimensional $(A/pA)$-vector space, which was what was needed. ■

**(3.1.4) Lemma.** *Let $L_v := A\frac{1}{p}\,v + v^{\#pA}$ and let $L_w := A\frac{1}{p}\,w + w^{\#pA}$ be two lattices in $K \otimes L$. Then $L_v = L_w$ if an only if $v + pL$ and $w + pL$ are equal in $\mathbb{P}(L/pL)$.*

*Proof.* Suppose $v + pL$ and $w + pL$ are equal. $A$ is a PID and thus $A/pA$ is a field, hence there is some $a \in A$, not divisible by $p$, such that $a.(v+pL) = (a/pA)\cdot(v+pL) = (w+pL)$. Hence $av - w \in pL$. Since $a$ is not divisible by $p$, and $A$ is a PID, we know that $(av)^{\#pA} = v^{\#pA}$ and

hence $w^{\#pA} = v^{\#pA}$. Note that the ideal generated by $p$ is a maximal ideal in $A$, and since $a$ is not divisible by $p$, $a$ is not in this ideal. Thus the ideal generated by both $p$ and $a$ must contain 1, and thus there is some $f, g \in A$ such that $1 = fp + ga$. Now we have $A_p^{\frac{1}{}} w = A_p^{\frac{1}{}} (aw) \subseteq A_p^{\frac{1}{}} (ga)v = A_p^{\frac{1}{}} (1 - fp)v = A_p^{\frac{1}{}} v + Af\, v$. Yet $(v, v) \in p^2 A$, hence $v \in v^{\#pA}$ and thus $Af\, v \subseteq v^{\#pA}$. Therefore $L_w = A_p^{\frac{1}{}} w + w^{\#pA} = A_p^{\frac{1}{}} w + v^{\#pA} \subseteq A_p^{\frac{1}{}} v + Af\, v + v^{\#pA} = A_p^{\frac{1}{}} v + v^{\#pA} = L_v$ and thus $L_w \subseteq L_v$. By symmetry, $L_v \subseteq L_w$, and hence $L_v = L_w$.

Now for the opposite direction; Suppose $L_v = L_w$. Then $pL_v = pL_w$, which after substitution becomes $Av + p(v^{\#pA}) = Aw + p(w^{\#pA})$. Yet both $p(v^{\#pA})$ and $p(w^{\#pA})$ are subsets of $pL$. Adding $pL$ to both sides of the equality gives $Av + pL = Aw + pL$ and thus $v + pL \in (A/pA)(w + pL)$. Therefore, $pL_v = pL_w$ implies that $v + pL$ and $w + pL$ are equal in $\mathbb{P}(L/pL)$. ■

**(3.1.5) Lemma.** *Suppose $p$ does not divide the descriminant of $L$. Let $J$ be an $A$-lattice in $K \otimes L$ that is a $p$-neighbour of $L$. Then there exists an vector $v \in L$ such that $J = A_p^{\frac{1}{}} v + v^{\#pA}$.*

*Proof.* Since $J/(L \cap J)$ is isomorphic to $A/pA$ as $A$-modules, we know that for every $w \in J$ we have $pw \in L$, and we know that $J/(L \cap J)$ is generated by a single element, say $x \in J$. $(x, J) \subseteq A$ implies $(px, J \cap L) \subseteq pA$ and thus $L \cap J \subseteq (px)^{\#pA}$. Now consider the element $v \in L$ such that $v = px$. Consider $v^{\#pA} \subseteq L$, we know that $L \cap J \subseteq v^{\#pA}$ and thus ${}^{v^{\#pA}}\!/_{L \cap J} \subseteq {}^{L}\!/_{L \cap J}$. We know that ${}^{L}\!/_{L \cap J} \cong A/pA$ as a $(A/pA)$-vector space, and thus the subspace ${}^{v^{\#pA}}\!/_{L \cap J}$ must be 0 or the entire space. yet if $v^{\#pA} = L$ then $x + L \in \mathrm{res}(L)$ and $px + L = 0 + L$, a contradiction under the assumption that no non-zero elements of $\mathrm{res}(L)$ are annihilated by $p$. Thus ${}^{v^{\#pA}}\!/_{L \cap J}$ must be 0, implying $v^{\#pA} = L \cap J$, and therefore $J = Ax + v^{\#pA} = A_p^{\frac{1}{}} v + v^{\#pA}$. ■

**(3.1.6) Proposition.** *Let $L$ be a lattice with symmetric bilinear form. Let $p$ be a prime element of $A$ , not equal to zero, that does not divide 2 or the discriminant of $L$. Then, there is a one-to-one correspondence between isotropic elements in $\mathbb{P}(L/pL)$ and $p$-neighbours of $L$ in $K \otimes L$. (isotropic elements of $\mathbb{P}(L/pL)$ as described in (3.1.2))*

*Proof.* First lets prove that for any isotropic element $[y] \in \mathbb{P}(L/pL)$, there is an element $v \in L$ such that $v + pL$ is in the project class $[y]$ and generates a p-neighbour as in (3.1.3). Let $x \in L$ such that $x + pL$ is in the projective class $[y]$. Since $[y]$ is isotropic, we know $(x + pL, x + pL) = 0 \in A/pA$ and thus $p$ must divide $(x, x)$. Let $f \in A$ such that $(x, x) = pf$. If $p$ divides $f$ then $p^2$ divides $(x, x)$ and we can apply (3.1.3) and be done. Assume not. Let $\{e_i\}$ be a basis for $L$. We will show that there is an $i$ such that $p$ does not divide $(x, e_i)$ via contradiction. If $p$ divides $(x, e_i)$ for all $i$, then $(x, L) \subseteq pA$ since $\{e_I\}$ is a basis for $L$. Thus $(\frac{1}{p}x, L) \subseteq A$ and hence $\frac{1}{p}x + L \in \mathrm{res}(L)$. Yet $x + pL \neq 0 + pL$ implies $x \notin pL$ and thus $\frac{1}{p}x \notin L$. Therefore $\frac{1}{p}x + L$ is an non-zero element of $\mathrm{res}(L)$ which is annihilated by $p$, a contradiction. Thus there is an $i$ such that $p$ does not divide $(x, e_i)$.

The characteristic of $A/pA$ is not equal to 2, since $p$ does not divide 2 and $A$ is of characteristic other than 2 (see 3.0.2). Thus, $2 + pA$ is invertible in $A/pA$. Both $(x, e_i)$ and $f$ are not divisible by $p$, there must be an element $a \in A/pA$ such that $(2 + pA)(a + pA)(x, e_i) = -(f + pA)$, since $A/pA$ is a field. Hence:

$$(x + pae_i,\, x + pae_i) + p^2 A = (x, x) + 2ap(x, e_i) + p^2 a^2 (e_i, e_i) + p^2 A$$

$$= pf + p(2a(x, e_i) + pA) + p^2 A = pf + p(-f + pA) + p^2 A$$

$$\implies (x + pae_i,\, x + pae_i) + p^2 A = p^2 A \implies (x + pae_i,\, x + pae_i) \equiv 0 \ (mod\ p^2)$$

Let $v = x + pae_i$, and thus $v + pLx + pae_i + pL = x + pL$ is in the projective class $[y]$ by choice of $x$. By (3.1.3), we can conclude that for every isotropic element $[y] \in \mathbb{P}(L/pL)$ there is some $v$ such that $v + pL$ is in the projective class $[y]$, and $A\frac{1}{p}\,v + v^{\#pA}$ is a $p$-neighbour of $L$.

By (3.1.4) we know that this $p$-neighbour is the same no matter the choice of such a $v$. Hence there is a well defined function from the isotropic elements of $\mathbb{P}(L/pL)$ to the set of neighbours of $L$ in $K \otimes L$, defined by $[y] \mapsto L_{[y]} := A\frac{1}{p}\,v + v^{\#pA}$, (where $v$ is as described above). By (3.1.4), we can conclude that this function is injective.

We need only show that this function $[y] \mapsto L_{[y]}$ is subjective. Let $J$ be any $p$-neighbour of $L$ in $K \otimes L$. By (3.1.5), there must be a $v \in L$ such that $J = A\frac{1}{p}\,v + v^{\#pA}$. Since $J \not\subseteq L$, we know $\frac{1}{p}v \notin L$. $J$ is an $A$-lattice, and thus $(\frac{1}{p}v, \frac{1}{p}v) \in A$, implying $(v, v) \in p^2A \subseteq pA$. Thus $v + pL$ is an isotropic element of $L/pL$, and moreover for any $a, b \in A$, $(av, bv) = ab(v, v) \in pA$. Hence the projective class containing $v + pL$ will be isotropic as described in (3.1.2). This implies that $L_{[v+pL]} = A\frac{1}{p}\,v + v^{\#pA} = J$, and thus the function $[y] \mapsto L_{[y]}$ is surjective. ■

**(3.1.7) Lemma.** *Let $Aut(L)$ be the automorphism group of $L$ (the group of automorphisms on $L$ that preserve the bilinear form). For any $p$-neighbour $L_v = \frac{1}{p}\mathbb{Z}\,v + v^{\#p\mathbb{Z}}$ and any automorphism $\phi \in Aut(L)$, the lattice $L_{\phi(v)}$ is isomorphic to $L_v$ with the isomorphism preserving bilinear form.*

*Proof.* Note thate $Aut(L) \subseteq Aut(K \otimes L)$ by extending any $f \in Aut(L)$ such that $f(\frac{a}{b} \otimes x) = \frac{a}{b} \otimes f(x)$. Now, $L_v = \frac{1}{p}\mathbb{Z}\,v + v^{\#p\mathbb{Z}}$ under the automorphism $\phi \in Aut(L) \subseteq Aut(K \otimes L)$ gives the lattice $\phi(\frac{1}{p}\mathbb{Z}\,v + v^{\#p\mathbb{Z}}) = \frac{1}{p}\mathbb{Z}\,\phi(v) + \phi(v)^{\#p\mathbb{Z}} = L_{\phi(v)}$. Thus $\phi$ is an isomorphism between $L_v$ and $L_{\phi(v)}$ that preserves the bilinear form. ■

**(3.1.8).** For any element $\phi \in Aut(L)$, $\phi$ must fix $aL$ for any $a \in A$ (since $\phi(aL) = a\,\phi(L) = aL$). Thus, there is a natural mapping $Aut(L) \to Aut(L/pL)$. Combined with the fact that any automorphism also acts on the projective space, we can conclude that there is a natural action of $Aut(L)$ on $\mathbb{P}(L/pL)$.

