Ternary Quadratic Forms
and
Modular Forms of Half Integral Weight

Tan Do
Supervisor: Dr. Steven Galbraith

May 10, 2012

Acknowledgement

I would like to thank Dr. Steven Galbraith for his support during my time of doing this thesis.

Contents

Chapter 1

Introduction

As the title suggests, this thesis consists of two parts: *quadratic forms* and *modular forms*. The theory of quadratic forms is among the oldest and most highly developed studies of mathematics, with various application in number theory, linear algebra, analytic geometry and algebraic topology, etc. Here we are interested in its number-theoretical aspect, in particular, quadratic forms of three variables over the rational integers or *integral ternary quadratic forms*. The motivation of our study began with Schiemann's result that *positive definite ternary quadratic forms are determined by their theta series*. In other words, if two positive definite ternary quadratic forms represent the same set of integers the same number of times, then they are the same. We then go on examining the effect of *multiplicities of representation* in this statement. That is, *what happens if we drop the condition "the same number of times"?* Somewhere along the line, we realised that this question was already considered by Kaplansky. He also made a conjecture about it in a letter to Schiemann in 1997. This conjecture involves Dickson's idea of *regular forms*. Loosely speaking, a ternary quadratic form is regular when the set of its non-representable numbers form some arithmetic progressions. A typical example is the form $x^2 + y^2 + z^2$ which misses all the numbers of the form $4^k(8n+7)$. With this idea, *Kaplanky's conjecture* are presented as follows:

"If two positive ternaries represent the same numbers ignoring multiplicity, then at least one of the following holds:

1. *Both are regular.*
2. *One is equivalent to $ax^2 + by^2 + bz^2 + byz$ and the other to $ax^2 + by^2 + 3bz^2$.*
3. *One is equivalent to $ax^2 + ay^2 + az^2 + byz + bxz + bxy$, one to $ax^2 + (2a - b)y^2 + (2a + b)z^2 + 2bxz$."*

In this thesis, we proved that Kaplansky's conjecture holds for a certain family of forms, which are known as *diagonal forms*. Jones (1928) proved that there are precisely 102 regular diagonal forms. This fact combined with our result implies further that Schiemann's statement becomes invalid but a near miss in this simplest case. Specifically, it remains true for all but two pairs of diagonal forms. These are presented in Subsection 2.4.3.

The theory of modular forms begins with the study of *theta functions*. It is closely related to the question of determining the number of ways to represent an integer as sums of n squares, where n is a positive integer. A classical result is *Jacobi's four squares theorem* which give the answer for the case $n = 4$. In fact, the question can be successfully dealt with for the case n is an even integer, using *modular forms of integral weights*. However, modular forms of integral weights are inapplicable when n is odd. To derive similar results in this case, we need the theory of *modular forms of half integral weights*. A systematic approach to this theory was first given by Shimura in 1973. For the second half of the thesis, we study both modular forms of integral and half integral weights. Some main results of this part include *the formulae of representing an integer as sums of two and four squares*, *a recursive relation for sums of three squares*, *relation between sums of five squares and Dirichlet L-function*. We emphasise modular forms of half integral weights due to their connection with ternary quadratic forms. In Subsection 3.3.4, we give one application to demonstrate the idea. Except for this subsection, the others are independent with the first half of the thesis.

Chapter 2

Ternary quadratic forms

2.1 General theory

In this section, $\mathbb{F}$ will be a field whose $\mathrm{char}(\mathbb{F}) \neq 2$. $I \subset \mathbb{F}$ is a subring or a subfield. The set of all units of I is denoted by $\mathrm{U}(I)$. We also denote the transpose of a matrix A by A^t, the set of all matrices of dimension $n \times n$ over I by $\mathrm{M}_n(I)$. We will use bold letters to denote vectors. Interpretation of vectors as row or column vectors is flexible, which depends on context.

2.1.1 Basic facts and notations

Definition 2.1.1.1. *A* ***quadratic form*** *in n variables $\boldsymbol{x} = (x_1, \dots, x_n)$ over I is defined by*

$$f(\boldsymbol{x}) = \sum_{i=1}^{n} f_{ii} x_i^2 + \sum_{1 \leq i < j \leq n} f_{ij} x_i x_j,$$

where $f_{ij} \in I$ $(1 \leq i, j \leq n)$.

We can rewrite f in matrix notation as

$$f(\boldsymbol{x}) = \boldsymbol{x} \mathrm{Gr}(f) \boldsymbol{x}^t,$$

where

$$\mathrm{Gr}(f) := \begin{bmatrix} f_{11} & \frac{f_{12}}{2} & \cdots & \frac{f_{1n}}{2} \\ \frac{f_{12}}{2} & f_{22} & \cdots & \frac{f_{2n}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{f_{1n}}{2} & \frac{f_{2n}}{2} & \cdots & f_{nn} \end{bmatrix}$$

is called the Gram matrix of f.

Definition 2.1.1.2. *The* ***determinant*** *of a quadratic form f, denoted by $D(f)$, is defined to be $2^n \det(\mathrm{Gr}(f))$.*
If $D(f) = 0$, we say that f is ***singular*** *(or degenerate). Otherwise, f is* ***non-singular*** *(or non-degenerate).*

Definition 2.1.1.3. *Let $k \in I$. We say that a quadratic form f* ***represents*** *k (or k is representable by f) if there exists $\boldsymbol{x} = (x_1, \ldots, x_n) \in I^n$ such that*

$$f(\boldsymbol{x}) = k.$$

If $\gcd(x_1, \ldots, x_n) = 1$*, then the representation is called* ***primitive*** *(or proper). Otherwise, it is called* ***imprimitive*** *(or non-proper).*
The number of representations of k by f is called the ***multiplicity of representation*** *and is denoted by $r_f(k)$.*
The set of all representable k of f over I is denoted by $V_I(f)$.

More generally, we can speak of a representation of a form g in m variables by a form f in n variables over I if there are $\mathbf{b}_1, \ldots, \mathbf{b}_m \in I^n$ such that

$$f(y_1\mathbf{b}_1 + \ldots + y_m\mathbf{b}_m) = g(y_1, \ldots, y_m).$$

We have the following definition

Definition 2.1.1.4. *Let f, g be two quadratic forms in n variables over I. We say that f, g are* ***equivalent*** *over I (or I-equivalent), denoted by $f \sim_I g$, if each represents the other.*

The following lemma gives a simple criterion to check if two forms are equivalent.

Proposition 2.1.1.5. ([Cas08], Lemma 2.1, p.7) *Two non-singular forms f, g are I-equivalent iff there exists a matrix $T \in \mathrm{M}_n(I)$ such that* $\det(T) \in \mathrm{U}(I)$ *and*

$$\mathrm{Gr}(f) = T^t \mathrm{Gr}(g) T.$$

2.1.2 Quadratic spaces

Definition 2.1.2.1. *A* ***quadratic space*** *over $\mathbb{F}$ is defined to be a finite dimensional $\mathbb{F}$-vector space U together with a symmetric bilinear form $\phi : U \times U \longrightarrow \mathbb{F}$.*

We will denote the dimension of U by $\dim(U)$ and set

$$\phi(u) = \phi(u, u) \quad (u \in U).$$

From the function $\phi(u)$ of the single variable u, we can derive the symmetric bilinear form $\phi(u_1, u_2)$ via the formula

$$\phi(u_1, u_2) = \frac{1}{4}\big[\phi(u_1 + u_2) - \phi(u_1 - u_2)\big]. \tag{2.1}$$

Therefore, instead of starting with the bilinear form $\phi(u_1, u_2)$, we could have started with a function $\phi(u)$ of a single variable subject to the following conditions

i. $\phi(\lambda u) = \lambda^2 \phi(u)$.

ii. The right hand side of (2.1) is a bilinear form in u_1 and u_2.

Immediately from Equation (2.1), we have

Lemma 2.1.2.2. *Suppose that the bilinear form $\phi(u_1, u_2)$ is not identically 0. Then there exists a $u \in U$ such that $\phi(u) \neq 0$.*

Let $\dim(U) = n$ and suppose $\{u_1, \ldots, u_n\}$ is a basis for U. Then

$$f(x_1, \ldots, x_n) = \phi\big(\sum_i x_i u_i\big) = \sum_{i,j} x_i x_j \phi(u_i, u_j) \tag{2.2}$$

is a quadratic form over $\mathbb{F}$.
If $\{u'_1, \ldots, u'_n\}$ is another basis for U, then

$$f(x'_1, \ldots, x'_n) = \phi\big(\sum_i x'_i u'_i\big) = \sum_{i,j} x'_i x'_j \phi(u'_i, u'_j)$$

is clearly equivalent to f. Also, every form equivalent to f arises in this way.

Definition 2.1.2.3. *The **dual** of U, denoted by $\mathrm{Hom}(U, \mathbb{F})$, is the set of all $\mathbb{F}$-linear maps from U to $\mathbb{F}$.*

Define

$$\begin{aligned} \psi : U &\longrightarrow \mathrm{Hom}(U, \mathbb{F}) \\ w &\longmapsto \phi_w : u \mapsto \phi(u, w) \end{aligned}$$

We have the following definition

Definition 2.1.2.4. *A quadratic space (U, ϕ) is **non-singular** if ψ is an isomorphism. Otherwise, (U, ϕ) is **singular**.*

Lemma 2.1.2.5. *The following statements are equivalent*

i. *(U, ϕ) is non-singular.*

ii. *If $w \in U$ and $\phi(u, w) = 0$ for all $u \in U$, then $w = 0$.*

iii. *$\det[\phi(u_i, u_j)]_{1 \leq i,j \leq n} \neq 0$, where $\{u_1, \ldots, u_n\}$ is any basis of U.*

iv. *The form f given by (2.2) is non-singular.*

Proof. Clearly, (i) $\iff$ (ii) and (iii) $\iff$ (iv). We will prove (ii) $\iff$ (iii). Indeed, if $\det[\phi(u_i, u_j)]_{1 \leq i,j \leq n} \neq 0$, then there is an r such that $\phi(u_r, u_j) = \sum_{k=1}^{r-1} c_k \phi(u_k, u_j) = \phi(\sum_{k=1}^{r-1} c_k u_k, u_j)$, where $c_k \in \mathbb{F}$ and $j \in \{1, \ldots, n\}$. Due to (ii), $u_r = \sum_{k=1}^{r-1} c_k u_k$, which is a contradiction since $\{u_i\}_i$ forms a basis for U. Therefore, (ii) $\Longrightarrow$ (iii). The argument is reversible, so (iii) $\Longrightarrow$ (ii). □

Definition 2.1.2.6. *The **radical** of a quadratic space (U, ϕ), denoted by U_0, is the set of all $a \in U$ such that $\phi(a, b) = 0$ for all $b \in U$.*

If $a_1, a_2 \in U_0$, then $x_1 a_1 + x_2 a_2 \in U_0$ due to bi-linearity of ϕ. Clearly, $0 \in U_0$. Therefore, U_0 is a subspace of U. Following Definition 2.1.2.4, the quadratic space (U, ϕ) is non-singular precisely when $U_0 = \{0\}$.
We will use the notion of radical later to prove the equivalence of a singular quadratic form (over a principal ideal domain) to a non-singular quadratic form in a smaller number of variables (see Subsection 2.1.4).

2.1.3 Lattices

Definition 2.1.3.1. *Let $U = \{u_1, \ldots, u_n\}$ be a set of n linearly independent vectors over F. A* ***lattice*** *over I with basis U is the set of all points of the form*

$$x_1u_1 + \ldots + x_nu_n, \quad x_i \in I,\ 1 \leq i \leq n.$$

A lattice may have many bases. The next proposition gives a necessary and sufficient condition for a set of vectors to be a basis for a lattice.

Proposition 2.1.3.2. ([Cas08], Lemma 2.1, p.103) *Let Λ be the lattice over I with basis $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ elements of Λ. Suppose that*

$$v_i = \sum_k r_{ik}u_k, \quad r_{ik} \in I,\ 1 \leq i, k \leq n.$$

Then $\{v_1, \ldots, v_n\}$ is a basis for Λ iff

$$\det[r_{ik}] \in \mathrm{U}(I).$$

If I is a principal ideal domain, then there is a special choice of basis for Λ to represent linearly independent elements as follows

Lemma 2.1.3.3. ([Cas08], Lemma 3.4, p.105) *Suppose that I is a principal ideal domain. Let $\{v_1, \ldots, v_k\}$ be linearly independent elements of Λ. Then there exist a basis $\{u_1, \ldots, u_n\}$ of Λ such that*

$$\begin{aligned} v_1 &= s_{11}u_1, \\ v_2 &= s_{21}u_1 + s_{22}u_2, \\ &\ \vdots \\ v_k &= s_{k1}u_1 + \ldots + s_{kk}u_k, \end{aligned}$$

where $s_{ij} \in I$ and $s_{ii} \neq 0$.

2.1.4 Quadratic forms over principal ideal domains

Proposition 2.1.4.1. *Suppose I is a principal ideal domain. Then any singular quadratic form is I-equivalent to a non-singular form in a smaller number of variables.*

Proof. Let Λ be an I-lattice in a quadratic space (U, ϕ) and Λ_0 the radical of Λ. That is,

$$\Lambda_0 = \{a \in \Lambda :\ \phi(a, b) = 0\ \forall\, b \in \Lambda\}.$$

Let k be the maximal number of linearly independent vectors in Λ_0. If $\{v_1, \ldots, v_k\}$ is a linearly independent set of elements of Λ_0, then by Lemma 2.1.3.3, there exist a basis $\{u_1, \ldots, u_n\}$ of Λ such that

$$\begin{aligned} v_1 &= s_{11}u_1, \\ v_2 &= s_{21}u_1 + s_{22}u_2, \\ &\ \vdots \\ v_k &= s_{k1}u_1 + \ldots + s_{kk}u_k, \end{aligned}$$

where $s_{ij} \in I$ and $s_{ii} \neq 0$.
It is easy to see that $u_i \in \Lambda_0$ $(1 \leq i \leq k)$. By maximality of k, the radical Λ_0 is the sub-I-module of Λ spanned by $\{u_1, \dots, u_k\}$.
Let Λ_1 be the submodule of Λ spanned by $\{u_{k+1}, \dots, u_n\}$. Clearly, the quadratic form induced by ϕ on Λ_1 is non-singular. □

In the next section, we will consider quadratic forms over the rational integer $\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, we will only need to consider non-singular quadratic forms due to the above proposition.

2.2 Quadratic forms over $\mathbb{Z}$

From this section onward, all quadratic forms are non-singular without being mentioned. We will use $\mathbb{Q}_p, \mathbb{Z}_p$ to denote the set of p-adic numbers and p-adic integers respectively. If $p = \infty$, we agree with the convention $\mathbb{Q}_\infty = \mathbb{Z}_\infty = \mathbb{R}$, the set of all real numbers. Also, $|\cdot|_p$ denotes the p-adic valuation on $\mathbb{Q}_p$ and $\mathbb{Z}_p$.

2.2.1 Positive definite forms

Definition 2.2.1.1. *A quadratic form f over $\mathbb{Z}$ is said to be* ***positive definite*** *if $V_{\mathbb{R}}(f) = \mathbb{R}_{\geq 0}$. It is said to be* ***strictly positive definite*** *if f is positive definite and $f(\boldsymbol{x}) = 0$ only when $\boldsymbol{x} = 0$.*

Definition 2.2.1.2. *Let $M = [m_{ij}]_{i,j=1,\dots,n} \in \mathrm{M}_n(\mathbb{R})$. Then its* ***leading principal matrices*** *are matrices of the form $[m_{ij}]_{i,j=1,\dots,k}$, where $k \in \{1, \dots, n\}$.*

The following way to determine the positivity of forms are usually known as *Sylvester criterion.*

Proposition 2.2.1.3. ([Hor90], Theorem 7.2.5, p.404) *A form f is (stricly) positive definite if and only if the leading principal minors of its Gram matrix have (positive) non-negative determinants.*

For convenience, we include the following definition (which does not logically belong here) in this subsection for later use.

Definition 2.2.1.4. *Let*

$$f(\boldsymbol{x}) = \sum_{i=1}^{n} f_{ii} x_i^2 + \sum_{1 \leq i < j \leq n} f_{ij} x_i x_j$$

be a quadratic form over $\mathbb{Z}$. If $\gcd(f_{ij}) = 1$, then f is called ***primitive***. *Otherwise, f is called* ***non-primitive***.

2.2.2 Equivalence classes

It is well-known that equivalence classes of a given determinant is finite, as stated in the following theorem

Theorem 2.2.2.1. ([Cas08], Theorem 1.1, p.128) *Let $n \in \mathbb{N}, d \in \mathbb{Z} \setminus \{0\}$ be given. Then there are only finitely many equivalence classes of integral quadratic forms f in n variables $(x_1, \dots, x_n)$ with $D(f) = d$.*

In 1958, Brandt and Intrau published a table of primitive positive definite ternary quadratic forms (up to equivalence) of discriminants up to 1000. Schiemann later recomputed it. We will therefore refer to this table as Brant-Intrau-Schiemann table and will use it later in Subsection 3.3.4. For details about Brant-Intrau-Schiemann table, see [Gab12].

2.2.3 Genera

Definition 2.2.3.1. *Two non-singular integral quadratic forms f, g are said to be in the same **genus** if they are equivalent in every $\mathbb{Z}_p$ (including $p = \infty$). That is,*

$$f(\boldsymbol{x}) = g(T_p \boldsymbol{x}) \tag{2.3}$$

for some $T_p \in \mathrm{M}_n(\mathbb{Z}_p)$ with $\det(T_p) \in \mathrm{U}(\mathbb{Z}_p)$ for all p.

We deduce immediately from Definition 2.2.3.1 that each quadratic form belongs to a unique genus. A procedure to find all forms in the same genus with a given one is given in Subsection 3.3.4. Here we only state some facts about forms in the same genus. Let f be a quadratic form. We denote the genus of f by $\mathrm{Gen}(f)$.

Proposition 2.2.3.2. *Let $g \in \mathrm{Gen}(f)$. Then $D(g) = D(f)$.*

Proof. Due to (2.3),

$$D(f) = \det(T_p)^2 D(g)$$

for all p. Therefore, $D(f)/D(g) \in \mathrm{U}(\mathbb{Z}_p)$ for all p, which means $D(f)/D(g) \in \{\pm 1\}$. The value $p = \infty$ eliminates the case $D(f)/D(g) = -1$. Thus, $D(f) = D(g)$. □

Theorem 2.2.2.1 and Proposition 2.2.3.2 together imply

Theorem 2.2.3.3. *The number of equivalence classes in a genus is finite.*

However, finiteness is not yet good enough, as it does not ensure a bound on the number of equivalence classes. In fact, we have

Theorem 2.2.3.4. ([Cas08], Corollary, p.154) *The number of equivalence classes in a genus may be arbitrarily large.*

There is an interesting link between forms in the same genus via the set of representable numbers, as stated in the following theorem

Theorem 2.2.3.5. ([Cas08], Theorem 1.3, p.129) *Let $f(x_1, \dots, x_n)$ be an integral form and let $a \neq 0$ be an integer which is represented by f over each $\mathbb{Z}_p$ (including $p = \infty$). Then a is represented over $\mathbb{Z}$ by some form g in the same genus as f.*

Two forms in the same genus are also 'p-adically close'. In particular,

Proposition 2.2.3.6. ([Cas08], Corollary 1, p.140) *Let P be a finite set of primes $p \neq \infty$ and let f, g be integral forms in the same genus. Then there is an f^* integrally equivalent to f which is arbitrarily close to g in the p-adic sense for each $p \in P$.*

Proposition 2.2.3.7. ([Cas08], Corollary 2, p.138) *Let f be a positive definite integral form in $n \leq 5$ variables with $D(f) = 1$. Then f is equivalent to*

$$x_1^2 + \ldots + x_n^2.$$

2.3 Reduction theory

2.3.1 Minkowski reduced forms

Since equivalence forms have the same properties and the same set of representable numbers, it is more convenient to work with a representative of an equivalence class than each individual in the same class. The problem of finding suitable representatives belongs to the so-called *reduction theory.* There are several ways to define such representatives in literature. Here we follow that of Minkowski, which appears to be the most suitable one.

Definition 2.3.1.1. *A strictly positive definite quadratic form f is said to be **Minkowski reduced** if for each j*

$$f(\boldsymbol{e}_j^*) \geq f(\boldsymbol{e}_j)$$

where $\boldsymbol{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ and $\boldsymbol{e}_j^*$ runs through all the integral vectors with which $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{j-1}\}$ can be extended to a basis $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{j-1}, \boldsymbol{e}_j^*, \ldots\}$ of the lattice of integral vectors.

Theorem 2.3.1.2. ([Cas08], Theorem 1.1, p.256) *Every strictly positive definite form is equivalent to at least one and at most finitely many reduced forms.*

Proposition 2.3.1.3. ([Cas08], Lemma 1.2, p.257) *Let $n \leq 4$ and $f(\boldsymbol{x}) = \sum_{i=1}^n f_{ii}x_i^2 + \sum_{1 \leq i < j \leq n} f_{ij}x_ix_j$, where $f_{ij} \in \mathbb{Z}$. A necessary and sufficient condition that $f(\boldsymbol{x})$ be Minkowski reduced form is that*

1. $0 < f_{11} \leq f_{22} \leq \ldots \leq f_{nn}$.
2. $f(\boldsymbol{s}) \geq f_{kk}$ *for* $1 \leq k \leq n$ *and for all* $\boldsymbol{s}$ *with*

$$\begin{aligned} s_j &= 0 \textit{ or} \pm 1 \quad \textit{for } j < k, \\ s_k &= 1, \\ s_j &= 0 \quad \textit{for } j > k. \end{aligned}$$

For convenience, we will write down conditions (1) and (2) of Proposition 2.3.1.3 more explicitly for the cases $n = 2$ and $n = 3$:

1. $n = 2$: A quadratic form $f(\boldsymbol{x}) = f_{11}x_1^2 + f_{22}x_2^2 + f_{12}x_1x_2$ is Minkowski reduced iff $0 < f_{11} \leq f_{22}$ and $|f_{12}| \leq f_{11}$.

2. $n = 3$: A quadratic form $f(\boldsymbol{x}) = f_{11}x_1^2 + f_{22}x_2^2 + f_{33}x_3^2 + f_{12}x_1x_2 + f_{13}x_1x_3 + f_{23}x_2x_3$ is Minkowski reduced iff $0 < f_{11} \leq f_{22} \leq f_{33}$, $\max\{|f_{12}|, |f_{13}|\} \leq f_{11}$, $|f_{23}| \leq f_{22}$ and $|f_{12} \pm f_{23}| \leq |f_{11} + f_{22} \pm f_{13}|$.

2.3.2 Geometry of positive definite forms and Minkowski reduced forms

The Gram matrix of a quadratic form in n variables is symmetric. So to understand the geometry of quadratic forms, we embed their Gram matrices into the space $\mathbb{R}^{n(n+1)/2}$. We have the following theorems

Theorem 2.3.2.1. ([Cas08], Theorem 5.1, p.270)

i. *The set $\mathscr{P}^0$ of all strictly positive definite forms is an open convex subset of $\mathbb{R}^{n(n+1)/2}$.*

ii. *The closure $\mathscr{P}$ of $\mathscr{P}^0$ consists of all positive definite forms or semi-definite forms.*

To understand the geometry of Minkowski reduced forms, we need the following definition

Definition 2.3.2.2. *A form f is called **strictly Minkowski reduced** if it is Minkowski reduced and the only integral unimodular transformation T such that $f(T\boldsymbol{x})$ is also Minkowski reduced are the diagonal transformations with entries ± 1.*

Theorem 2.3.2.3. ([Cas08], Lemma 5.3, p.271)

i. *The set $\mathscr{R}^0$ of all strictly Minkowski reduced forms is convex and open.*

ii. *The set $\mathscr{R}$ of all Minkowski forms is the relative closure of $\mathscr{R}^0$ in $\mathscr{P}^0$.*

2.4 Ternary quadratic forms and Kaplansky's conjecture

This section presents our work on Kaplansky's conjecture. Our main results are Theorem 2.4.3.12 and Theorem 2.4.3.13. For simplicity, we will denote a ternary quadratic form by

$$T(z, y, z) := \langle a, b, c, d, e, f\rangle := ax^2 + by^2 + cz^2 + dyz + ezx + fxy,$$

where $a, b, c, d, e, f \in \mathbb{Z}$, throughout this section. If $d = e = f = 0$, we call T a *diagonal form*. Diagonal forms are of main interest in the last subsection.

2.4.1 Schiemann reduced forms

By Theorem 2.3.1.2, we know that at most finitely many Minkowski reduced forms are equivalent to a given form. For binary quadratic forms, there is only one such Minkowski reduced form (see [Cox89]). For ternary quadratic forms, this is no longer true. For example, the form $x^2+3y^2+3z^2+2xy-2yz-xz$ is equivalent to $x^2+2y^2+3z^2-2yz-xz$

and $x^2+2y^2+2z^2+xz$, both of which are Minkowski reduced. However, the uniqueness property is so highly desirable that much effort was made to find such a reduction procedure for ternary quadratic forms (see [Dic92], Chapter IX). One such procedure was given by Schiemann in [Sch97]. Here we present Schiemann's idea.

Definition 2.4.1.1. *A positive ternary quadratic form*

$$T(x,y,z)=ax^2+by^2+cz^2+dyz+ezx+fxy$$

is called ***Schiemann reduced*** *iff the following conditions are satisfied*

1. *T is Minkowski reduced.*
2. *$e\geq 0, f\geq 0$,*
   $e=0$ or $f=0 \Longrightarrow d=0$.
3. *$a=b \Longrightarrow |d|\leq e$,*
   $b=c \Longrightarrow |e|\leq f$.
4. *$a+b+d-e-f=0 \Longrightarrow 2a-2e-f\leq 0$,*
   $f=a \Longrightarrow e\leq 2d$,
   $e=a \Longrightarrow e\leq 2d$,
   $d=b \Longrightarrow f\leq 2e$,
   $d>-b$.