**(3.1.9) Lemma.** *Let $p$ be a prime element of $A$ that does not divide 2 or the determinant of $L$. Then, each element of $[v] \in Aut(L) \setminus \mathbb{P}(L/pL)$ will determine a isomorphism class corresponding to a $p$-neighbour of $L$. ie any element of the orbit of any $v \in \mathbb{P}(L/pL)$ will generate a $p$-neighbour isomorphic to that generated by $v$ (as in (3.1.6)).*

*Proof.* By discussion (3.1.8) we know the action of $Aut(L)$ on $\mathbb{P}(L/pL)$ by action on the representatives as elements of $L$ is well defined. Applying (3.1.7) to the correspondence seen in (3.1.6) concludes the proof. ■

## 3.2 Kneser's Connected Genus Theorem

**(3.2.1).** This subsection follows of [4, Theorem 3.1.12]. In this section, we will only consider the ring $\mathbb{Z}$. We will call a $\mathbb{Z}$-lattice *even* if $(x, x)$ is an even number for every $x$.

Using his expertise on algebraic groups, Kneser [11] proved that given any prime integer p and an even unimodular lattice of rank n, the connected component containing this lattice in the graph corresponding to the "p-neighbour" relation will contain (and only contain) every lattice (up to isomorphism) in the genus of said lattice. Combined with the fact that any lattice can only have finitely many p-neighbours and one can compute these neighbours with relative ease, Kneser's result gives a useful method for the classification of even unimodular lattices.

**(3.2.2) Definition.** *(Genus).* Let $L$ be an even $\mathbb{Z}$-lattice. Then, the *genus* of $L$ is the set of all $\mathbb{Z}$-lattices $J$ satisfying the following:

(i) $L \otimes \mathbb{Z}_p$ is isomorphic to $J \otimes \mathbb{Z}_p$ as bilinear formed $\mathbb{Z}_p$-modules.

(ii) $L \otimes \mathbb{R}$ is isomorphic to $J \otimes \mathbb{R}$ as bilinear formed $\mathbb{R}$-modules.

**(3.2.3) Lemma.** *[4, Theorem 2.2.8]. Let $L$ and $J$ be even $\mathbb{Z}$-lattices. Let $p$ be a prime that does not divide the discriminant of $L$. Then, the following are equivalent:*

*(i) $L \otimes \mathbb{R}$ is isomorphic to $J \otimes \mathbb{R}$ as bilinear formed $\mathbb{R}$-modules.*

*(ii) $L \otimes \mathbb{Z}[\frac{1}{p}]$ is isomorphic to $J \otimes \mathbb{Z}[\frac{1}{p}]$ as bilinear formed $\mathbb{Z}[\frac{1}{p}]$-modules.*

*Proof.* This proof can be found in [4, Theorem 2.2.8]. It is omitted here due to the fact it requires results on approximation for algebraic groups. ■

**(3.2.4) Lemma.** *Let $A$ be a Dedekind domain and $K$ its field of fractions. Let $L$ and $J$ be unimodular $A$-lattices in $L \otimes K$. $J$ is a $\mathfrak{p}$-neighbour of $L$ if and only if $res(L \cap J)$ is isomorphic to the hyperbolic module $H(A/\mathfrak{p}A)$, with isomorphism preserving bilinear form.*

*Proof.* Applying (3.0.4), we get $J$ is a $p$-neighbour of $L$ if and only if $L$ and $J$ are transverse Lagrangians in $\mathrm{res}(L \cap J)$. Moreover, by (2.2.6), we know $\mathrm{res}(L \cap J)$ is unimodular. Thus, by (1.5.5), the proof is finished. ■

**(3.2.5) Lemma.** *(Partial Statement of of [4, Theorem 3.1.12]). Let $A$ be a principal ideal domain and $K$ its field of fractions. Let $L$ and $H$ be two $A$-lattices in $L \otimes K$ that have quadratic forms. Let $pA$ be a prime ideal that does not divide the discriminant of $L$ or $H$. Then, if the ideal $(L \cap H : L + H)$ is a power of $pA$, then $L$ and $H$ are connected by the $p$-neighbour relation.*

*Proof.* neighbour localization lemma Well (2.4.2) implies $L/L \cap H$ and $H/L \cap H$ will be Lagrangians of $\mathrm{res}(L \cap H) = (L \cap H)^{\#A}/(L \cap H)$. For ease of reference, let $\bar{H} := H/(L \cap H)$ and $\bar{L} := L/(L \cap H)$. By (1.6.4), we know that $(L \cap H)^{\#A} = L + H$, and thus $\mathrm{res}(L \cap H) = \bar{H} + \bar{L}$

$(L \cap H : L + H)$ will be a power of $\mathfrak{p}$, and $(L + H)/L \cap H$ is isomorphic to $\mathrm{res}(L \cap H)$. So, by the fundamental theorem of finitely generated modules over principal ideal domains, there must be a chain $0 = L_0 \subseteq ... \subseteq L_n = L/(L \cap H)$ of submodules in $res(L \cap H)$ such that $L_i/L_{i-1} \cong A/\mathfrak{p}$. We will proceed via induction on $n$. Note that if $n = 1$ we are done. Assume the theorem for $n - 1$. Let $H_i := L_i^{\#0} \cap \big(H/(L \cap H)\big)$, which yields a chain $H/(L \cap H) = H_0 \supseteq H_2 \supseteq ... \supseteq H_n = 0$

Lets show $L_i + H_i$ is a Lagrangian for each $i$. Let $x \in (L_i + H_i)^{\#0})$. Then since $\mathrm{res}(L \cap H) = \bar{L} + \bar{H}$, we know $x = y + z$ for $y \in \bar{L}$ and $z \in \bar{H}$. $(x, L_i + H_i) = 0$ implies $0 = (x, L_i) = (z, L_i)$ and hence $x \in L_i^{\#0} \cap \bar{H} = H_i$. Also $0 = (x, H_i) = (y, H_i)$, and thus $y \in H_i^{\#0} \cap \bar{L} = (L_i^{\#0} \cap \bar{H})^{\#0} \cap \bar{L} = L_i$, and thus $y \in L_i$. Hence $x = y + z \in L_i + H_i$ and therefore $L_i + H_i$ is a Lagrangian in res$L \cap H$.

By (2.4.2), we have that the inverse image of $L_i + H_i$ under the canonical map $L^{\#A} \to \mathrm{res}(L)$ is a unimodular lattice, call it $K_i$. The intersection of $K_i$ with $L$ is the inverse of $L_i$ under the canonical $(L \cap H)^{\#A} \to \mathrm{res}(L \cap H)$. Since this inverse of $L_i$ will contain $L \cap H$, the quotient $L/(K_i \cap L)$ will be a torsion module because $L/(H \cap L)$ is a torsion module. By (2.4.2), we know that the images of $K_i$ and $L$ under the morphism $K_i + L \to \mathrm{res}(K_i \cap L)$ will be lagrangians. Now, we can apply (3.0.4) to get that $K_i$ is a $L/(K_i \cap L)$-neighbour of $L$. Since $L/(K_{n-1} \cap L) \cong \bar{L}/(\bar{L} \cap (L_{n-1} + H_{n-1})) \cong \bar{L}/L_{n-1} \cong A/\mathfrak{p}$, we get that $K_{n-1}$ is a $p$-neighbour of $L$.

Thus, applying the induction assumption to $\mathrm{res}(K_{n-1} \cap H)$ shows us that $H$ is connected to $K_{n-1}$ via the $p$-neighbour relation. Since $K_{n-1}$ is a $p$-neighbour of $L$, we can conclude that $H$ and $L$ are connected via the $p$-neighbour relation. ■

**(3.2.6) Theorem.** *(M. Kneser). [4, Theorem 3.1.12]. Suppose $L$ is an even $\mathbb{Z}$-lattice whose discriminant is not divisible by $p$. Then the isomorphism classes in the genus of $L$ is fully connected by the $p$-neighbour relation.*

*Proof.* Let $H$ be in the genus of $L$. Therefore by (3.2.3), $L \otimes A[\frac{1}{p}] \cong H \otimes A[\frac{1}{p}]$. Specifically, we may and will consider $H$ as $H \subseteq L \otimes A[\frac{1}{p}] \subseteq L \otimes K$. In particular, the ideal $(L \cap H : H + L)$ is a power of $p$. By (3.2.5) we are done. ■

# 4 Algorithms

**(4.0.1).** For this section, every lattice will be assumed to be a $\mathbb{Z}$-lattice inside the vector space $\mathbb{R}^n$, where $\mathbb{R}^n$ is equipped with a quadratic non-degenerate bilinear form for some finite $n$. In other words, a lattice here will be a finitely generated free abelian group with a quadratic bilinear form to $\mathbb{Z}$ with the property that $\mathcal{B}_L$ is injective.