Taking the conditions of Minkowski's reduction into account, we have the following sets of inequalities for Schiemann reduced forms

1. $0<a\leq b\leq c$,
   $-b<d\leq b$,
   $0\leq e\leq a$,
   $0\leq f\leq a$,
   $a+b\leq -d+e+f$.
2. $e=0$ or $f=0 \Longrightarrow d=0$.
3. $a=b \Longrightarrow |d|\leq e$,
   $b=c \Longrightarrow |e|\leq f$,
   $f=a \Longrightarrow e\leq 2d$,
   $e=a \Longrightarrow e\leq 2d$,
   $d=b \Longrightarrow f\leq 2e$.
4. $a+b+d-e-f=0 \Longrightarrow 2a-2e-f\leq 0$.

Note that $D(T)=4abc+def-ad^2-be^2-cf^2$, and when T is Schiemann reduced, we have

$$2abc\leq D(T)\leq 4abc.$$

The significance of Schiemann reduded forms is expressed by the following theorem.

Theorem 2.4.1.2. ([Sch97], pp.$509-510$) *Each positive ternary quadratic form is equivalent to a unique Schiemann reduced form.*

2.4.2 Regular forms

Following Dickson in [Dic27], we make the following definition

Definition 2.4.2.1. *Let n be a positive integer. We call n an **eligible number** for representation by $T(x, y, z)$ if the congruence equation*

$$T(x, y, z) \equiv n \pmod{k}$$

*is solvable for all integer $k \geq 1$. The set of all eligible numbers of $T(x, y, z)$ is denoted by $E(T)$. If an integer is not eligible, then we say it is **ineligible** (or sporadic).*
*A form $T(x, y, z)$ is **regular** if it represents all of its eligible numbers.*

Theorem 2.4.2.2. ([Jag97], [Jon28]) *There are at most* 913 *regular positive ternary quadratic forms and precisely* 102 *regular positive diagonal ternary quadratic forms.*

The list of 913 possibly regular forms can be found in [Jag97], 899 of which are proved regular. So there remain 14 candidates (see [Jag10]). Also, [Dic39] gives a list of all 102 regular diagonal forms together with their ineligible numbers (see pp.$111 - 113$).

Theorem 2.4.2.3. ([Jon39], p.166) *An eligible number of a ternary form T is represented by a ternary form $T' \in \mathrm{Gen}(T)$.*

Proposition 2.4.2.4. *Any form in a genus of one class is regular.*

Proof. By Theorem 2.4.2.3, any form in a genus of one class represents all of its eligible numbers, thus regular. □

As mentioned in Theorem 2.4.2.2, there are precisely 102 regular positive diagonal forms. This result was proved by Jones in 1928. It happens that 82 of these forms are in genera of one class (see [Jon39], p.167), so regularity follows at once from Proposition 2.4.2.4. Therefore, the hardest part of the proof is perhaps due to the word "precisely".

Corollary 2.4.2.5. *The form $x^2 + y^2 + z^2$ is regular.*

Proof. By Proposition 2.2.3.7, $x^2 + y^2 + z^2$ is in a genus of one class. □

Corollary 2.4.2.6. *The form $2x^2 + 2y^2 + 3z^2 + 2yz + 2xz + 2xy$ is regular.*

Proof. As proved in Example 3.3.4.10, $2x^2 + 2y^2 + 3z^2 + 2yz + 2xz + 2xy$ is in a genus of one class. □

With Definition 2.4.2.1, we can now reformulate what it means for two ternary quadratic forms to be in the same genus in terms of their eligible numbers (Proposition 2.4.2.9). We first state two lemmas used in the proof of this reformulation.

Lemma 2.4.2.7. ([Cas08], Lemma 5.2, p.123) *Let $T = \langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle$ and $T' = \langle b_1, b_2, b_3, b_4, b_5, b_6 \rangle$ be ternary quadratic forms with $D(T) = D(T')$ and p a prime. Suppose that*

$$a_i \equiv b_i \pmod{p^{\delta + 2\lambda}},$$

where $|D(T)|_p = p^{-\delta}$ and

$$\lambda = \begin{cases} 1 & \text{if } p = 2 \\ 0 & \text{otherwise} \end{cases}.$$

Then $T \sim_{\mathbb{Z}_p} T'$.

Lemma 2.4.2.8. ([Jon39], p.165) *Let T and T' be ternary quadratic forms. Then $D(T') = D(T)$ and $E(T') = E(T)$ if and only if there exists a matrix $M = [m_{ij}] \in \mathrm{M}_3(\mathbb{Q})$ with the following properties:*

(i) $\det(M) = 1$.

(ii) $|m_{ij}|_p \leq 1$ *for all prime $p|2D(T)$ and $i, j \in \{1, 2, 3\}$.*

(iii) $T'(\boldsymbol{x}) = T(M\boldsymbol{x})$ *for all $\boldsymbol{x} \in \mathbb{Z}^3$.*

Proposition 2.4.2.9. *Let T and T' be ternary quadratic forms. Then $T' \in \mathrm{Gen}(T)$ if and only if $D(T') = D(T)$ and $E(T') = E(T)$.*

Proof. ($\Longrightarrow$) We denote $T = \langle a_1, a_2, a_3, a_4, a_5, a_6\rangle$, $T' = \langle b_1, b_2, b_3, b_4, b_5, b_6\rangle$. By Proposition 2.2.3.2, $D(T') = D(T)$. Now let $n \in E(T)$. Then $T(\boldsymbol{x}) \equiv n \pmod k$ is solvable for all integer $k \geq 1$, where $\boldsymbol{x} \in \mathbb{Z}^3$. By Proposition 2.2.3.6. There is a form $T^* = \langle a_1^*, a_2^*, a_3^*, a_4^*, a_5^*, a_6^*\rangle$ such that T^* is integrally equivalent to T and $a_i^* \equiv b_i \pmod k$ for arbitrary $k \in \mathbb{Z}$, where $i \in \{1, 2, 3, 4, 5, 6\}$. Since T^* is integrally equivalent to T, there is a matrix $M \in \mathrm{M}_3(\mathbb{Z})$ such that $T^*(\boldsymbol{x}) = T(M\boldsymbol{x})$. Therefore, $T^*(\boldsymbol{x}) \equiv n \pmod k$ is solvable for all integer $k \geq 1$. Thus, $T'(\boldsymbol{x}) \equiv n \pmod k$ is solvable for all integer $k \geq 1$.
($\Longleftarrow$) Let $D(T') = D(T)$ and $E(T') = E(T)$. If $p \nmid 2D(T)$, then $T \sim_{\mathbb{Z}_p} T'$ by Lemma 2.4.2.7. If $p \mid 2D(T)$, then $T \sim_{\mathbb{Z}_p} T'$ by Lemma 2.4.2.8. Finally, the condition $D(T) = D(T')$ says that T and T' are also equivalent over the reals. Hence T and T' are in the same genus. □

Recall that we denote the set of representable numbers of a form T by $V_{\mathbb{Z}}(T)$. We will drop the subscript $\mathbb{Z}$ as it is clear in our present consideration.

Proposition 2.4.2.10. *If $V(T) = V(T')$, then $E(T) = E(T')$.*

Proof. Let $n \in E(T)$, then

$$\forall\, k \in \mathbb{Z} \;\; T \equiv n \pmod k \text{ is solvable.}$$

Therefore,

$$\forall\, k \in \mathbb{Z} \;\exists\, m \in \mathbb{Z} \;\exists (x, y, z) \in \mathbb{Z}^3, \;\; T(x, y, z) = n + mk.$$

Since $V(T) = V(T')$, $n + mk \in V(T')$ and so $n \in E(T')$. By symmetry, $E(T) = E(T')$. □

Corollary 2.4.2.11. *If $V(T) = V(T')$ and $D(T) = D(T')$, then $T' \in \mathrm{Gen}(T)$.*

Proposition 2.4.2.12. *If $V(T) = V(T')$, then T is regular if and only if T' is regular.*

Proof. By Proposition 2.4.2.10, $E(T) = E(T')$. Suppose T is regular, then $V(T) = E(T)$. So $V(T') = E(T')$. □

Proposition 2.4.2.13. *If T, T' are inequivalent forms in the same genus of size 2, then $V(T) = V(T')$ if and only if T and T' are regular.*

Proof. ($\Longrightarrow$) Let $n \in E(T)$. Then by Theorem 2.4.2.3, either $T(x,y,z) = n$ or $T'(x,y,z) = n$ is solvable. Therefore, we always have $n \in V(T)$. Clearly, $n \in V(T)$ implies $n \in E(T)$. Hence, $V(T) = E(T)$. This together with Proposition 2.4.2.12 say that T and T' are regular. ($\Longleftarrow$) Let T and T' be both regular. Then $V(T) = E(T)$ and $V(T') = E(T)$. Since they are in the same genus, $E(T) = E(T')$ by Proposition 2.4.2.9. Thus, $V(T) = V(T')$. □

Corollary 2.4.2.14. *The form $x^2 + y^2 + 10z^2$ is irregular.*

Proof. The only form in the same genus with $x^2 + y^2 + 10z^2$ is $2x^2 + 2y^2 + 3z^2 + 2yz$ (see Example 3.3.4.9). Note that $x^2 + y^2 + 10z^2$ does not represent 3 whereas the latter does. So by Proposition 2.4.2.13, $x^2 + y^2 + 10z^2$ is irregular. □

The form $x^2 + y^2 + 10z^2$ is known in literature as the *Ramanujan form.*

2.4.3 On Kaplansky's conjecture

Schiemann (1993) proved that positive ternary quadratic forms are determined by their theta series. In particular, two positive ternary quadratic forms are equivalent if they represent the same set of integers the same number of times up to a bound. For details, see [Sch97]. We are then led to consider the question: "*What happens if two positive ternary quadratic forms represent the same set of integers, ignoring their multiplicities of representation?*". Kaplansky (1997) gave the following conjecture

If two positive ternaries represent the same numbers ignoring multiplicity, then at least one of the following holds:

1. Both are regular.

2. One is equivalent to $< s, t, t, t, 0, 0 >$ and the other to $< s, t, 3t, 0, 0, 0 >$.

3. One is equivalent to $< t, t, t, s, s, s >$, one to $< t, 2t - s, 2t + s, 0, 2s, 0 >$.

In this subsection, we will prove Kaplansky's conjecture holds when the two forms are diagonal. But first, we rule out the possibility that if two positive ternary quadratic forms have the same set of representable numbers, then they are equivalent.

Proposition 2.4.3.1. *If $V(ax^2 + by^2 + fxy) = V(a'x^2 + b'y^2 + f'xy)$, then*

$$V(ax^2 + by^2 + mz^2 + fxy) = V(a'x^2 + b'y^2 + mz^2 + f'xy) \ \forall m \in \mathbb{Z}.$$

Proof. Let $n \in V(ax^2 + by^2 + mz^2 + fxy)$. Then

$$\exists\, (x_0, y_0, z_0) \in \mathbb{Z}^3, n = ax_0^2 + by_0^2 + mz_0^2 + fx_0y_0.$$

So that $n - mz_0^2 \in V(ax^2 + by^2 + fxy) = V(a'x^2 + b'y^2 + f'xy)$. Then

$$\exists\, (x_1, y_1) \in \mathbb{Z}^2, n - mz_0^2 = a'x_1^2 + b'y_1^2 + mz_0^2 + f'x_1y_1.$$

Thus, $n \in V(a'x^2 + b'y^2 + f'xy)$. The statement follows by symmetry. □

Example 2.4.3.2. We know that $V(x^2+y^2+xy) = V(x^2+3y^2)$. By Proposition 2.4.3.1, $V(x^2+y^2++3z^2+xy) = V(x^2+3y^2+3z^2)$. Note also that $x^2+y^2+3z^2+xy$ and $x^2+3y^2+3z^2$ are Schiemann reduced, hence not equivalent.

In what follows, we will denote $T = ax^2+by^2+cz^2$ and $T' = a'x^2+b'y^2+c'z^2$. Since each ternary quadratic form is equivalent to a unique Schiemann reduced form and the Schiemann reduced form of a diagonal form remains diagonal, we will assume T, T' are Schiemann reduced in what follows. Also, note that if $V(T) = V(T')$ and $s \in \mathbb{Z}$, then s divides $V(T)$ implies s divides $V(T')$ and vice versa. We can therefore assume further that T, T' are primitive. To prove Kaplansky's conjecture for diagonal forms, we divide the problem into 4 cases: $a = c$, $a = b < c$, $a < b = c$ and $a < b < c$. The general setting for our method is to find some bounds on the coefficients a, b, c, a', b', c' and then to examine all the possibilities given by the bounds. This requires detailed checking of approximately 70 sub-cases, which sometimes can be labourious. To shorten the work, we will present here some most common sub-cases. The others will follow by similar arguments. In general, the method works well for most sub-cases. There are a few sub-cases when the bounds are too large. We overcome this by using congruence equations. We now start by listing all lemmas used for proving the above 4 cases.

Lemma 2.4.3.3. *Let $x \in \mathbb{Z}$. Then*

(i) x^2+1 *is a square* $\iff x = 0$.

(ii) x^2+2 *is not a square.*

(iii) x^2+3 *is a square* $\iff x = \pm 1$.

(iv) x^2+4 *is a square* $\iff x = 0$.

Proof. We prove (iv) only. The others follow from the same argument. ($\Longrightarrow$) Let $x^2+4 = y^2$. Then $(|y|-|x|)(|y|+|x|) = 4$. It follows that $|y|-|x| = 1, |y|+|x| = 4$ or $|y|-|x| = |y|+|x| = 2$. The first case is not solvable in $\mathbb{Z}$. The latter gives $x = 0$. ($\Longleftarrow$) Clear. □

Lemma 2.4.3.4. *Let $m, u \in \mathbb{Z}_{\geq 0}$. Then $4^m(4u+1)$ is the sum of two squares and $4^m(4u+3)$ is not the sum of two squares.*

Proof. Since $4u+1 \equiv 1 \pmod 4$, every prime factors $p \equiv 3 \pmod 4$ are of even powers. Also, $4u+3 \equiv 3 \pmod 4$ implies $4u+3$ contains a prime factor $p \equiv 3 \pmod 4$ of odd powers. Thus, the lemma follows. □

Lemma 2.4.3.5. *Let $x, y, m \in \mathbb{Z}$ and $m > 0$. If $x^2+y^2 \equiv 0 \pmod{4^m}$, then $x = 2^m x_0$ and $y = 2^m y_0$ for some $x_0, y_0 \in \mathbb{Z}$.*

Proof. First, note that $x^2+y^2 \equiv 0 \pmod 4$ implies x, y are both even. The result follows from induction on m. □

Proposition 2.4.3.6. *Let $T = ax^2+by^2+cz^2$, where $a = c$, and $T' = a'x^2+b'y^2+c'z^2$ be primitive Schiemann reduced positive definite ternary quadratic forms. Suppose $V(T') = V(T)$. Then both T and T' are regular.*

Proof. Since T is Schiemann reduced, we have $a \leq b \leq c$. But $a = c$, so we must have $a = b = c$. Primitivity implies $a = b = c = 1$. Therefore, $T = x^2 + y^2 + z^2$ which is regular. The proposition now follows from Proposition 2.4.2.12. □

Proposition 2.4.3.7. *Let $T = ax^2 + ay^2 + cz^2$, where a, c are distinct, and $T' = a'x^2 + b'y^2 + c'z^2$ be primitive Schiemann reduced positive definite ternary quadratic forms. Suppose $V(T') = V(T)$. Then either $T = T'$ or both T and T' are regular.*

Proof. Since T' is Schiemann reduced, we have $a' \leq b' \leq c'$. Being the smallest representable numbers of T and T', $a = a'$. Also, since $2a \in V(T)$, $b' = a$. So far, we have

$$T = ax^2 + ay^2 + cz^2,$$
$$T' = ax^2 + ay^2 + c'z^2.$$

Without loss of generality, we suppose $c \leq c'$. If $c = c'$, then $T = T'$ and we are done. If $c < c'$, then $c' = c + k$ for some $k > 0$ and $ax^2 + ay^2 = c$ is solvable. Since T is primitive, $a = 1$. Note that $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. So we will consider the following cases: $c = 4t$, $c = 4t + 1$ and $c = 4t + 2$ for some $t \in \mathbb{Z}$.

Case 1: Let $c = 4t$. Since c is the sum of two squares, using Lemma 2.4.3.4, we can be more precise and write $c = 4^n(4s + r)$, where $n \in \mathbb{Z}_{\geq 1}$, $s \in \mathbb{Z}_{\geq 0}$ and $r \in \{1, 2\}$. So $T = x^2 + y^2 + 4^n(4s + r)z^2 \equiv x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. For any specific $(x_0, y_0, z_0) \in \mathbb{Z}^3$, we always have

$$T'(x_0, y_0, z_0) = T(x_0, y_0, z_0) + kz_0^2 \equiv 0, 1, 2 \pmod 4,$$

Let $(x_0, y_0, z_0) = (0, 1, 1)$, we deduce that $k \equiv 0, 1, 3 \pmod 4$. Similarly, $(x_0, y_0, z_0) = (0, 2, 1)$ implies $k \equiv 0, 1, 2 \pmod 4$ and $(x_0, y_0, z_0) = (1, 1, 1)$ implies $k \equiv 0, 2, 3 \pmod 4$. So we must have $k \equiv 0 \pmod 4$. Let us write $k = 4^m(4u + v)$, where $m, u \in \mathbb{Z}_{\geq 0}$, $v \in \{0, 1, 2, 3\}$. If $u = v = 0$, then $T = T'$. So we can restrict further that $v \in \{1, 2, 3\}$. Therefore,

$$T = x^2 + y^2 + 4^n(4s + r)z^2,$$
$$T' = x^2 + y^2 + \left(4^n(4s + r) + 4^m(4u + v)\right)z^2.$$

We need to check the following 2 sub-cases

(1i) $r = 1$: Observe that $4^n(4s + 3) \in V(T)$. Since $V(T) = V(T')$, the equation

$$x^2 + y^2 + \left(4^n(4s + r) + 4^m(4u + v)\right)z^2 = 4^n(4s + 3)$$

is solvable. Since $4^n(4s+3) \leq 3\times 4^n(4s+1)$, we have $z = 1$ and so $x^2+y^2+4^m(4u+v) = 2 \times 4^n$ is solvable. This implies $m \leq n$.

If $m = n$, then $x^2 + y^2 \equiv 0 \pmod{4^m}$. By Lemma 2.4.3.5, $x = 2^m x_1$ and $y = 2^m y_1$ for some $x_1, y_1 \in \{0, \pm 1\}$. If $x_1, y_1 \in \{\pm 1\}$, then $u = v = 0$ and so $T = T'$. For other values of x_1, y_1, we have either $u = 0, v = 1$ or $u = 0, v = 2$. Therefore, $T = x^2+y^2+4^n(4s+1)z^2$ and $T' = x^2+y^2+4^n(4s+2)z^2$ or $T' = x^2+y^2+4^n(4s+3)z^2$. In either case, $4^n(4s+7) \in V(T')$. It follows that $x^2+y^2+4^n(4s+1)z^2 = 4^n(4s+7)$ is solvable. Since $4s+7 \equiv 3 \pmod 4$, using Lemma 2.4.3.4, we deduce that $z = 1$, which

implies $x^2+y^2=6\times 4^n$ is solvable. Now use Lemma 2.4.3.5, we have $x_2^2+y_2^2=6$, where $x=2^n x_2$ and $y=2^n y_2$. But this equation has no solution, so these cases are impossible.
If $m<n$, then $x^2+y^2\equiv 0 \pmod{4^m}$. By Lemma 2.4.3.5, $x=2^m x_1$ and $y=2^m y_1$ for some $x_1, y_1\in\mathbb{Z}$. Then $x^2+y^2+4u+v=2\times 4^{n-m}$. It follows that $x_1^2+y_1^2+v\equiv 0 \pmod 4$. Since $x_1^2+y_1^2\equiv 0,1,2 \pmod 4$, we have $v\in\{2,3\}$. If $v=3$, then $T'=x^2+y^2+\left(4^n(4s+1)+4^m(4u+3)\right)z^2$. Then $4^n(4s+1)+4^m(4u+3)\in V(T')$. Therefore, $x^2+y^2+4^n(4s+1)z^2=4^n(4s+1)+4^m(4u+3)$ is solvable. Note that $4^n(4s+1)+4^m(4u+3)<3\times 4^n(4s+1)$. This forces $z=1$, and so $x^2+y^2=4^m(4u+3)$ is solvable. By Lemma 2.4.3.4, $4^m(4u+3)$ is not the sum of two squares. So this case is not possible. If $v=2$, then $T'=x^2+y^2+\left(4^n(4s+1)+4^m(4u+2)\right)z^2$. Then we also have $4^n(4s+1)+4^m(4u+3)\in V(T')$. Using the same argument as before, we deduce that this case is also not possible.

(1ii) $r=2$: We have $T=x^2+y^2+4^n(4s+2)z^2$. Therefore, $4^n(4s+3)\in V(T)$ and we are back in the case (1i).

Case 2: If $c=4t+1$ or $c=4t+2$, then $T=x^2+y^2+(4t+1)z^2$ or $T=x^2+y^2+(4t+2)z^2$. In either case, $4t+3\in V(T)$. This means $x^2+y^2+c'z^2=4t+3$ is solvable. But $4t+3\equiv 3 \pmod 4$ and $4t+3\le 2c<2c'$. It follows that $z=1$ and so $x^2+y^2+c'=4t+3$. Therefore, $x^2+y^2+k=2$, which implies $k\in\{1,2\}$. We consider the following 2 sub-cases

(2i) $c'=c+1$: We have

$$T=x^2+y^2+cz^2,$$
$$T'=x^2+y^2+(c+1)z^2.$$

Then $c+6=1^2+2^2+(c+1)1^2\in V(T')$. So $x^2+y^2+cz^2=c+6$ is solvable. But $c+6\equiv 3 \pmod 4$, we must have $x=y=0$ and $z=2$. Then $c=2$. Note that $x^2+y^2+2z^2$ is regular. Now use Proposition 2.4.2.12 and we are done.

(2ii) $c'=c+2$: Similar to the above case, $c+6\in V(T')$ and we deduce that $T=x^2+y^2+2z^2$ which is regular.

The proposition now follows. □

Proposition 2.4.3.8. *Let $k\in\{1,2\}$ and $s\in\mathbb{Z}_+$. Let $T=kx^2+s^2y^2+s^2z^2$ and $T'=kx^2+s^2y^2+c'z^2$ be Schiemann reduced positive definite ternary quadratic forms. Suppose $V(T')=V(T)$. Then $T=T'$ or both T and T' are regular.*

Proof. We prove the case $k=1$ only. The case $k=2$ is proved similarly. When $k=1$, we have $T=x^2+s^2y^2+s^2z^2$ and $T'=x^2+s^2y^2+c'z^2$. Since $2s^2+4\in V(T)$, the equation $x^2+s^2y^2+c'z^2=2s^2+4$ is solvable. Clearly, $y=0$ since otherwise, s^2+4 is a square, which would imply $s=0$. If $z=0$, then $2s^2+4$ is a square and so is $2s^2+1$. But then 3 is the difference of two squares, which is not possible. Thus $z\neq 0$ and $c'\le 2s^2+4$. Note also that $c'\ge s^2$ since T' is Schiemann reduced. If $c'=s^2$, then $T=T'$. We now consider other sub-cases.

(i) $c' = 2s^2 + r$, $r \in \{1, 2, 3, 4\}$: Since $3s^2 \in V(T)$. So $x^2 + s^2y^2 + (2s^2 + r)z^2 = 3s^2$ is solvable. So either $x^2 = 3s^2$ or $x^2 = 2s^2$ or $x^2 + r = s^2$ is solvable. The first two cases are clearly not possible. For the last case, using lemma 2.4.3.3, we have either $s^2 = 1$ with $r = 1$ or $s^2 = 4$ with $r = 3, 4$ respectively. The 3 corresponding cases are $T = x^2 + y^2 + z^2, T' = x^2 + y^2 + 3z^2$ and $T = x^2 + 4y^2 + 4z^2, T' = x^2 + 4z^2 + 11z^2$ and $T = x^2 + 4y^2 + 4z^2, T' = x^2 + 4z^2 + 12z^2$. For the first case, T does not represent 7, whereas T' does. So this case is not possible. For the second case, T does not represent 11 whereas T' does. So this case is also not possible. For the last case, T does not represent 28 whereas T' does. So this case is also not possible. Therefore, $c' \leq 2s^2$.

(ii) $c' = 2s^2$: Then $T' = x^2 + s^2y^2 + 2s^2z^2$. Note that T' represents $15s^2$, whereas T does not. So this case is not possible.

(iii) $c' = s^2 + r$, $0 < r < s^2$: If $r = l^2$ for some $l \in \mathbb{Z}$, then $T' = x^2 + s^2y^2 + (s^2 + l^2)z^2$. We have $s^2 + l^2 + 1 \in V(T')$. Since $x^2 + l^2 + 1 \leq 2s^2$, we have either $x^2 = l^2 + 1$ or $x^2 = s^2 + l^2 + 1$ is solvable. The first case implies $l = 0$ by Lemma 2.4.3.3, so not possible since $r > 0$. For the second case, if $s = 1$, then $T = x^2 + y^2 + z^2$ and $T' = x^2 + y^2 + 2z^2$. Since 15 is in $V(T')$ but not $V(T)$, this case is not possible. If $s \geq 2$, then $s^2 + l^2 + 4 \leq 3s^2$. So either $x^2 = l^2 + 4$ or $x^2 = s^2 + l^2 + 4$ is solvable. The latter case combined with the fact $s^2 + l^2 + 1$ is a square will imply $l = 0$, so not possible. So $l^2 + 4$ is a square. By Lemma 2.4.3.3, we have $l = 0$. So we eliminate this case also. Now we consider $r \neq l^2$ for any $l \in \mathbb{Z}$. Since $s^2 + r \in V(T')$, we must have $s^2 + r$ is a square. Similar to previous case, we consider $s^2 + r + 1$ and $s^2 + r + 4$ and finally conclude that this case is also not possible.