**(4.0.2) Lemma.** *By the equivalence given by* (3.1.5)*, any $p$-neighbour $L_2$ of a lattice $L_1$ (inside $\mathbb{Q} \otimes L_1$) can be generated by a (not necessarily unique) vector $v \in L_1$ by the process*

$$v \mapsto \frac{1}{p}\mathbb{Z}\, v + v^{\#p\mathbb{Z}} = L_2.$$

*For any vector $v \in L_1$, $\frac{1}{p}\mathbb{Z}\, v + v^{\#p\mathbb{Z}}$ is a $p$-neighbour of $L_1$ if and only if the following hold:*

*(i)* $(v, v)\ mod\ p^2 = 0$ *if* $p \neq 2$.

*(ii)* $(v, L) \not\subseteq p\mathbb{Z}$

*Proof.* First the forward direction. $(i)$ follows from the fact that $L_2 = \frac{1}{p}\mathbb{Z}\, v + v^{\#p\mathbb{Z}}$ being integral implies $(\frac{1}{p}v, \frac{1}{p}v) \in \mathbb{Z}$ and thus $(v, v)\ mod\, p^2 = 0$. $(ii)$ follows from the fact that if $(v, L_1) \subseteq pL_1$ then $v^{\#p\mathbb{Z}} = L_1$ and hence $L_1 \subseteq L_2$, contradicting the fact that $[L_1 : L_1 \cap L_2] = p$.

Now for the " $\Longleftarrow$ " direction. By $(ii)$ we know that $L_2 \cap L_1 = (\frac{1}{p}\mathbb{Z}\, v + v^{\#p\mathbb{Z}}) \cap L_1 = \mathbb{Z}\, v + v^{\#p\mathbb{Z}}$ and thus $[L_2 : L_2 \cap L_1] = \left|{}^{(\frac{1}{p}\mathbb{Z}\, v)}\!/_{\mathbb{Z}\, v}\right| = p$. By $(i)$, $v \in v^{\#p\mathbb{Z}}$ and thus $L_1 \cap L_2 = \mathbb{Z}\, v + v^{\#p\mathbb{Z}} = v^{\#p\mathbb{Z}}$. Therefore $[L_1 : L_1 \cap L_2] = \left|{}^{L_1}\!/_{v^{\#p\mathbb{Z}}}\right| = p$. $v^{\#p\mathbb{Z}}$ contains $pL_1$ and hence is a $\mathbb{F}_p$-vector space, thus we need only show it is of dimension 1. Suppose $w, u \notin v^{\#p\mathbb{Z}}$. Then $(v, w)$ will be invertible mod p. Thus there is a $c \in \mathbb{Z}$ such that $c(v, w)\ mod\, p = (v, u)\ mod\, p$. This implies $(v, cw - u)\ mod\, p = 0$ and therefore $cw - u \in v^{\#p\mathbb{Z}}$. Hence two vectors in $L_1/v^{\#p\mathbb{Z}}$ cannot be linearly independent and hence $L_1/v^{\#p\mathbb{Z}} = L_1/L_1 \cap L_2$ has dimension 1. ■

**(4.0.3).** So our objective is to do two things efficiently: Find all such vectors $v$, and from such a vector $v$ construct its corresponding $p$-neighbour $L_v$.

## 4.1 From a Vector to a Neighbour

**(4.1.1).** Given such a vector $v \in L$ (as in (4.0.2)) we must construct the corresponding $p$-neighbour lattice which we will denote $L_v$. By (3.1.5) we know that this lattice will be precicely

$$L_v := \frac{1}{p}\mathbb{Z}v + v^{\#p\mathbb{Z}} = \frac{1}{p}\mathbb{Z}v + \{x \in L \,;\, (v,x)\ mod\ p = 0\}$$

Notice that we need only find a generating set for $v^{\#p} \subseteq L$ since appending $\frac{1}{p}v$ to this set will give a generating set for $L_v$. Since $L$ and $L_v$ are integral lattices, we know that $pL \subseteq v^{\#p\mathbb{Z}}$ and $pL_v \subseteq v^{\#p\mathbb{Z}}$. If we can find a set of vectors $\{w_i\} \subseteq L$ which generate $v^{\#p}/pL \cong (v^{\#p}/pL)$ when mapped to $L/pL$, then we can find a generating set for $L_v$ by taking the union of $\{w_i\}$ with $\{p \cdot g_i\}$, where $\{g_i\}$ is a generating set for $L$. Thus, it suffices to find an $\mathbb{F}_p$ basis for $v^{\#p}/pL \cong \mathbb{F}_p \otimes (v^{\#p})$. Note that $pL \subseteq v^{\#p\mathbb{Z}}$ and hence

$$p = [L : L \cap L_p] = [L : v^{\#p\mathbb{Z}}] = [{}^{L}\!/_{pL} : {}^{v^{\#p\mathbb{Z}}}\!/_{pL}] = \left|{}^{({}^{L}\!/_{pL})}\!/_{({}^{v^{\#p\mathbb{Z}}}\!/_{pL})}\right| = \left|{}^{(L/pL)}\!/_{(v^{\#p\mathbb{Z}}/pL)}\right|$$

This implies that $p = \left|{}^{(L/pL)}\!/_{(v^{\#p\mathbb{Z}}/pL)}\right|$ and thus the dimension of ${}^{(L/pL)}\!/_{(v^{\#p\mathbb{Z}}/pL)}$ as a $\mathbb{F}_p$-vector space must be one. By the rank nullity theorem,

$$\dim\left({}^{(L/pL)}\!/_{(v^{\#p\mathbb{Z}}/pL)}\right) = \dim(L/pL) - \dim(v^{\#p\mathbb{Z}}/pL)$$

Since $L$ is a free module of rank $n$, $\dim(L/pL) = n$ and thus

$$\dim(v^{\#p\mathbb{Z}}/pL) = n - 1$$

Any $n-1$ linearly independent vectors in $v^{\#p\mathbb{Z}}/pL$ will be a basis of $v^{\#p\mathbb{Z}}/pL$. Therefore it suffices to find $n-1$ vectors $\{w_i\}_{i=1}^{n-1}$ such that $w_i \in v^{\#p\mathbb{Z}}$ and $\{w_i + pL\}_{i=1}^{n-1}$ is linearly independent. Since lifting vectors from $L/pL \cong L/pL$ to $L$ is computationally negligible, we need only focus on finding a basis of $v^{\#p\mathbb{Z}}/pL$.

**(4.1.2)Algorithm.** Let $v \in L$ be a vector which generates a neighbour as described in (4.0.2). Equip $L/pL$ with bilinear form in $\mathbb{F}_p$ inherited from $L$. Let $L$ and $v$ be the inputs. Define this algorithm as follows:

```
B := {}
while B contains less than rank(L) − 1 elements do
    if (w, v + pL) = 0 and w is not in the span of B then
        B := B union {w}
    end
end
return B
```

## 4.2 Finding and Counting All p-Neighbours

**(4.2.1).** First lets clarify the direction and motivation behind this discussion and resulting algorithm. Our main goal is to look at how many p-neighbours of a lattice $L$ are isomorphic to a given lattice $J$ in the genus of $L$. Since every p-neighbour of $L$ will be isomorphic to some member of the

genus of $L$ (because both lattices live in the tensor product of the field of fractions with their intersection, apply (3.2.3) to get they are in the same genus), it is enough to first find every p-neighbour of $L$ (which will be a finite set by (3.1.5) along side the fact that the discriminant group of their non-zero intersection with be finite) and then, for each member of the genus, we count the number of lattices in this set of p-neighbours isomorphic to it.

We will restrict our focus to the case where $p$ is an odd prime that does not divide the discriminant of the lattice $L$. From (3.1) we can draw a one-to-one correspondence between $p$-neighbours of $L$ in $\mathbb{Q} \otimes L$ (up to equality, not isomorphism) and isotropic lines of $L/pL$; ie points in $\mathbb{P}(L/pL)$ which are isotropic when viewed as an equivalence class in (and subset of) $L/pL$. For any element of the automorphism group $\phi \in Aut(L)$ (automorphism preserving bilinear form structure), the projective line containing $\phi(v)$ ($\phi$ is well defined on $L/pL$ since $\phi(pL) = pL$) generates a $p$-neighbour isomorphic to the one generated by $v$. It may be convenient to reference the following diagram from (3.1.2):

$$\begin{array}{ccc} p\text{-Neighbours of } L & \twoheadrightarrow & \text{Lattices in the Genus of } L \\ \downarrow & & \downarrow \\ \text{Isotropic Lines in } \mathbb{P}(L/pL) & \twoheadrightarrow & \text{Isotropic Lines in } Aut(L)\backslash\mathbb{P}\big(L/pL\big) \end{array}$$

**(4.2.2).** Recall that we are concerned with the number of $p$-neighbours of $L$ isotropic to each element of the genus of $L$. (3.1.6) and (3.1.9) imply that, for each element $J$ in the genus of $L$, we need only sum the size (as subsets of $\mathbb{P}(L/pL)$) of isotropic elements of $Aut(L)\backslash\mathbb{P}(L/pL)$ which generate $p$-neighbours isomorphic to $J$. Since $Aut(L)$ acts on $\mathbb{P}(L/pL)$, for any representative $x$ of an element $[x] \in Aut(L)\backslash\mathbb{P}(L/pL)$ we can use the orbit-stabilizer theorem on $x$ to calculate the size of the subset $[x] \subseteq \mathbb{P}(L/pL)$. Thus it is enough to find a representative of each isotropic element of $Aut(L)\backslash\mathbb{P}(L/pL)$, then apply algorithm (4.1.2) to find the lattice in the genus of $L$ that each element of said isotropic member of $Aut(L)\backslash\mathbb{P}(L/pL)$ generates (keeping track of multiplicity). Therefore, our objective is to find a set containing exactly one representative of each isotropic member of $Aut(L)\backslash\mathbb{P}(L/pL)$.