Note that the conclusion for $k = 1$ is $T = T'$. For $k = 2$, by the same argument as above, we have either $T = T'$ or $T = x^2 + 2y^2 + 2z^2$ which is regular. The proposition now follows. □

Proposition 2.4.3.9. *Let $T = ax^2 + by^2 + bz^2$, where a, b are distinct, and $T' = a'x^2 + b'y^2 + c'z^2$ be primitive Schiemann reduced positive definite ternary quadratic forms. Suppose $V(T') = V(T)$. Then either $T = T'$ or both T and T' are regular.*

Proof. Since T' is Schiemann reduced, we have $a' \leq b' \leq c'$. Being the smallest representable numbers of T and T', $a = a'$. Since $b \in V(T)$, b is also representable by T'. So there is some $(x_0, y_0, z_0) \in \mathbb{Z}^3$ such that $ax_0^2 + b'y_0^2 + c'z_0^2 = b$. We consider 2 cases as follows: $y_0 = z_0 = 0$ and either $y_0 \neq 0$ or $z_0 \neq 0$.
Case 1: If $y_0 = z_0 = 0$, then $b = ax_0^2$ for some $x_0 \in \mathbb{Z}_+$. Since T is primitive, $a = 1$. So that $T = x^2 + x_0^2y^2 + x_0^2z^2$. Then $x_0^2 + 1 \in V(T)$. Note that $x_0^2 + 1$ can not be a square when $x_0 \neq 0$. Therefore, $b' \leq x_0^2 + 1$. We consider the following 2 sub-cases

(1i) $b' = x_0^2 + 1$: Then $T' = x^2 + (x_0^2 + 1)y^2 + c'z^2$. It follows that $x_0^2 + 2 \in V(T')$. But neither 2 nor $x_0^2 + 2$ is a square, this case is not possible.

(1ii) $b' \leq x_0^2 = b$: Then $b' = x_1^2$ for some $x_1^2 \in \mathbb{Z}_+$. The value $x_1^2 + 1 \in V(T')$ forces $x_1 = x_0$. So that $T' = x^2 + x_0^2y^2 + c'z^2$. By Proposition 2.4.3.8, we have $T = T'$.

Case 2: Either y_0 or z_0 is non-zero. Then $b' \leq b$. If $b' = b$, then $T' = ax^2 + by^2 + c'z^2$. Since $2b \in V(T)$, there is some $(x_1, y_1, z_1) \in \mathbb{Z}^3$ such that $ax_1^2 + by_1^2 + c'z_1^2 = 2b$. So either $ax_1^2 = 2b$ or $ax_1^2 = b$. The latter case boils down to the sub-case (1ii), and so $T = T'$. For the first case, we consider $2T = 2x^2 + x_1^2y^2 + x_1^2z^2$ and $T' = 2x^2 + x_1^2y^2 + 2c'z^2$ instead. By Proposition 2.4.3.8, $T = T'$ or both are regular.
The proposition now follows. □

Proposition 2.4.3.10. *Let $T = ax^2 + by^2 + cz^2$, where a, b, c are distinct, and $T' = a'x^2 + b'y^2 + c'z^2$ be primitive Schiemann reduced positive definite ternary quadratic forms. Suppose $b \neq b'$ and $V(T') = V(T)$. Then either $T = T'$ or both T and T' are regular.*

Proof. Schiemann reduced condition just means $a \leq b \leq c$ and $a' \leq b' \leq c'$. Since a, b, c are distinct, we have $a < b < c$. As before, $a = a'$. We can suppose $b' < b$. The case $b < b'$ is dealt with similarly. Since $b' < b$, $b' = au^2$ for some $u \in \mathbb{Z}$. Next, we consider c'. There are only 3 possibilities: $c' < b$, $c' = b$ and $c' > b$.
If $c' < b$, then $c' = av^2$ for some $v \in \mathbb{Z}$, and so $a = 1$ as T' is primitive. Then $T = x^2 + by^2 + cz^2$ and $T' = x^2 + u^2y^2 + v^2z^2$. Note that $u^2 + 1 \leq b$. If $u^2 + 1 < b$, then $u^2 + 1$ is a square, but it is not. So $u^2 + 1 = b$. Therefore, $u^2 + 2 \in V(T) = V(T')$. Since $u^2 + 2$ is not a square, this case is not possible.
If $c' = b$, then $T' = ax^2 + au^2y^2 + bz^2$. Since $u^2 + 1$ is not a square, $a + au^2 \notin V(ax^2)$. So $b \leq a + au^2$. If $b = a + au^2$, then $a = 1$ as T' is primitive. Then $T = x^2 + (1 + u^2)y^2 + cz^2$ and $T' = x^2 + u^2y^2 + (1 + u^2)z^2$. From $u^2 + 4 \in V(T')$, we deduce that $c \leq u^2 + 4$. If $c = u^2 + 4$, then $u^2 + 8 \in V(T)$. If $u^2 + 8$ is a square, then $u = 1$. It follows that $T' = x^2 + y^2 + 2z^2$ which is regular. If $u^2 + 8 \in V(x^2 + u^2y^2)$ with $y \neq 0$, then $u = 1$ and again $T' = x^2 + y^2 + 2z^2$ which is regular. The case $u^2 + 8 \in V(T')$ with $z \neq 0$ also gives $u = 1$. If $b < a + au^2$, then $b = au^2 + k$ for some $0 \leq k < a$. Note that $a + au^2 \in V(ax^2 + (au^2 + k)y^2)$ with $y \neq 0$. If $y = 1$, then $k = 0$. This case gives $T = x^2 + y^2 + 2z^2$ or $T' = x^2 + y^2 + z^2$ which are regular. If $y \geq 2$, then $4au^2 > a + au^2$, so $c \leq a + au^2$. If $c = a + au^2$, then again $T = x^2 + y^2 + 2z^2$ or $T' = x^2 + y^2 + z^2$. If $c < a + au^2$, then $T = x^2 + y^2 + z^2$.
If $c' > b$, then $b = am^2 + au^2n^2$ for some $m, n \in \mathbb{Z}$. So $T = ax^2 + a(m^2 + u^2n^2)y^2 + cz^2$. Since $au^2 + a \in V(T')$ is not a square, we have $a(m^2 + u^2n^2) \leq au^2 + a$. It follows that $m = n = 1$. So $a(u^2+2) \in V(T)$. Easy checking shows that $c' \leq a(u^2+2)$. If $c' = a(u^2+2)$, then $a = 1$. The value $u^2 + 3 \in V(T')$ tells us that $c \leq u^2 + 3$. So $c = u^2 + 2$ and $c = u^2 + 3$. But we can check that c does not assume these two values. So this case is not possible. If $a(u^2 + 1) < c' < a(u^2 + 2)$, then $c' = a(u^2 + 1) + k$ for some $0 < k < a$. The value $a(u^2 + 1) + k \in V(T')$ gives $c \leq c'$. Checking the two cases $c = c'$ and $c < c'$ to see that this case is also not possible.
The proposition now follows. □

Proposition 2.4.3.11. *Let $T = ax^2 + by^2 + cz^2$, where a, b, c are distinct, and $T' = a'x^2 + b'y^2 + c'z^2$ be primitive Schiemann reduced positive definite ternary quadratic forms. Suppose $b = b'$ and $V(T') = V(T)$. Then $T = T'$ or both T and T' are regular.*

Proof. Without loss of generality, we suppose $c \leq c'$. If $c = c'$, then $T = T'$. If $c < c'$, then $c = au^2 + bv^2$ for some $u, v \in \mathbb{Z}$. The primitive condition of T now implies $\gcd(a, b) = 1$. We will consider the following 2 cases: $a \equiv b \equiv 1, 3 \pmod 4$ and $a \not\equiv b \pmod 4$. The latter case divides into 10 sub-cases: $a \equiv 0 \pmod 4$, $b \equiv 1, 3 \pmod 4$; $a \equiv 1 \pmod 4$, $b \equiv 0, 2, 3$

(mod 4); $a \equiv 2 \pmod 4$, $b \equiv 1, 3 \pmod 4$ and $a \equiv 3 \pmod 4$, $b \equiv 0, 1, 2 \pmod 4$. We will prove the first case only. The second case is proved similarly.
Now suppose $a \equiv b \equiv r \pmod 4$, $r \in \{1, 3\}$. Note that $u^2, v^2 \equiv 0, 1 \pmod 4$. So we will consider the following 4 sub-cases:
Case 1. $u^2 \equiv v^2 \equiv 1 \pmod 4$: Consider $A = a + au^2 + bv^2 \in V(T)$. If $A \in V(ax^2 + by^2)$, then $1 + u^2 + v^2 \equiv x^2 + y^2 \pmod 4$ is solvable. It follows that $3 \equiv x^2 + y^2 \pmod 4$ is solvable. This is impossible by Lemma 2.4.3.4. So $A \notin V(ax^2 + by^2)$. This means $c' \leq A$. So $c' = c + k$, where $0 < k \leq a$.

(1i) $k = a$: Then $T = ax^2 + by^2 + (au^2 + bv^2)z^2$ and $T' = ax^2 + by^2 + (au^2 + bv^2 + a)z^2$. Consider $b + au^2 + bv^2 \in V(T)$. As before, $b + au^2 + bv^2 \notin V(ax^2 + by^2)$. So $au^2 + bv^2 + b = ax^2 + by^2 + au^2 + bv^2 + a$. Then $b - a = ax^2 + by^2$. Note that $0 < b - a < b$. Therefore, $b - a = ax_0^2$ for some $x_0 \in \mathbb{Z}$. So $a \mid b$, which implies $a = 1$ since $\gcd(a, b) = 1$. It follows that $b = 1 + x_0^2$, where $x_0 = 2x_1$ for some $x_1 \in \mathbb{Z}$. So far, we have $T = x^2 + (1 + 4x_1^2)y^2 + (u^2 + (1 + 4x_1^2)v^2)z^2$ and $T' = x^2 + (1 + 4x_1^2)y^2 + (u^2 + (1 + 4x_1^2)v^2 + 1)z^2$. Consider $u^2 + (1 + 4x_1^2)v^2 + 5 \in V(T')$. As before, $u^2 + (1 + 4x_1^2)v^2 + 5 \notin V(x^2 + (1 + 4x_1^2)y^2)$. This means $5 = x^2 + (1 + 4x_1^2)y^2$. So $x_1 = y = 1$. Therefore, $b = 5$. We have $T = x^2 + 5y^2 + (u^2 + 5v^2)z^2$ and $T' = x^2 + 5y^2 + (u^2 + 5v^2 + 1)z^2$. But then $u^2 + (1 + 4x_1^2)v^2 + 17 \in V(T')$, whereas $u^2 + (1 + 4x_1^2)v^2 + 17 \notin V(T)$. So this case is not possible.

(1ii) $0 < k < a$: Consider $au^2 + bv^2 + a \in V(T)$. As before, $au^2 + bv^2 + a \notin V(ax^2 + by^2)$. So $au^2 + bv^2 + a = ax^2 + by^2 + au^2 + bv^2 + k$. Then $a - k = ax^2 + by^2$. This is not possible since $a - k < a$.

Case 2. $u^2 \equiv 0 \pmod 4$, $v^2 \equiv 1 \pmod 4$: Consider $a + b + au^2 + bv^2 \in V(T)$. If $a + b + au^2 + bv^2 \in V(ax^2 + by^2)$, then $3 \equiv x^2 + y^2 \pmod 4$ is solvable. This is not true by Lemma 2.4.3.4. So $a + b + au^2 + bv^2 \notin V(ax^2 + by^2)$. Therefore, $c' \leq a + b + au^2 + bv^2$. We consider the following subcases:

(2i) $c' = a+b+au^2+bv^2$: We have $9a+b+au^2+bv^2 \in V(T)$. As before, $9a+b+au^2+bv^2 \notin V(ax^2+by^2)$. So $9a+b+au^2+bv^2 = ax_0^2+by_0^2+a+b+au^2+bv^2$, whence $8a = ax_0^2+by_0^2$ for some $x_0, y_0 \in \mathbb{Z}$. Note that $x_0 < 3$. If $x_0 = 0$, then $8a = by^2$. Then $y = 1$, $b = 8a$ or $y = 2$, $b = 2a$. Since $\gcd(a, b) = 1$, $a = 1$. Then $b = 8$ or $b = 2$. These two values for b are not possible in our current consideration as $a \equiv b \pmod 4$. Note that the second possibility is valid when we consider the case when $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$. It gives the form $x^2 + 2y^2 + 4z^2$ which is regular.

(2ii) $c' = au^2 + bv^2 + b + k$, where $0 < k < a$: Consider $a + b + au^2 + bv^2 \in V(T)$. Since $a+b+au^2+bv^2 \notin V(ax^2+by^2)$, we have $a+b+au^2+bv^2 = ax^2+by^2+au^2+bv^2+b+k$. Then $a - k = ax^2 + by^2$. This is not possible since $a - k < a$.

(2iii) $c' = au^2+bv^2+b$: Consider $a+9b+au^2+bv^2 \in V(T)$. As before, $a+9b+au^2+bv^2 \notin V(ax^2+by^2)$. So $a+9b+au^2+bv^2 = ax_0^2+by_0^2+(au^2+bv^2+b)z_0^2$ for some $x_0, y_0, z_0 \in \mathbb{Z}$. Clearly, $0 < |z_0| < 3$. If $|z_0| = 2$, then $a + 5b = ax_0^2 + by_0^2 + 3(au^2 + bv^2)$, whence $|v| = 1$. Then $a + 2b = ax_0^2 + by_0^2 + 3au^2$. If $|y_0| = 1$, then $a + b = ax_0^2 + 3au^2$. Therefore, $a|b$ and so $a = 1$. Then $1 + b = x_0^2 + 3u^2$. But $1 + b \equiv 2 \pmod 4$, whereas

$x_0^2+3u^2 \equiv 0,1 \pmod{4}$. So $y_0 = 0$. Then $a+2b = ax^2+3au^2$. Again, $a|b$ so $a = 1$. We have $1+2b = x_0^2+3u^2$. But $1+2b \equiv 3 \pmod{4}$, whereas $x_0^2+3u^2 \equiv 0,1 \pmod{4}$. So $|z_0| = 1$. We have $a+8b = ax_0^2+by_0^2$. Clearly, $|y_0| \leq 2$. If $|y_0| = 2$, then $a+4b = ax_0^2$. Since $\gcd(a,4) = 1$, we have $a|b$, and so $a = 1$. Therefore, $T = x^2+by^2+(u^2+bv^2)z^2$ and $T' = x^2+by^2+(u^2+bv^2+b)z^2$. Consider $u^2+bv^2+b+1 \in V(T')$. Since $u^2+bv^2+b+1 \notin V(x^2+by^2)$, we have $1+b = s^2+bt^2$ for some $s,t \in \mathbb{Z}$. If $t = 0$, then $2b = s^2$. But $2b \equiv 2 \pmod{4}$, so this is not possible. Thus, $|t| = 1$. Then $b = s^2$. Consider $u^2+s^2u^2+2s^2+4 \in V(T')$. Again, $u^2+s^2u^2+2s^2+4 \notin V(x^2+by^2)$ implies $2s^2+4 = x^2+s^2y^2$ is solvable. It is easy to check that this is not possible. If $|y_0| = 1$, then $a+7b = ax^2+by^2$ is solvable. Therefore, $7b = a(x^2-1)$ is solvable. But then $3 \equiv x^2-1 \pmod{4}$. It follows that $2|x$ and so $4|b$, which is not possible. If $y_0 = 0$, then $a+8b = ax^2$ is solvable. Then $8b = a(x^2-1)$. Since $\gcd(a,8) = 1$, we have $a|b$ and so $a = 1$. Then $8b = x^2-1$ is solvable. But $8b+1 \equiv 3 \pmod{4}$, whereas $x^2 \equiv 0,1 \pmod{4}$. So this case is not possible.

(2iv) $c' = au^2+bv^2+k$, where $0 < k < b$: Consider $a+b+au^2+bv^2 \in V(T)$. Since $a+b+u+bv^2 \notin V(ax^2+by^2)$, we have $a+b-k = ax_0^2+by_0^2$ for some $x_0, y_0 \in \mathbb{Z}$. If $|y_0| = 1$, then $a-k = ax_0^2$, which implies $a|k$. This is impossible since $a-k < a$. So $y_0 = 0$. Then $a+b-k = ax_0^2$, and so $k = a+b-ax_0^2$. Note that $x_0^2 \equiv 0,1 \pmod{4}$. If $x_0^2 \equiv 0 \pmod{4}$, then consider $au^2+bv^2+k \in V(T')$. We have $au^2+bv^2+k \equiv 3a \pmod{4}$, so $au^2+bv^2+k \notin V(ax^2+by^2)$. Therefore, $a+b-ax_0^2 = k = as^2+bt^2$ for some $s,t \in \mathbb{Z}$. But $a+b-ax_0^2 < b$, so $t = 0$ and $a+b-ax_0^2 = as^2$. Then $a|b$ and so $a = 1$. We have $1+b = s^2+x_0^2$. This is not possible since $1+b \equiv 2 \pmod{4}$, whereas $s^2+x_0^2 \equiv 0,1 \pmod{4}$. If $x_0^2 \equiv 1 \pmod{4}$, then consider $a+b+(au^2+bv^2+k) \in V(T')$. Note that $a+b+(au^2+bv^2+k) \equiv 3a \pmod{4}$, so $a+b+(au^2+bv^2+k) \notin V(ax^2+by^2)$. This means $2(a+b)-ax_0^2 = as^2+bt^2$ for some $s,t \in \mathbb{Z}$. Note that $|t| < 2$. If $|t| = 1$, then $2a+b-ax_0^2 = as^2$, whence $a|b$. So $a = 1$. Then $2+b = s^2+x_0^2$. But $2+b \equiv 3 \pmod{4}$. So this is not possible. If $t = 0$, then $2(a+b)-ax_0^2 = as^2$. We still have $a|b$ and so $a = 1$. It follows that $2(1+b) = x^2+x_0^2$. But $2(1+b) \equiv 0 \pmod{4}$, whereas $s^2+x_0^2 \equiv 1,2 \pmod{4}$. So this is also not possible. In sum, this case is not possible.

Case 3. $u^2 \equiv 1 \pmod{4}$, $v^2 \equiv 0 \pmod{4}$: Similar to case 2.

Case 4. $u^2 \equiv v^2 \equiv 0 \pmod{4}$: We write $u = 4^{e_u}u_0^2$ and $v = 4^{e_v}v_0^2$, where $u_0^2 \equiv v_0^2 \equiv 1 \pmod{4}$. We first consider the case $e_u = e_v$. In what follows, we assume $r = 1$. The case $r = 3$ is treated similarly. We consider $4^{e_u}a+au^2+bv^2 \in V(T)$. Suppose $4^{e_u}a+au^2+bv^2 \in V(ax^2+by^2)$. Then $4^{e_u}a+au^2+bv^2 = ax^2+by^2$ is solvable. Using Lemma 2.4.3.5, we know that $a+au_0^2+bv_0^2 = ax^2+by^2$ is solvable. This will imply $3 \equiv x^2+y^2 \pmod{4}$ is solvable, which is a contradiction. So $4^{e_u}a+au^2+bv^2 \notin V(ax^2+by^2)$. Therefore, $c' \leq 4^{e_u}a+au^2+bv^2$. Let us write $c' = au^2+bv^2+k$, where $0 < k \leq 4^{e_u}a$. Let $k = 4^l k_0$, where $k_0 \not\equiv 0 \pmod{4}$. We also assume $l < e_u$. The cases $l = e_u$ and $l > e_u$ are treated similarly. If $k_0 \equiv 1 \pmod{4}$, then consider $4^l a+4^l b+au^2+bv^2+k \in V(T')$. Note that $4^l a+4^l b+au^2+bv^2+k = 4^l(a+b+4^{e_u-l}(au_0^2+bv_0^2)+k_0)$ and $a+b+4^{e_u-l}(au_0^2+bv_0^2)+k_0 \equiv 3 \pmod{4}$. So $4^l a+4^l b+au^2+bv^2+k \notin V(ax^2+by^2)$. Also $4^l a+4^l b+au^2+bv^2+k < 4(au^2+bv^2)$, so $4^l a+4^l b+k = ax^2+by^2$. But this implies $3 \equiv a+b+k_0 \equiv x^2+y^2 \pmod{4}$ is solvable, which is a contradiction. So this cases is not possible. The case $k_0 \equiv 2,3 \pmod{4}$ are

treated similarly.
The proposition now follows. □

We combine all the above propositions to derive the following theorem

Theorem 2.4.3.12. *Let T and T' be positive definite quadratic forms. Suppose $T \sim ax^2 + by^2 + cz^2$, $T' \sim a'x^2 + b'y^2 + c'z^2$, where $a, b, c, a', b', c' \in \mathbb{Z}$, and $V(T') = V(T)$. Then either $T \sim T'$ or both T and T' are regular.*

Thus, we have proved that Kaplansky's conjecture holds for diagonal forms. Recall that there are exactly 102 regular forms (see Theorem 2.4.2.2). The next step is therefore to go on checking what regular diagonal forms have the same set of representable numbers. We went through 102 regular diagonal forms listed in [Dic39] and observed that there are only 2 pairs of such forms. One is $T = x^2 + y^2 + z^2$ and $T' = x^2 + 2y^2 + 2z^2$. The other is $T = x^2 + y^2 + 2z^2$ and $T' = x^2 + 2y^2 + 4z^2$. Note that all these forms appeared in our proofs of the above propositions. This fact together with Theorem 2.4.3.12 gives

Theorem 2.4.3.13. *Let T and T' be positive definite quadratic forms. Suppose $T \sim ax^2 + by^2 + cz^2$, $T' \sim a'x^2 + b'y^2 + c'z^2$, where $a, b, c, a', b', c' \in \mathbb{Z}$, and $V(T') = V(T)$. Then one of the following holds*

(i) $T \sim x^2 + y^2 + z^2$ *and* $T' \sim x^2 + 2y^2 + 2z^2$, *or vice versa.*

(ii) $T \sim x^2 + y^2 + 2z^2$ *and* $T' \sim x^2 + 2y^2 + 4z^2$, *or vice versa.*

(iii) $T \sim T'$.

Recall that Schiemann proved if two ternary quadratic forms represent the same set of integers and each integer has the same multiplicity of representation by these two forms, then the two forms are the same (see [Sch97]). The above theorem says that Schiemann's result will not hold, even for the simplest case when the two forms are diagonal, if the multiplicity condition is dropped. However, it is a "near miss" as we can see.
We also notice that if we increase T and T' by a term xy or zx, say $T \sim ax^2 + by^2 + cz^2 + fxy$ and $T' \sim a'x^2 + b'y^2 + c'z^2 + f'xy$, then in Schiemann reduced forms, $a, b, c, f, a', b', c', f' > 0$ and a, a' will still be the smallest elements represented by T, T' respectively. These facts are crucial in our proof of Kaplansky's conjecture for diagonal forms. So we expect the result will still hold in this case. In fact, the author strongly believe this is the case. The proof, if follows the above method, will clearly consume a considerable amount of time and effort. Therefore, a subtler method, if exists, will be our delight.

Chapter 3

Modular forms of half integral weight

3.1 Modular group, congruence subgroups and cusps

3.1.1 Modular group

Definition 3.1.1.1. *The **modular group** is the group*

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

For short, we will denote the modular group by Γ. Elements of Γ can also be viewed as automorphisms of the Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$ via the *fractional linear transformation*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (z) = \frac{az+b}{cz+d}, \quad z \in \hat{\mathbb{C}}.$$

By definition,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (-\frac{d}{c}) = \infty, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} (\infty) = \begin{cases} a/c & \text{if } c \neq 0, \\ \infty & \text{if } c = 0. \end{cases}$$

Note that for $\gamma, \gamma' \in \Gamma$, we have $(\gamma'\gamma)(z) = \gamma'(\gamma(z))$ and $\pm\gamma \in \Gamma$ give the same transformation on $\hat{\mathbb{C}}$.

Definition 3.1.1.2. *The **upper half plane** is the set*

$$\mathfrak{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}.$$

Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$. Simple calculations show that

$$\mathrm{Im}(\gamma(z)) = \frac{\mathrm{Im}(z)}{|cz+d|^2},$$

which implies that $\gamma(z) \in \mathfrak{H}$ whenever $z \in \mathfrak{H}$. That is, the modular group preserves the upper half plane.