**(4.2.3).** For computational reasons, it is useful to first consider $Aut(L)\backslash(L/pL)$, which is a "subpartition" of $Aut(L)\backslash\mathbb{P}(L/pL)$, when both are viewed as partitions in $L/pL$. This is because, given $v \in \mathbb{P}(L/pL)$, multiple scalar multiples of $v$ can be in the $Aut(L)$-orbit of $v$. If we are able to find a set containing exactly one representative of each isotropic member of $Aut(L)\backslash(L/pL)$, it is easy to convert this to a set containing exactly one representative of each isotropic member of $Aut(L)\backslash\mathbb{P}(L/pL)$.

**(4.2.4).** Suppose we have some $v \in L/pL$ and we know that $N$ is the size of the $Aut(L)$-orbit of $v$ in $L/pL$, we need a computationally efficient way to infer, with high probability, whether a given isotropic element $w \in L/pL$ lies in the orbit of $v$. We will do this by taking two random subsets of $Aut(L)$ and use them to make a subset of the orbits of $v$ and $w$ respectively. We will generate these subsets of $Aut(L)$ by choosing, with replacement, $\lceil c \cdot \sqrt{N} \rceil$ random elements of $Aut(L)$, where $c$ is a constant. The larger the value of $c$ the more accurate and expensive the computation becomes.

**(4.2.5)Algorithm.** Let $v \in L/pL$, let $N$ is the size of the $Aut(L)$-orbit of $v$ in $L/pL$, and let $c$ be a positive real number. Let $w \in L/pL$ be an isotropic element.

```
w_list := { Random(G).w    for i from 1 to c√N }
v_list := { Random(G).v    for i from 1 to c√N }
for x in w_list do
    if x in v_list then
        return True
        (End algorithm)
    end
end
return False
```

**(4.2.6) Remark.** Note that a false positive in the process (4.2.4) will often result in the sum of the size of orbits found not equaling the actual size of the number of isotropic elements of $L/pL$ (for which there exists a known and convenient formula). Code to implement a contingency plan, in this case, is easy but can avoid having to redo computations. Moreover, when the list mentioned in (4.2.3) has been found, it is useful to use the process (4.2.4) to compare representatives with orbits the same size. This will lower the chances of inaccuracies.

**(4.2.7).** Suppose we implement the following algorithm:

```
RepList := [ ]
while the sum of each n for ⟨v, n⟩ in RepList is less than NumberOfIsotropics do
    w := Random(L/pL)
    if w isn't zero and (w, w) isn't zero then
        if (4.2.5) applied to v, N, and w returns false for each pair ⟨v, N⟩ in RepList then
            M := |Aut(L)| / |Stabalizer(v)|
            TempList := [⟨w, M⟩]
            for i from 2 to p − 1 do
                if (4.2.5) applied to iw, M, and v returns false for each ⟨v, N⟩ in TempList
                 then
                    append the pair ⟨iw, M⟩ to TempList
                end
            end
            append each element of TempList to RepList
        end
    end
end
```

**Algorithm:** Inefficient Version

(NOTE: it is more computationally efficient to replace $Aut(L)$ with $Aut(L)$ coerced into its action in $L/pL$.)
Using the above algorithm, we run into a bottle neck when almost all orbits have been found. The smaller orbits are more like to be found towards the end of the random search. This makes the bottleneck worse.

**(4.2.8).** The discussion (4.2.7) leads us to ask the following question: *is there a computationally efficient way we can decrease the expected time taken to find the smaller orbits?* The answer to this is yes. By the orbit-stabilizer theorem, we know that for any element $v$ of $L$, the size of the stabilizer of $v$ will be inversely proportional to the size of the orbit of $v$. Moreover if there is a subgroup $H \leq Aut(L)$ that stabilizes $v$, then the size of the orbit of $v$ will be less than or equal to

$\frac{|Aut(L)|}{|H|}$.

If we find a new isotropic orbit with representative $w \in L/pL$. We will need to calculate its stabilizer to find its orbit size: let $S$ be the stabilizer of $w$. Any vector $v \in L/pL$ that is stabilized by $S$ will have an orbit size less than the size of the orbit of $w$. Since $S$ is a finitely generated group that acts linearly on the vector space $L/pL$, we need only compute the intersection of the eigenvalues associated to one for each generator of $S$ (a computationally affordable process).

**(4.2.9) Algorithm.**

```
G := Aut(L) coerced into its action on L/pL.
ParentStabilizerOrbitSize := Null
StabilizedVectors := [ ]
RepList := [ ]
while the sum of each n for ⟨v, n⟩ in RepList is less than NumberOfIsotropics do
    if StabilizedVectors is empty then
        w := Random(L/pL)
        if w isn't zero and (w, w) isn't zero then
            if (4.2.5) applied to v, N, and w returns false for each pair ⟨v, N⟩ in RepList
             then
                S := Stabilizer of v in G
                M := |G|/|S|
                TempList := [⟨w, M⟩]
                for i from 2 to p − 1 do
                    if (4.2.5) applied to iw, M, and v returns false for each ⟨v, N⟩ in
                     TempList then
                        append the pair ⟨iw, M⟩ to TempList
                    end
                end
                Append each element of TempList to RepList
                ParentStabilizerOrbitSize := M
                StabilizedVectors := [ x ∈ L/pL | x is in the intersection of the eigenspaces of
                 1 for each generator of S, x has first entry one, and x is isotropic ]
            end
        end
    else
        w := the first entry of StabilizedVectors
        Remove w from StabilizedVectors
        if (4.2.5) applied to v, N, and w returns false for each pair ⟨v, N⟩ in RepList such
         that N ≤ParentStabilizerOrbitSize then
            S := Stabilizer of v in G
            M := |G|/|S|
            TempList := [⟨w, M⟩]
            for i from 2 to p − 1 do
                if (4.2.5) applied to iw, M, and v returns false for each ⟨v, N⟩ in TempList
                 then
                    Append the pair ⟨iw, M⟩ to TempList
                end
            end
            Append each element of TempList to RepList
        end
    end
end
```

**(4.2.10).** Algorithm (4.2.9) can be made quicker by making a set LikelyOrbits, which contains both the members $\langle v, M\rangle$ of RepList were the orbit of $v$ has been found to contain a member of StabilizedVectors, and the members of RepList who were found using StabilizedVectors; as more members of StabilizedVectors are found, it is most probable that a new isotropic vector $w$ from StabilizedVectors will be in the orbit of some member of this set "LikelyOrbits". Thus, one can save time by checking the orbit overlap of $w$ with members of LikelyOrbits before checking the rest of RepList.

# 5 Modular Forms

**(5.0.1).** The content of this section can be found in [15], [4], [5], [12], [13], and [**?**], among others.

## 5.1 Fourier Series and Poisson Summation

**(5.1.1).** Here, we will let $V$ denote a finite-dimensional $\mathbb{R}$-vector space, and we will let $\Lambda$ be finitely generated subgroup of the additive group of $V$. We will also denote $\Lambda^{\#}$ to be $\Lambda^{\#\mathbb{Z}}$.

**(5.1.2).** The content of this section can be found in [15], [5], [**?**], as well as any standard textbooks in real analysis.

**(5.1.3) Definition.** (Periodic Functions). We say a function with domain $V$ is $\Lambda$-periodic iff for any $x \in V$ and $m \in \Lambda$ we have $f(x+m) = f(x)$. Moreover, we can equivalently define $f$ to be a function on $V/\Lambda$.

**(5.1.4) Definition.** ($\mathcal{L}^1$ Functions). Define $\mathcal{L}^1(V/\Lambda)$ to be the set of functions $V \to \mathbb{C}$ that are $\Lambda$-periodic and whose integral

$$\int_{V/L} f(x)\,\overline{f(x)}\,dx$$

is well defined and finite.