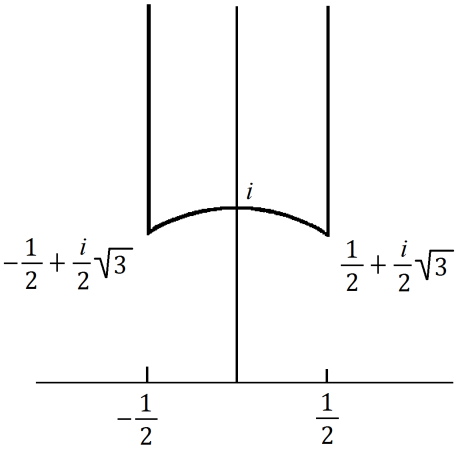
i
$-\frac{1}{2}+\frac{i}{2}\sqrt{3}$
$\frac{1}{2}+\frac{i}{2}\sqrt{3}$
$-\frac{1}{2}$
$\frac{1}{2}$

Figure 3.1: Fundamental domain $F(\Gamma)$

Proposition 3.1.1.3. ([Fre05], Proposition V.I.8, p.335) Γ *is generated by the two elements*

$$T := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad S := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Let G be a subgroup of Γ acting on $\mathfrak{H}$. We say that two points $z_1, z_2 \in \mathfrak{H}$ are G-equivalent if there is a $g \in G$ such that $z_2 = gz_1$. This leads to the following definition

Definition 3.1.1.4. *A region $F \subset \mathfrak{H}$ is called a* ***fundamental domain*** *for the subgroup G of Γ if F satifies the following conditions*

i. *F is closed.*

ii. *Every $z \in \mathfrak{H}$ is equivalent to a point in F.*

iii. *No points in F are equivalent to each other, except the boundary points.*

Proposition 3.1.1.5. ([Kob84], Proposition 1, p.102) *A fundamental domain for Γ is*

$$F(\Gamma) := \{z \in \mathfrak{H} : -\frac{1}{2} \leq \text{Re}z \leq \frac{1}{2} \text{ and } |z| \geq 1\}.$$

3.1.2 Congruence subgroups

Definition 3.1.2.1. *Let N be a positive integer. The* ***principal congruence subgroup*** *of level N is defined by*

$$\Gamma(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod N \right\},$$

where we interpret the matrix congruence entry-wise.

Definition 3.1.2.2. *A subgroup of Γ is called a* ***congruence subgroup*** *if it contains $\Gamma(N)$ for some positive integer N, in which case it is also called a* ***congruence subgroup of level N***.

The two most important congruence subgroups are

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod N \right\},$$

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod N \right\},$$

where $*$ indicates arbitrary integers.

Proposition 3.1.2.3. ([Kil08], Proposition 2.12, 2.13, pp.23-24) *Let N be a positive integer. Then*

$$\Gamma(N) \trianglelefteq \Gamma_1(N) \trianglelefteq \Gamma_0(N) \trianglelefteq \Gamma$$

and

$$\begin{aligned}[]
[\Gamma_1(N) : \Gamma(N)] &= N, \\
[\Gamma_0(N) : \Gamma_1(N)] &= \phi(N), \\
[\Gamma : \Gamma_0(N)] &= N \prod_{p|N} (1 + \frac{1}{p}),
\end{aligned}$$

where ϕ is the Euler totient function.

Following the previous subsection, we will find a fundamental domain for a congruence subgroup of level N. Here we illustrate the method for the case $\Gamma_0(N)$ when $N = 4$. First, we need the following proposition

Proposition 3.1.2.4. ([Kil08], Proposition 2.15, p.26) *Let $\Gamma' \subset \Gamma$ be a congruence subgroup. Suppose that $[\Gamma : \Gamma'] = n$ and*

$$\Gamma = \bigcup_{i=1}^{n} \alpha_i \Gamma'.$$

Then

$$F(\Gamma') = \bigcup_{i=1}^{n} \alpha_i^{-1} F(\Gamma).$$

Example 3.1.2.5. In this example, we will construct a fundamental domain for $\Gamma_0(4)$ using Proposition 3.1.2.4. First, note that the coset representatives for Γ modulo $\Gamma_0(4)$ are $\{I, S, T^{-1}S, T^{-2}S, T^{-3}S, ST^{-2}S\}$. So the fundamental domain for $\Gamma_0(4)$ is given by Figure 3.2.

3.1.3 Cusps

Let $\bar{\mathfrak{H}} = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$. That is, we extend $\mathfrak{H}$ to $\bar{\mathfrak{H}}$ by adjoinging to it the set $\mathbb{Q} \cup \{\infty\}$. Each element of $\mathbb{Q} \cup \{\infty\}$ is called a *cusp*. Note that we visualise ∞ as a point far up in positive imaginary axis direction. For this reason, we sometines denote it $i\infty$.

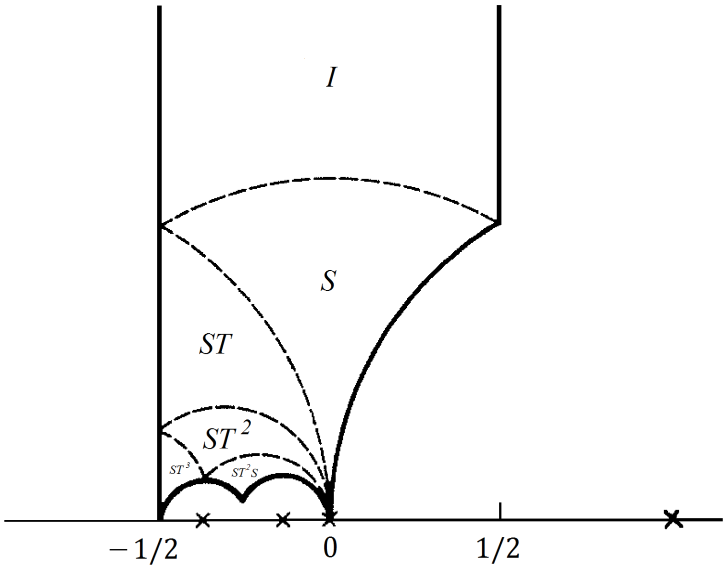

Figure 3.2: Fundamental domain $F(\Gamma_0(4))$

Each $a/c \in \mathbb{Q}$ in the lowest terms will determine a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ (by solving $ad - bc = 1$) such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (\infty) = \frac{a}{c}.$$

This means that all rational numbers are in the same Γ-equivalence class as ∞. Therefore, Γ permutes the cusps transitively.
If $\Gamma' \subset \Gamma$ is a subgroup, then Γ' permutes the cusps, but in general not transitively. This means there may be more than one Γ'-equivalence class among the cusps. By a *cusp of* Γ', we mean a Γ'-equivalence class of cusps. Any convenient representative of a Γ'-equivalence class can be chosen to be a cusp. Figure 3.1 says that Γ has a single cusp at ∞, whereas Figure 3.2 says $\Gamma_0(4)$ has 2 cusps at 0 and $-1/2$. Figure 3.2 also gives a geometrical explanation of "cusp", as at 0 and $-1/2$, the fundamental domain of $\Gamma_0(4)$ has the appearance that we usually associate with the word "cusp".

3.2 Modular forms of integral weights

3.2.1 Modular forms of integral weights for Γ

Definition 3.2.1.1. *Let k be an integer. A meromorphic function $f : \mathfrak{H} \longrightarrow \mathbb{C}$ is called a* ***weakly modular form*** *of weight k for Γ if*

$$f(\gamma(z)) = (c\tau + d)^k f(z), \quad \forall\, \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma, \quad z \in \mathfrak{H}.$$

Let $\gamma = -I$ in Definition 3.2.1.1, we obtain $f = (-1)^k f$. Therefore, the only weakly modular form of odd weight k (on Γ) is the zero function.

Next, let $\gamma = T$, where T is the translation

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} : z \longmapsto z + 1.$$

Then $f(z+1) = f(z)$. By Fourier analysis, we know that f has the Fourier expansion

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n, \quad q = e^{2\pi i z}. \tag{3.1}$$

The expansion (3.1) is called the *q-expansion* of f.

Definition 3.2.1.2. *The function f is said to be holomorphic (resp. vanishes) at infinity if $a_n = 0$ for $n < 0$ (resp. $n \leq 0$) in the q-expansion* (3.1).

Definition 3.2.1.3. *Let k be an integer. A function $f : \mathfrak{H} \longrightarrow \mathbb{C}$ is called a* ***modular form*** *of weight k for Γ if f satisfies the following conditions*

i. *f is holomorphic on $\mathfrak{H}$.*

ii. *f is weakly modular of weight k.*

iii. *f is holomorphic at ∞.*

The $\mathbb{C}$-vector space of all modular forms of weight k for Γ is denoted by $\mathrm{M}_k(\Gamma)$. Moreover, if condition (iii) *is replaced by*

iii'. *f vanishes at ∞,*

then f is called a ***cusp form*** *of weight k for Γ. The $\mathbb{C}$-vector space of all cusp forms of weight k for Γ is denoted by $\mathrm{S}_k(\Gamma)$.*

Remark 3.2.1.4. It follows from Definition 3.2.1.3 that the product of two modular forms (resp. cusp forms) of weight k_1 and k_2 is a modular form (resp. cusp form) of weight $k_1 + k_2$; the quotient of two modular forms (resp. cusp forms) of weight k_1 and k_2 is a modular form (resp. cusp form) of weight $k_1 - k_2$.

Next, we will construct concrete examples of modular forms and cusp forms of weight k for Γ. We start with a definition.

Definition 3.2.1.5. *Let k be an even integer greater than 2 and $z \in \mathfrak{H}$. The* ***Eisenstein series*** *of weight k is defined to be*

$$G_k(z) := {\sum_{m,n}}' \frac{1}{(mz+n)^k},$$

where the prime summation means to sum over all pairs of integers $(m, n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

Proposition 3.2.1.6.

$$G_k \in \mathrm{M}_k(\Gamma).$$

Proof. There are 3 conditions to check

i. Since $k > 2$, G_k converges absolutely on $\mathfrak{H}$ and uniformly on any compact subset of $\mathfrak{H}$. Therefore, G_k is holomorphic on $\mathfrak{H}$.

ii. For the weakly modular condition, it suffices to check $G_k(T(z)) = G_k(z)$ and $G_k(S(z)) = G_k(z)$. But this is obvious.

iii. G_k is holomorphic at infinity because

$$\lim_{z \to i\infty} \sum_{m,n}{}' \frac{1}{(mz+n)^k} = \sum_{n}{}' \frac{1}{n^k} = 2\zeta(k) < \infty,$$

where $\zeta(k)$ denotes the Rieman zeta function of level k.

□

In the proof above, we have proved that G_k is holomorphic at infinity without using the q-expansion of G_k. However, it will be useful to compute explicitly the q-expansion of $G_k(z)$.

Proposition 3.2.1.7.

$$G_k(z) = 2\zeta(k)\Big(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\Big),$$

where $q = e^{2\pi i z}$, B_k *is the* k*-th Bernoulli number defined by*

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!},$$

and σ_{k-1} *is the arithmetic divisor-sum function*

$$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}.$$

Proof. From complex analysis, we have

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty}\Big(\frac{1}{z+n} + \frac{1}{z-n}\Big), \quad z \in \mathfrak{H}. \tag{3.2}$$

Continuously differentiating both side of (3.2) and replacing z by mz, we obtain

$$\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} = \frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n m z}. \tag{3.3}$$

It is well-known that (for details, see [Whi35]) for even k

$$\zeta(k) = -\frac{(2\pi i)^k}{2k!} B_k. \tag{3.4}$$

Substituting (3.4) into (3.3), we have

$$\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} = -\frac{2k}{B_k}\zeta(k)\sum_{d=1}^{\infty} d^{k-1}q^{dm}.$$

Hence,

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^k} = 2\zeta(k)\Big(1-\frac{2k}{B_k}\sum_{m,d=1}^{\infty} d^{k-1}q^{dm}\Big).$$

We now collect coefficients of a fixed power q^n in the last double sum to obtain the proposition. □

Define

$$E_k(z) := \frac{1}{2\zeta(k)}G_k(z) = 1-\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n. \tag{3.5}$$

Then E_k has coefficient $a_0 = 1$ in its q-expansion. We call E_k the *normalised Eisenstein series*. Another way to look at the normalised Eisenstein series is

$$E_k = \frac{1}{2}\sum_{\substack{m,n\in\mathbb{Z}\\ \gcd(m,n)=1}}\frac{1}{(mz+n)^k}, \quad k\in 2\mathbb{Z},\ k\geq 4. \tag{3.6}$$

To see this, note that for each pair $(m,n)\in\mathbb{Z}^2$ with $\gcd(m,n)=1$, the multiples of $(mz+n)^{-k}$ appear $\zeta(k)$ times in G_k. Since G_k converges absolutely for $k>2$, we can rewrite it as $G_k = 2\zeta(k)E_k$. Therefore, (3.5) and (3.6) define the same series.
Let $g_2(z) = 60G_4(z)$ and $g_3(z) = 140G_6(z)$. Define

$$\Delta(z) := g_2(z)^3 - 27g_3(z)^2.$$

The function $\Delta(z)$ is normally called the *modular discriminant*. It arises from the study of elliptic curves. For details, see [Kob84].

Proposition 3.2.1.8.

$$\Delta(z)\in \mathrm{S}_{12}(\Gamma).$$

Proof. Since

$$\zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945},$$

we can rewrite g_2 and g_3 in terms of E_k as

$$g_2(z) = \frac{4\pi^4}{3}E_4(z), \quad g_3(z) = \frac{8\pi^6}{27}E_6(z).$$

Therefore,

$$\Delta(z) = \frac{(2\pi)^{12}}{1728}\big[E_4(z)^3 - E_6(z)^2\big]. \tag{3.7}$$

It follows from Remark 3.2.1.4 that $\Delta(z)\in \mathrm{M}_{12}(\Gamma)$. Equation (3.7) tells us that $a_0 = 0$ in the q-expansion of Δ. Thus, $\Delta(z)\in \mathrm{S}_{12}(\Gamma)$. □

The following propositions describe dimensions of spaces of modular forms and cusps forms.