**(5.1.5) Lemma.** *If $\{g_i\}_{i=1}^n$ are the generators of $\Lambda$. Let $H$ be the subspace of $V$ orthogonal to $span_{\mathbb{R}}(\Lambda)$. We define $\langle -,-\rangle$ as*

$$\langle f, g\rangle \;=\; \begin{cases} \int_0^{g_1}\int_0^{g_2}\cdots\int_0^{g_n} f(x)\,\overline{g(x)}\,dx_n\ldots dx_2\,dx_1 & \text{if } H \text{ is zero} \\ \int_H \int_0^{g_1}\int_0^{g_2}\cdots\int_0^{g_n} f(x)\,\overline{g(x)}\,dx_n\ldots dx_2\,dx_1\,dH & \text{otherwise} \end{cases}$$

*Proof.* This follows linearly from the definition of $\Lambda$ and $V$ given in (5.1.1). ■

**(5.1.6) Lemma.** *Suppose the a generating set of $\Lambda$ is also a basis of $V$. Let $\{e_v\}_{v\in\Lambda^{\#}}$ be a set of functions from $V$ to $\mathbb{C}$ given by $e_v(t) = e^{-2\pi i(v,t)}$. Then this set of functions is an linearly independent and orthogonal subset of $\mathcal{L}^1(V/\Lambda)$. Moreover, the $\mathbb{R}$-span of $\{e_v\}_{v\in\Lambda^{\#}}$ is a dense subspace of $\mathcal{L}^1(V/\Lambda)$.*

*Proof.* Suppose that $V$ is of dimension $n$. By the definition of $\Lambda$ and $V$ given in (5.1.1) and the inner product given in (5.1.5), we can define a linear automorphism on $V$ that takes $\Lambda \subseteq V$ to

the case $\mathbb{Z}^n \subseteq \mathbb{R}^n$, with the resulting inner product on $\mathscr{L}^1(\mathbb{R}^n/\mathbb{Z}^n)$ being a scalar multiple of the inner product on $\mathscr{L}^1(V/\Lambda)$. Note that when we restrict our attention to the case $\mathbb{Z}^n \subseteq \mathbb{R}^n$, we arrive at the standard definition of the Fourier series, in which case the statement of the lemma is a well-known result. All the properties mentioned in the statement of this lemma are left unchanged under such a linear automorphism. The proof follows from this fact.

■

**(5.1.7) Definition.** (Fourier Transform on $\mathscr{L}^1(V/\Lambda)$). Let $f \in \mathscr{L}^1(V/\Lambda)$. Define the Fourier transform $\mathfrak{F}_L : f \mapsto \hat{f}$ to be

$$\hat{f}(t) := \mathfrak{F}_\Lambda\big(f\big)(t) = \int_{V/\Lambda} e^{-2\pi i x t}\, f(x)\, dx$$

**(5.1.8) Lemma.** *Let $|L|$ denote the determinant of $\Lambda$. Let $f$ be a continuous function in $\mathscr{L}^1(V/L)$. Then,*

$$f(x) = \frac{1}{|\Lambda|} \sum_{m \in \Lambda^\#} \hat{f}(m)\, e^{2\pi i (m,x)}$$

*Proof.* By applying a linear change of basis as seen in the proof of (5.1.6), we can apply the standard results on the convergence of the Fourier series for smooth functions. ■

**(5.1.9) Theorem.** *(Poisson Summation). Let $|L\Lambda|$ denote the determinant of $\Lambda$. Suppose $f \in \mathscr{L}^1(V)$ such that $\sum_{n\in\Lambda} f(x+n)$ converges to a continuous function, then,*

$$\sum_{n \in \Lambda} f(x+n) = \frac{1}{|\Lambda|} \sum_{m \in \Lambda^\#} \hat{f}(m)\, e^{2\pi i (m,x)}$$

*Where $\hat{f}$ is the $\mathscr{L}^1(V)$ fourier transform of $f$.*

*Proof.* $\sum_{n\in\Lambda} f(x+n)$ will be $\Lambda$-periodic and converges to a continuous function in $\mathscr{L}^1(V/\Lambda)$. Thus we can apply (5.1.8) to get:

$$f(x) = \frac{1}{|\Lambda|} \sum_{m \in \Lambda^\#} \Big( \int_{V/L} \sum_{n \in \Lambda} f(t+n)\, e_m(-t)\, dt \Big)\, e^{2\pi i (m,x)}$$

Let $\{g_i\}_{i=1}^n$ be the generators of $\Lambda$. Let $a_i$ be the (compact) line connecting 0 and $g_i$, and define $I = \prod_{i=1}^n a_i \subseteq V$. Note that the family of compact sets $\{n + I\}_{n\in\Lambda}$ has union equal to $V$, and intersection of measure zero. Also, for any $\Lambda$ period function $g$, we know $\int\limits_{V/\Lambda} g(t)\ dt = \int\limits_{I} g(t)\ dt = \int\limits_{(n+I)} g(t)\ dt$ for any $n \in \Lambda$. Both $\sum_{n\in\Lambda} f(x+n)$ and $e_v$ are $\Lambda$-periodic, thus

$$\frac{1}{|\Lambda|} \sum_{m \in \Lambda^\#} \Big( \int_{V/L} \sum_{n \in \Lambda} f(t+n)\, e_m(-t)\, dt \Big)\, e^{2\pi i (m,x)}$$

$$= \frac{1}{|\Lambda|} \sum_{m \in \Lambda^\#} \Big( \int_{I} \sum_{n \in \Lambda} f(t+n)\, e_m(-t-n)\, dt \Big)\, e^{2\pi i (m,x)}$$

$$= \frac{1}{|\Lambda|} \sum_{m \in \Lambda^\#} \Big( \sum_{n \in \Lambda} \int_{(-n+I)} f(t)\, e_m(-t)\, dt \Big)\, e^{2\pi i (m,x)} = \frac{1}{|\Lambda|} \sum_{m \in \Lambda^\#} \hat{f}(m)\, e^{2\pi i (m,x)}$$

And therefore $\sum_{n\in\Lambda} f(x+n) = \frac{1}{|\Lambda|} \sum_{m\in\Lambda^\#} \hat{f}(m)\, e^{2\pi i (m,x)}$. ■

**(5.1.9.1) Corollary.** *(Standard Poisson Summation). Suppose $\sum_{n\in\mathbb{Z}} f(x+n)$ converges, then,*

$$\sum_{n\in\mathbb{Z}} f(x+n) = \sum_{m\in\mathbb{Z}} \hat{f}(m)\, e^{2\pi i m x}$$

*Proof.* Follows from (5.1.9) applied to the case where $\Lambda = \mathbb{Z}$ and $V = \mathbb{R}$. ■

## 5.2 Group Actions on the Complex Half-Plane

**(5.2.1) Definition.** ($GL_2^+(\mathbb{R})$ Action on the Complex Half Plane). Let $\mathfrak{H} = \{x \in \mathbb{C} \mid \mathrm{Im}(x) > 0\}$ be the complex half plane. Define the action of $GL_2^+(\mathbb{R})$ on $\mathfrak{H}$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} . x = \frac{ax+b}{cx+d}$$

for any $x \in \mathfrak{H}$ and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbb{R})$.

**(5.2.2) Lemma.** *The action of $GL_2^+(\mathbb{R})$ on $\mathfrak{H}$ is a group action.*

*Proof.* This action is well defined in the sense that the denominator will never be zero. The image of this action will always be in $\mathfrak{H}$. A direct calculation yields $(\alpha\beta).x = \alpha(\beta.x)$. The rest follows from the fact identity acts trivially. ■

**(5.2.3) Definition.** (Congruence Groups, and the Principle Congruence Group). Let $n \in \mathbb{N}$. The principle congruence group of level $n$, denoted $\Gamma(n)$, is defined to be the subgroup of $SL_2(\mathbb{Z})$ given by

$$\Gamma(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod n \right\}$$

Moreover, we call a subgroup $H \leq SL_2(\mathbb{Z})$ a congruence group of level $n$ iff $\Gamma(n) \subseteq H$.

**(5.2.4) Definition.** Let $n \in \mathbb{Z}^+$. we define $\Gamma_0(n)$ and $\Gamma_1(n)$ as follows:

$$\Gamma_0(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \mod n \right\}$$

$$\Gamma_1(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \mod n \right\}$$

**(5.2.5) Lemma.** *Let $n \in \mathbb{N}$. The following are true:*

*(i)* $\Gamma(n)$ *is the kernel of the canonical morphism $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})$.*

*(ii) There is an one-to-one correspondence between congruence subgroups of level $n$ and subgroups of $SL_2(\mathbb{Z}/n\mathbb{Z})$.*

*(iii)* $\Gamma_1(n)$ *is the kernel of the morphism $\Gamma_0(n) \to \mathbb{Z}/n\mathbb{Z}$ given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d$.*

*(iv)* $\Gamma_0(n)/\Gamma_1(n) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^*$

*Proof.* The proof follows from the definitions (5.2.3) and (5.2.4), as well as the isomorphism theorems for groups. ■

## 5.3 Introduction to Modular Functions

**(5.3.1) Definition.** Let $\phi = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbb{R})$. Define *automorphic factor* to be the function $j : GL_2^+(\mathbb{R}) \times \mathfrak{H} \to \mathbb{C}$ given by $j(\phi, x) = cx + d$. For $\phi$ , define the weight $k$ operator, denoted $|_\phi$, to be the endomorphism of vector space of functions $f : \mathfrak{H} \to \mathbb{C}$ with

$$f|_\phi(x) = \big(\det(\phi)\big)^{k-1}\, j(\phi, x)^{-k}\, f\big(\phi(x)\big) \qquad \text{for all } x \in \mathfrak{H}$$

**(5.3.2) Remark.** Although this fact will not be used here, the (and its natural generalizations) are a special case of a class of functions called *crossed homomorphisms*. A function $f$ from a group $G$ to a $G$-module $H$ is called a crossed homomorphism if, for every $x$ and $y$ in $G$, $f(xy) = x.f(y) + f(x)$.

**(5.3.3) Definition.** Let $H$ be a subgroup of $SL_2(\mathbb{Z})$ of finite index. We say that a holomorphic function $f$ is weakly modular of weight $n$ over $H$ iff $f|_\phi = f$ for every $\phi \in H$.

We say $f$ is a modular form of weight $n$ over $H$ iff $f$ is weakly modular of weight $n$ over $H$, $f$ is holomorphic on $\mathfrak{H}$, and $f$ is holomorphic as $z \to i\infty$. The set of all modular forms of weight $n$ over $H$ is denoted $M_n(H)$.

**(5.3.4) Theorem.** *Let $H$ be a subgroup of $SL_2(\mathbb{Z})$ of finite index. Then $\dim_{\mathbb{C}}\big(M_n(H)\big)$ is finite.*

*Proof.* The proof of this is standard, and only a rough sketch will be provided here. A rigorous proof that includes an explicit formula for $\dim_{\mathbb{C}}\big(M_n(SL_2(\mathbb{Z}))\big)$ can be found at ("a course in Arithmetic" by Serre, page 88, Theorem 4 and Corollary 1) or at ("An Introduction to Modular Forms" by Cohen, page 12, Corollary 3.6).

The quotient $\mathfrak{H}/SL_2(\mathbb{Z})$ union the point $i\infty$ can be given the structure of a compact Riemann surface in a way which extends the natural Riemann surface structure on $\mathfrak{H}/SL_2(\mathbb{Z})$ (ie the compactification of $\mathfrak{H}/SL_2(\mathbb{Z})$). A standard compactness argument can be used to prove that, for any finite index subgroup $H \leq SL_2(\mathbb{Z})$, $\mathfrak{H}/H$ will be a Riemann surface when the point $i\infty$ is added. Let $g \in M_k(H)$ be non-zero. For any $f \in M_k(H)$, $f$ will be holomorphic on $\mathfrak{H}$ and at $i\infty$. Moreover,

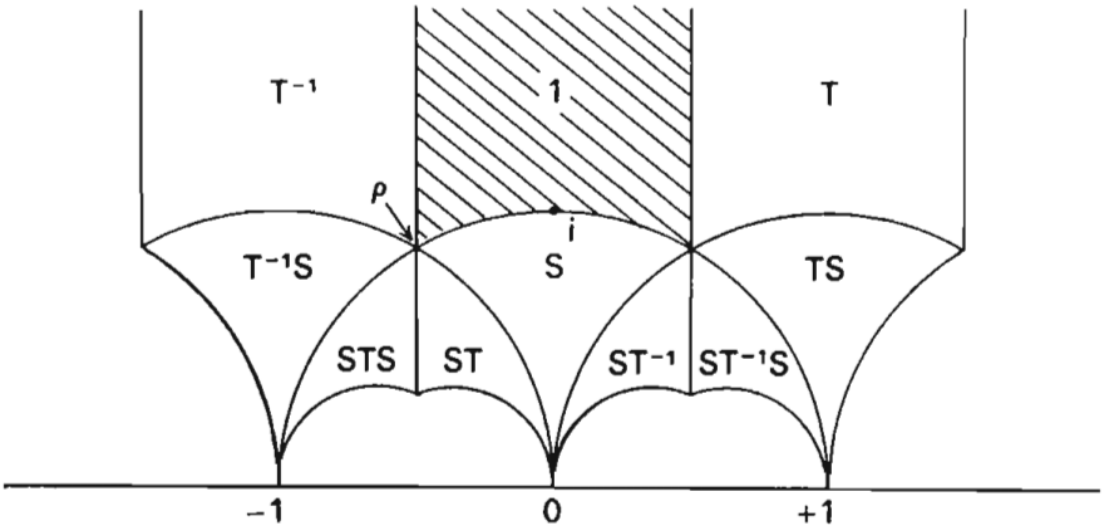



Figure 1: Found in "*A Course in Arithmetic*" by Serre; the action of $SL_2(\mathbb{Z})$ on $\mathfrak{H}$.

$\frac{f}{g}(x) = \frac{f}{g}|_\phi(x) = \frac{f}{g}(\phi.x)$, thus $\frac{f}{g}$ is defined and holomorphic on $\mathfrak{H}/H \cup \{i\infty\}$. Hence we have an

injection of vector spaces taking $M_k(H)$ into the space of meromorphic functions on the compact Riemann surface $\mathfrak{H}/H \cup \{0\}$ with divisor greater than the divisor of $\frac{1}{g}$ - ie with poles only at the zeros of $g$, and with order less than the order of the zero of $g$. By the Riemann-Roch theorem [16, Theorem 6.1], this space must be finite-dimensional, thus $M_k(H)$ must be finite-dimensional. ■

**(5.3.5) Examples.** (Examples of Modular Forms)

(i) (Eisenstein Series). Define the *Eisenstein series* to be the modular form

$$G_k(z) = \sum_{(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(xz+y)^k}$$

(ii) (Theta Function). Let $L$ be an arbitrary $\mathbb{Z}$-lattice. Define the *theta function* of $L$ to be

$$\Theta_L(z) = \sum_{x\in L} e^{\pi i(x,x)\, z}$$

(iii) (Ramanujan Tau Function). The *Ramanujan tau function* is a modular form of weight 12 defined by

$$\Delta(z) = q\prod_{m\geq 1}(1-q^m)^{24} = \sum_{n\geq 1}\tau(n)q^n \qquad \text{where } q = e^{2\pi iz}$$

## 5.4 Modular Forms with a Character

**(5.4.1).** The content of this section can be found in [15], [4], [5], [12], [13], and [**?**], among others.

**(5.4.2) Definition.** (Character). A character $\phi$ on a group $G$ is a group homomorphism $\phi : G \to \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of units on $\mathbb{C}$.

**(5.4.3) Definition.** (Dirichlet Character). A *Dirichlet character* of modulus $k$ is a function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying

(i) $\chi(mn) = \chi(m)\chi(n)$

(ii) $\chi(n+k) = \chi(n)$

(iii) $\chi(n) = 0 \iff gcd(k,\, n) \neq 1$

ie a Dirichlet character of modulus $k$ can be thought of as a monoid homomorphism $\chi : (\mathbb{Z}/k\mathbb{Z},\, \cdot\,) \to (\mathbb{C},\, \cdot\,)$ whose image is a group union zero (ie an absorbing element).

**(5.4.4) Lemma.** *There is an isomorphism between the (group of) characters on $(\mathbb{Z}/n\mathbb{Z})^*$ and the (group of) Dirichlet characters of modulus $k$. This isomorphism takes a character $\phi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ to the Dirichlet character $\overline{\phi}$ given by:*

$$\overline{\phi}(x) = \begin{cases} \phi(x + N\mathbb{Z}) & \text{if } gcd(x, N) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* $\overline{\phi}$ is a Dirichet character. Suppose $\chi$ is a Dirichlet character of modulus $k$, then when we view $\chi$ as a monoid homomorphism from the monoid $(\mathbb{Z}/n\mathbb{Z},\, \cdot\,)$ to the monoid $(\mathbb{C},\, \cdot\,)$, the inverse of 0 under $\chi$ is the set of all non-units of $\mathbb{Z}/n\mathbb{Z}$. Thus, $\chi$ can be defined simply by its values of the units of $(\mathbb{Z}/n\mathbb{Z},\, \cdot\,)$, which is the group $(Z/n\mathbb{Z})^*$. This serves as a inverse to the function $\phi \mapsto \overline{\phi}$ (since monoid homomorphisms send units to units). Therefore the function $\phi \mapsto \overline{\phi}$ must be bijective. ■

**(5.4.5) Lemma.** *Let $G_1 \subseteq G_0$ be subgroups of $SL_2(\mathbb{Z})$ of finite index such that $G_1$ is normal in $G_0$. Let $f$ be a modular form for $G_1$ of weight $k$. Then, for any $\beta \in G_0$, $f|_\beta(z)$ is a modular form for $G_1$ of weight $k$. Moreover, if $\beta' \in \beta G_1$, then $f|_\beta = f|_{\beta'}$. Thus there is an action of $G_0/G_1$ on the space $M_k(G_1)$.*

*Proof.* Let $\alpha \in G_1$, since $G_1$ is normal in $G_0$, we have that there exists $\alpha' \in G_1$ such that $\beta\alpha = \alpha'\beta$. Thus $f_\beta|_\alpha = f|_{\beta\alpha} = f|_{\alpha'\beta} = f|_{\alpha'}|_\beta = f|_\beta$. Every other condition for $f|_\beta$ to be a modular form is trivial.

Let $\beta' \in \beta G_1$, then since $G_1 \lhd G_0$, there is some $\alpha \in G_1$ such that $\beta' = \alpha\beta$. Thus $f|_{\beta'} = f|_{\alpha\beta} = f|_\alpha|_\beta = f|_\beta$. This completes the proof. ∎

**(5.4.6) Definition.** (Modular Forms of Nebentypus). Let $k, N \in \mathbb{N}$, and let $\chi$ be a Dirichlet character of modulus $N$. We say a function $f : \mathfrak{H} \to \mathbb{C}$ is a modular form of weight $k$, level $N$, and Nebentypus $\chi$, if $f$ is a modular form of weight $k$ for $\Gamma_1(N) \subseteq \Gamma_0(N)$, and:

$$f|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} = \chi(d)\, f \qquad \text{for all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$$

$M_k(\Gamma_0(N), \chi))$ denotes the $\mathbb{C}$-vector space of modular form of weight $k$, level $N$, and Nebentypus $\chi$.

**(5.4.7) Lemma.** *Let $G_1 \subseteq G_0$ be finite index subgroups of $SL_2(\mathbb{Z})$ such that $G_1$ is normal in $G_0$. Then,*

$$M_k(G_1) \cong \oplus_\lambda M_k(G_0, \lambda)$$

*Where $\lambda$ is taken over the set of characters on $G_0/G_1$, and the isomorphism is the natural one: $\oplus_\lambda f_\lambda \mapsto \sum_\lambda f_\lambda$.*

*Proof.* (proof is given by "*Lectures on Modular Forms and Hecke Operators*" by Kenneth Ribet and William Stein, January 12, 2017, Lemma 8.2.4).

By (5.4.5), $G_0/G_1$ acts on $M_k(G_1)$ via $g.f = f|_{\phi(g)}$. Let $n$ be the order of $G_0/G_1$. Since $G_1$ and $G_0$ have finite index in $SL_2(\mathbb{Z})$, $G_0/G_1$ must be finite, and thus $n$ must be finite. Let $g \in G_0/G_1$ be arbitrary. The operator $(g.-) : M_k(G_1) \to M_k(G_1)$ is $\mathbb{C}$-linear, and moreover $g^n = id$. Thus the characteristic polynomial of the linear transformation $(g.-)$ must divide $x^n - 1$, which is square free. Hence $(g.-)$ is diagonalizable, $M_k(G_1)$ can be decomposed as a direct sum of eigenspaces. Moreover, (5.3.4) implies that $M_k(G_1)$ must be finite-dimensional, and hence for each $g \in G_0/G_1$, $M_k(G_1) = \bigoplus_{i=1}^n V_{g,\lambda_{g,i}}$ for some set of $\lambda_{g,i} \in \mathbb{C}$.

Let $V_{g,\lambda}$ be the $\lambda$ eigenspace for $g$. We will now show that for any $h \in G_0/G_1$, the linear transformation $(h.-)$ will fix the space $V_{g,\lambda}$. This is because for any $f \in V_{g,\lambda}$,

$$\lambda(f|_{\phi(h)}) = (\lambda f)|_{\phi(h)} = (f|_{\phi(g)})|_{\phi(h)} = f|_{\phi(gh)} = f|_{\phi(hg)} = (f|_{\phi(h)})|_{\phi(g)}$$

which implies that for any $f \in V_{g,\lambda}$, $(f|_{\phi(h)})|_{\phi(g)} = \lambda(f|_{\phi(h)})$ and thus $(h.-)$ fixes the space $V_{g,\lambda}$. By an inductive application of the above argument, for every function (not necessarily a morphism) $\lambda : G_0/G_1 \to \mathbb{C}$, the morphism $(h.-)$ must fix $V_\lambda := \bigcap_{g \in G_0/G_1} V_{g,\lambda(g)}$. Thus we can decompose $M_k(G_1)$ into a direct sum $\bigoplus_{\lambda : G_0/G_1 \to \mathbb{C}^*} V_\lambda$ for which each component is a fixed subspace of the $\lambda(g)$ eigenspace for the transformation $(g, -)$ for each $g \in G_0/G_1$.

If $V_\lambda$ is non-empty, then let $f \in V_\lambda$ such that $f(x) \neq 0$ for some $x \in \mathfrak{H}$. We can write $\lambda$ as a morphism $n \mapsto \frac{f|_{\phi(n)}}{f}(x)$. Then we have $\lambda(nm) = \frac{f|_{\phi(nm)}}{f}(x) = \frac{(f|_{\phi(n)})|_{\phi(m)}}{f}(x) = \frac{\lambda(n) f|_{\phi(m)}}{f}(x) =$

$\lambda(n)\lambda(m)$. Since $\lambda(1) = \frac{f}{f}(x) = 1$ we can conclude that $\lambda : G_0/G_1 \to \mathbb{C}^*$ is a morphism and thus a character. By definition of $M_k(G_0, \lambda)$, we know $V_\lambda = M_k(G_0, \lambda)$. Therefore, $M_k(G_1)$ is canonically isomorphic to $\bigoplus_\lambda M_k(G_0, \lambda)$, where $\lambda$ is taken over the set of characters. ■

**(5.4.7.1) Corollary.** *[14, Lemma 8.2.4].*

$$M_k(\Gamma_1(N)) \cong \bigoplus_\chi M_k(\Gamma_0(N), \chi)$$

*Where $\chi$ is taken over the set of Dirichlet characters of modulus $N$, and the isomorphism is the natural one: $\bigoplus_\chi f_\chi \mapsto \sum_\chi f_\chi$.*

*Proof.* By (5.2.5), we have the natural isomorphism $\phi : (\mathbb{Z}/N\mathbb{Z})^* \to \Gamma_0(N)/\Gamma_1(N)$. By (5.4.4), any character $\lambda$ for the group $\Gamma_0(N)/\Gamma_1(N)$ (which is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$) is a Dirichlet character. Therefore, $M_k(\Gamma_1(N))$ is canonically isomorphic to $\bigoplus_\lambda M_k(\Gamma_0(N), \lambda)$, where $\lambda$ is taken over the set of Dirichlet characters. ■

# 6 Observations and Conjectured Formulas

**(6.0.1) Definition.** *($T_p$ Operator).* Suppose $G$ is a genus of $\mathbb{Z}$-lattices (2.1.1) contained in some $\mathbb{Q}$-vector space $V$, and let $\{L_i\}$ be the (finite) set of representatives of isomorphism class of $G$ (unique up to isomorphism). Let $\mathbb{Z}[\{L_i\}]$ be the free $\mathbb{Z}$-module (ie free abelian group) generated by a basis labeled by $\{L_i\}$. Let $p \in Z$ be a prime number and consider the morphism $T_p : \mathbb{Z}[\{L_i\}] \to \mathbb{Z}[\{L_i\}]$ defined by

$$T_p(L) = \sum_J [J]$$

Where $J$ is taken over all $p$-neighbours of $L$, and $[J]$ is equal to the representative of $\{L_i\}$ that $J$ is isomorphic to.

**(6.0.2) Lemma.** *[10, Page 153]. Let $L$ be an even non-degenerate $\mathbb{Z}$-lattice of even rank. Let $r$ be the rank of $L$ and let $D$ be the determinant of the Gram matrix of $L$. Let $c(p)$ be the number of isotropics in $\mathbb{P}(L/pL)$, where $p$ does not divide the discriminant of $L$. Then*

$$c(p) = \left(\frac{D\,(-1)^{(\frac{r}{2})}}{p}\right) p^{(\frac{r}{2}-1)} + \sum_{i=0}^{r-2} p^i$$

## 6.1 Results and Inspiration from Chenevier and Lannes

The following theorem is a result that Chenevier and Lannes prove, but also states are well known to specialists. They also prove a similar statement for the Niemeier lattices.

**(6.1.1) [4, Theorem A].** *Consider the unique genus of symmetric unimodular even lattices of rank 16 (containing lattices $E_8 \oplus E_8$ and $E_{16}$, ). the matrix of $T_p$ is*

$$T_p = c_{16}(p)\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + (1 + p + p^2 + p^3)\frac{1 + p^{11} - \tau(p)}{691}\begin{bmatrix}-405 & 286\\ 405 & -286\end{bmatrix}$$

*Where $q\prod_{m\geq 1}(1-q^m)^{24} = \sum_{n\geq 1}\tau(n)q^n$ is the Fourier series expansion of a modular form called Ramanujan's function, and $c(p)$ is the number of isotropic lines in $L_i/pL_i$, which will be the same for all $L_i$ in the genus.*

## 6.2 Conjectured Formulas For $T_p$

**(6.2.1).** We will look at a select few conjectures obtained as a result of an ongoing collaboration between Adam Logan, Colin Ingalls, Dan Fretwell, and Spencer Secord. The project has yielded many more conjectures similar in format to the ones seen here, including in connection to lattices of larger even rank.

In this section we will look at conjectured connections between even non-degenerate lattices of rank 4 whose genus has two isomorphism classes. For primes $p$ that do not divide the discriminant of the lattices in the genus, we will present $T_p$ of the form

$$T_p \;=\; c(p)\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + \frac{w(p)}{|Aut(L_1)| + |Aut(L_2)|}\begin{bmatrix}-|Aut(L_1)| & |Aut(L_2)|\\ |Aut(L_1)| & -|Aut(L_2)|\end{bmatrix}$$

Where $c(p)$ will be the number of isotropic lines in $L_i/pL_i$, which will be the same for each $L_i$, and $w(p)$ is a function, which will be connected to the $p^{th}$ coefficients of a specific modular form of weight 3 in genera containing lattices of rank 4.

**(6.2.2).** First, we guessed a space of modular forms with a specific weight and character. Since the space of modular forms for a specific character and weight is finite-dimensional (5.3.4), we made sure we had computed more values for $T_p$ (where $p$ is an odd prime not dividing the discriminant) than the dimension of the corresponding space of modular forms with specified character and weight. This is to make sure that the formulas are indeed likely to be correct. After the formulas were formulated, more $T_p$ matrices were computed to verify confirm the guess.

**(6.2.3) Conjecture.** *(a3⊕6). Let $L_1$ be the lattice given by the Gram matrix*

$$Gram(L_1) := \begin{bmatrix}2 & -1 & 0 & 0\\ -1 & 2 & -1 & 0\\ 0 & -1 & 2 & 0\\ 0 & 0 & 0 & 6\end{bmatrix}$$

*The genus containing $L_1$ has one other lattice $L_2$. Both lattices in this genus have discriminant 24. Let $c(p)$ be the number of isotropic elements of $\mathbb{P}(L/pL)$.*

*Then, there is a modular form of weight 3 with character the Kronecker character over $-7$ (which is equivalent to the Kronecker character over the negitive of the determinant of the lattice), and with fourier expansion $\sum_{n=0}^{\infty} a_n q^n$. The Matrix which counts p-neighbours (ie the matrix of the Hecke operator) for the genus containing $L_1$ is the following matrix:*

$$T_p \;=\; c(p)\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + \frac{w(p)}{|Aut(L_1)| + |Aut(L_2)|}\begin{bmatrix}-|Aut(L_1)| & |Aut(L_2)|\\ |Aut(L_2)| & -|Aut(L_1)|\end{bmatrix}$$

*Where*

$$w(p) \;=\; c(p) \;-\; a_p + p\,(1 + \left(\frac{-3}{p}\right))$$

*In magma [2], the modular form $\sum_{n=0}^{\infty} a_n q^n$ is the sum $f_2 - 2\,f_3$, where $f_2$ and $f_3$ are the second and third basis elements of $ModularForms(KroneckerCharacter(-7), 3)$.*

**(6.2.4) Conjecture.** *Let $L_1$ be the lattice given by the Gram matrix*

$$Gram(L_1) := \begin{bmatrix}2 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\\ 0 & 0 & 2 & -1\\ 0 & 0 & -1 & 4\end{bmatrix}$$

*The genus containing $L_1$ has one other lattice $L_2$. Both lattices in this genus have discriminant 28. Let $c(p)$ be the number of isotropics in $\mathbb{P}(L/pL)$, which works out to $p^3 - 1 + \left(\frac{7}{p}\right)(p^2 - p)$ whenever $p$ is a prime number that that does not divide the descriminant of the lattice.*

*Then, there is a modular form of weight 3 with character the Kronecker character over $-7$ (which is equivalent to the Kronecker character over the negitive of the determinant of the lattice), and with fourier expansion $\sum_{n=0}^{\infty} a_n q^n$. the Matrix $T_p$ corresponding p-neighbours (ie the matrix of the Hecke operator) for the genus containing $L_1$ is the following matrix:*

$$T_p \;=\; c(p)\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + \frac{w(p)}{|Aut(L_1)| + |Aut(L_2)|}\begin{bmatrix}-|Aut(L_1)| & |Aut(L_2)|\\ |Aut(L_2)| & -|Aut(L_1)|\end{bmatrix}$$

*Where*

$$w(p) = \; p\left(\left(\frac{7}{p}\right) + \left(\frac{-1}{p}\right)\right)a_p - 2\,p\left(\left(\frac{-1}{p}\right) + 1\right) + \left(p+1\right)^2$$

*In magma [2], the modular form $\sum_{n=0}^{\infty} a_n q^n$ is the sum $-f_2 + 3\,f_3$, where $f_2$ and $f_3$ are the second and third (default) basis elements of the vector space $ModularForms(KroneckerCharacter(-7), 3)$.*

**(6.2.5) Conjecture.** *Let $L_1$ be the lattice given by the Gram matrix*

$$Gram(L_1) := \begin{bmatrix}2 & 0 & 0 & 0\\ 0 & 2 & -1 & 1\\ 0 & -1 & 4 & -1\\ 0 & 1 & -1 & 4\end{bmatrix}$$

*The genus containing $L_1$ has one other lattice $L_2$. Both lattices in this genus have discriminant 48. Let $c(p)$ be the number of isotropics in $\mathbb{P}(L/pL)$.*

*Then, there is a modular form of weight 3 with character the (Dirchlet) Kronecker character over 48 (which is equivalent to the Kronecker character over the negitive of the determinant of the lattice), and with fourier expansion $\sum_{n=0}^{\infty} a_n q^n$. the Matrix $T_p$ corresponding p-neighbours (ie the matrix of the Hecke operator) for the genus containing $L_1$ is the following matrix:*

$$T_p \;=\; c(p)\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + \frac{w(p)}{|Aut(L_1)| + |Aut(L_2)|}\begin{bmatrix}-|Aut(L_1)| & |Aut(L_2)|\\ |Aut(L_2)| & -|Aut(L_1)|\end{bmatrix}$$

*Where the relation between $w(p)$ and $a(p)$ when $p$ is an odd prime that does not divide the discriminant, is:*

$$a_p = \left(1 + \left(\frac{-3}{p}\right)\right)\left(\left(w(p)/(p-1) - (\frac{p+1}{2})^2\right)\left(5\left(\frac{-3}{p}\right) + 3\right) + p\left(3\left(\frac{-3}{p}\right) - \left(\frac{-1}{p}\right) + \left(\frac{3}{p}\right) + 1\right)\right)$$

*In magma [2], the modular form $\sum_{n=0}^{\infty} a_n q^n$ is the sum $-4f_2 + 12f_4 - 8f_8 - 36f_{10} + 88f_{14} - 104f_{20}$, where $f_i$ is the $i^{th}$ (default) basis elements of the vector space*

$$ModularForms(DirichletGroup(48)!KroneckerCharacter(48), 3)$$

*in magma.*

## 6.3 Similarities Across Different Genera

**(6.3.1).** The following are some observations (conjectures) on the similarities between $T_p$ matrices and $w(p)$ coefficients across different genera of non-degenerate even $\mathbb{Z}$-lattices of rank 4. Many other similar examples of these phenomenon have been found. It is important to note that none of these observations have been mathematically proven.

**(6.3.2) Observation.** *The following lattices are members of different genera, with all of the genera have the same $T_p$ matrices (when $p$ does not divide any of the Determinants):*

*Determinant: 24*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 1 & 0 \\ -1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}$$

*Determinant: 96*
*Inner Product Matrix:*
$$\begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 4 & 0 & 1 \\ 2 & 0 & 4 & -1 \\ 1 & 1 & -1 & 4 \end{bmatrix}$$

*Determinant: 96*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 8 \end{bmatrix}$$

*Determinant: 96*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & 1 & 0 \\ -1 & 1 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

*Determinant: 96*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 2 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

**(6.3.3) Observation.** *The genera generated by each of the following lattices have the same $w(p)$ value for all prime $p$ that don't divide the discriminant, they they do not have the same $T_p$ matrix.*

*Determinant: 40*
*Inner Product Matrix:*

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 \\ 0 & 0 & 2 & 1 \\ 0 & -1 & 1 & 6 \end{bmatrix}$$

*Determinant: 40*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 4 & 2 \\ 1 & 0 & 2 & 4 \end{bmatrix}$$

**(6.3.4) Observation.** *The genera generated by each of the following lattices have the same $w(p)$ value for all prime $p$ that don't divide the discriminant, yet they they do not have the same $T_p$ matrix.*

*Determinant: 44*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & -1 & 1 \\ 0 & -1 & 2 & -1 \\ 0 & 1 & -1 & 8 \end{bmatrix}$$

*Determinant: 44*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & -1 & 0 \\ 1 & -1 & 4 & -1 \\ 0 & 0 & -1 & 4 \end{bmatrix}$$

**(6.3.5) Observation.** *Let $p$ be an odd prime that does not divide 52. The following three lattices each generate a genus, all of which have the same $w(p)$ value. Moreover, the first two (excluding the third) have the same matrix $T_p$ for each odd prime not dividing their discriminant. The third lattice listed has the same $w(t)$ value:*

*Determinant: 72*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}$$

*Determinant: 72*
*Inner Product Matrix:*
$$\begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & -1 & 0 \\ 1 & -1 & 4 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}$$

*Determinant: 72*
*Inner Product Matrix:*

$$\begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -1 & -1 \\ -1 & -1 & 4 & 1 \\ 0 & -1 & 1 & 4 \end{bmatrix}$$

# References


[1] Michael Atiyah and Ian Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Henri Cartan and Samuel Eilenberg. *Homological Algebra*. Princeton University, 1956.

[4] Gaëtan Chenevier and Jean Lannes. *Automorphic Forms and Unimodular Lattices*, volume 69 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer, 2019.

[5] Henri Cohen. An Introduction to Modular Forms, 2018.

[6] John Little David Cox and Hal Schenck. *Toric Varieties*. American Mathematical Society, 2011.

[7] George Grätzer. *Universal Algebra*. Springer, 1979.

[8] Jacques Helmstetter and Artibano Micali. *Quadratic Mappings and Clifford Algebras*. Birkhäuser Basel, 2008.

[9] James E. Humphreys. *Linear Algebraic Groups*, volume 21 of *Graduate Texts in Mathematics*. Springer, 1975.

[10] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer, 1990.

[11] Martin Kneser. Strong approximation. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, volume 187, page 196, 1966.

[12] Hao Billy Lee. Hecke Operators. 2015.

[13] Kimball Martin. A Brief Overview of Modular and Automorphic Forms. 2016.

[14] Kenneth Ribet and William Stein. Lectures on Modular Forms and Hecke Operators. 2011.

[15] Jean-Pierre Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer, 1973.

[16] Valeriya Talovikova. Riemann Roch Theorem. 2009.