Proposition 3.2.1.9. ([Kob84], Proposition 9, p.117) *Let k be an even integer.*

i. $\mathrm{M}_0(\Gamma) = \mathbb{C}$.

ii. $\mathrm{M}_k(\Gamma) = 0$ *if k is negative or* $k = 2$.

iii. $\mathrm{M}_k(\Gamma) = \mathbb{C}E_k$ *if* $k \in \{4, 5, 6, 10, 14\}$.

iv. $\mathrm{S}_k(\Gamma) = 0$ *if* $k < 12$ *or* $k = 14$*;* $\mathrm{S}_{12}(\Gamma) = \mathbb{C}\Delta$*;* $\mathrm{S}_k(\Gamma) = \Delta\mathrm{M}_{k-12}(\Gamma)$.

v. $\mathrm{M}_k(\Gamma) = \mathrm{S}_k(\Gamma) \bigoplus \mathbb{C}E_k$ *if* $k > 2$.

We formulate the above proposition as

Theorem 3.2.1.10. *Let k be an even positive integer. Then*

$$\mathrm{dim}\mathrm{M}_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \pmod{12} \end{cases},$$

and

$$\mathrm{dim}\mathrm{S}_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \not\equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor - 1 & \text{if } k \equiv 2 \pmod{12} \end{cases}.$$

3.2.2 Modular forms of integral weights for congruence subgroups

First, we introduce some notations.
Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ and let f be a function on $\bar{\mathfrak{H}}$ with values in $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$. We denote

$$f(z)|[\gamma]_k := (cz + d)^{-k} f(\gamma(z)).$$

$[\gamma]_k$ is called *weight k operator* for Γ. It follows immediately that $f|[\gamma_1\gamma_2]_k = \big(f|[\gamma_1]_k\big)|[\gamma_2]_k$. Also, let q_N denote $e^{2\pi i z/N}$.

Definition 3.2.2.1. *Let k be an integer and $\Gamma' \subset \Gamma$ be a congruence subgroup of level N. A function $f : \bar{\mathfrak{H}} \longrightarrow \hat{\mathbb{C}}$ which is meromorphic on $\mathfrak{H}$ is called a* ***weakly modular form*** *of weight k for Γ' if*

$$f(z)|[\gamma]_k = f(z), \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma', \quad z \in \bar{\mathfrak{H}}.$$

Note that $T^N = \begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} \in \Gamma(N)$. So let $\gamma = T^N$ in the above definition, we have $f(z + N) = f(z)$. By Fourier analysis, f has the *q_N-expansion*

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q_N^n. \tag{3.8}$$

Definition 3.2.2.2. *The function f is said to be holomorphic (resp. vanishes) at infinity if $a_n = 0$ for $n < 0$ (resp. $n \leq 0$) in the q_N-expansion* (3.8).

Definition 3.2.2.3. *Let f be a meromorphic function on $\mathfrak{H}$ and let $\Gamma' \subset \Gamma$ be a congruence subgroup of level N. Let $k \in \mathbb{Z}$. Then f is called a* ***modular form*** *of weight k for Γ' if f satisfies the following conditions*

i. *f is holomorphic on $\mathfrak{H}$.*

ii. *f is weakly modular of weight k for Γ'.*

iii. *$f|[\gamma]_k$ is holomorphic at ∞ for all $\gamma \in \Gamma$.*

The $\mathbb{C}$-vector space of all modular forms of weight k for Γ' is denoted by $\mathrm{M}_k(\Gamma')$. Moreover, if condition (iii) *is replaced by*

iii'. *$f|[\gamma]_k$ vanishes at ∞ for all $\gamma \in \Gamma$,*

then f is called a ***cusp form*** *of weight k for Γ'. The $\mathbb{C}$-vector space of all cusp forms of weight k for Γ' is denoted by $\mathrm{S}_k(\Gamma')$.*

It is useful to point out some simple facts from the above definition

1. If $f \in \mathrm{M}_k(\Gamma')$ and $\Gamma'' \subset \Gamma'$ is a subgroup, then $f \in \mathrm{M}_k(\Gamma'')$.
2. If $f \in \mathrm{M}_{k_1}(\Gamma')$ and $g \in \mathrm{M}_{k_2}(\Gamma')$, then $fg \in \mathrm{M}_{k_1+k_2}(\Gamma')$.

The above statements still hold when we replace $\mathrm{M}_k(\Gamma')$ by $\mathrm{S}_k(\Gamma')$.

Proposition 3.2.2.4. *Let $s \in \mathbb{Q} \cup \{\infty\}$. The condition* (iii) *in Definition 3.2.2.3 depends only on the Γ'-equivalence class of s. More precisely, if $s = \gamma_1\infty$ and $\gamma_1\infty = \gamma\gamma_2\infty$ for some $\gamma_1, \gamma_2 \in \Gamma$ and $\gamma \in \Gamma'$, then the smallest power of q_N that occurs in the Fourier expansion of $f|[\gamma_1]_k$ and $f|[\gamma_2]_k$ is the same.*

Proof. Since $\gamma_1\infty = \gamma\gamma_2\infty$, we have $\gamma_1^{-1}\gamma\gamma_2$ fixes ∞. Therefore, $\gamma_1^{-1}\gamma\gamma_2 = \pm T^j$ for some $j \in \mathbb{Z}$. It follows that $\gamma_2 = \pm\gamma^{-1}\gamma_1 T^j$. Let $f(z)|[\gamma_1]_k = \sum_{n\in\mathbb{Z}} a_n q_N^n$. Then

$$f|[\gamma_2]_k = f(z)|[\pm\gamma^{-1}\gamma_1 T^j] = (\pm 1)^k (f|[\gamma_1]_k)|[T^j]_k,$$

where we have used $f|[\pm I]_k = (\pm 1)^k f$ and $f|[\gamma^{-1}]_k = f$.
Denote $g = f|[\gamma_1]_k$. Then

$$f(z)|[\gamma_2]_k = (\pm 1)^k g(z+j) = (\pm 1)^k \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n j/N} q_N^n.$$

The proposition now follows. □

Let f be weakly modular for Γ' and let $s \in \mathbb{Q} \cup \{\infty\}$. We write $s = \gamma\infty$ for some $\gamma \in \Gamma$. Then f is said to be *holomorphic* (resp. *vanishing*) at the cusp s if $f|[\gamma]_k$ is holomorphic (resp. vanishing) at ∞. The above proposition says that the choice of $\gamma \in \Gamma$ such that $s = \gamma\infty$ is not important. Thus, the condition (iii) in Definition 3.2.2.3 is really a condition about holomorphicity at each cusp of Γ'.

As before, the next step is to give explicit examples to show that modular forms and cusp forms for congruence subgroups do exist.
In what follows, we will use bold letters to denote vectors.

Definition 3.2.2.5. *Let N be a positive integer. Let $\boldsymbol{a} = (a_1, a_2)$ and $\boldsymbol{m} = (m_1, m_2)$ be in $(\mathbb{Z}/N\mathbb{Z})^2$. Let k be an integer greater than 2. The **Eisenstein series of level** N is defined by*

$$G_k^{\boldsymbol{a}}(z) = G_k^{\boldsymbol{a} \bmod N}(z) := \sum_{\substack{\boldsymbol{m}\in\mathbb{Z}^2 \\ \boldsymbol{m}\equiv\boldsymbol{a} \bmod N}} \frac{1}{(m_1 z + m_2)^k}, \quad z \in \mathfrak{H}. \tag{3.9}$$

If $\mathbf{a} = (0,0)$, we delete $\mathbf{m} = (0,0)$ in the sum (3.9). Note that when $\mathbf{a} = (0,0)$, $\mathbf{m} = (Nm, Nn)$ and the Eisenstein series of level N now becomes

$$G_k^{\mathbf{0}}(z) = N^{-k} \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(mz+n)^k} = N^{-k} G_k(z),$$

which is the Eisenstein series for Γ. Therefore, it is unnecessary to consider this case any more. So for Eisenstein series of level N, we suppose $\mathbf{a} \neq (0,0)$.

Proposition 3.2.2.6.

$$G_k^{\boldsymbol{a}} \in \mathrm{M}_k(\Gamma(N)), \quad G_k^{(0,a_2)} \in \mathrm{M}_k(\Gamma_1(N)).$$

Proof. We will prove the first statement only. The latter follows by the same argument. There are 3 conditions to check

i. $G_k^{\boldsymbol{a}}$ converges absolutely on $\mathfrak{H}$ and uniformly on any compact subset of $\mathfrak{H}$, hence is holomorphic on $\mathfrak{H}$.

ii. Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$. Consider

$$\begin{aligned} G_k^{\boldsymbol{a}}(z)|[\gamma]_k &= (cz+d)^{-k} \sum_{\boldsymbol{m}\equiv\boldsymbol{a} \bmod N} \frac{1}{\left(m_1 \frac{az+b}{cz+d} + m_2\right)^k} \\ &= \sum_{\boldsymbol{m}\equiv\boldsymbol{a} \bmod N} \frac{1}{[(m_1 a + m_2 c)z + (m_1 b + m_2 d)]^k}. \end{aligned}$$

Let $\boldsymbol{m'} = (m_1 a + m_2 c, m_1 b + m_2 d) = \boldsymbol{m}\gamma$. Since $\boldsymbol{m} \equiv \boldsymbol{a} \pmod N$, we have $\boldsymbol{m'} \equiv \boldsymbol{a}\gamma \pmod N$. Note that the map

$$\begin{aligned} f : \{\boldsymbol{m} : \boldsymbol{m} \equiv \boldsymbol{a} \ (\mathrm{mod}\, N)\} &\longrightarrow \{\boldsymbol{m'} : \boldsymbol{m'} \equiv \boldsymbol{a}\gamma \ (\mathrm{mod}\, N)\} \\ \boldsymbol{m} &\longmapsto \boldsymbol{m'} = \boldsymbol{m}\gamma \end{aligned}$$

is a bijection. Therefore,

$$\sum_{\boldsymbol{m}\equiv\boldsymbol{a} \bmod N} \frac{1}{[(m_1 a + m_2 c)z + (m_1 b + m_2 d)]^k} = G_k^{\boldsymbol{a}\gamma}(z).$$

It follows that

$$G_k^{\boldsymbol{a}}(z)|[\gamma]_k = G_k^{\boldsymbol{a}\gamma}(z). \tag{3.10}$$

If $\gamma \in \Gamma(N)$, then $\gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod N$. Thus,

$$G_k^{\boldsymbol{a}}(z)|[\gamma]_k = G_k^{\boldsymbol{a}}(z), \quad \gamma \in \Gamma(N).$$

iii. By (3.10), we know that $[\gamma]_k$ permutes $G_k^{\boldsymbol{a}}$ for $\gamma \in \Gamma$. Therefore, it suffices to show $G_k^{\boldsymbol{a}}$ is finite at ∞. We have

$$\lim_{z \to i\infty} G_k^{\boldsymbol{a}}(z) = \sum_{\substack{\boldsymbol{m} \equiv \boldsymbol{a} \bmod N \\ m_1 = 0}} \frac{1}{m_2^k} = \begin{cases} 0 & \text{if } a_1 \neq 0 \\ \sum_{n \equiv a_2 \bmod N} n^{-k} & \text{if } a_1 = 0 \end{cases}.$$

In either case, we always have $\lim_{z \to i\infty} G_k^{\boldsymbol{a}}(z) < \infty$ since $k \geq 2$.

The proposition now follows. □

Recall that the Dedekind η-function is defined by

$$\eta(z) = e^{2\pi i z/24} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z}), \quad z \in \mathfrak{H}.$$

It satisfies the following functional equation

$$\eta(-\frac{1}{z}) = \sqrt{\frac{z}{i}} \eta(z), \tag{3.11}$$

where $\sqrt{\ }$ denotes the principal branch of square root. For details about the Dedekind η-function, see [Kob84] and [Apo90]. We will use the Dedekind η-function to construct an example of cusp forms for congruence subgroups.

Proposition 3.2.2.7.

$$[\eta(z)\eta(2z)]^8 \in \mathrm{S}_8(\Gamma_0(2)).$$

Proof. Again, there are 3 conditions to check

i. Clearly, $f(z) := [\eta(z)\eta(2z)]^8$ is holomorphic on $\mathfrak{H}$.

ii. Note that $\Gamma_0(2)$ is generated by $-I, T$ and $ST^2S = \begin{bmatrix} -1 & 0 \\ 2 & -1 \end{bmatrix}$. It is trivial to check that f is invariant under $[-I]_8$ and $[T]_8$. For $[ST^2S]_8$, we write $\begin{bmatrix} -1 & 0 \\ 2 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 & -1 \\ 2 & 0 \end{bmatrix} T \begin{bmatrix} 0 & -1 \\ 2 & 0 \end{bmatrix}$ and check

$$\begin{aligned} f(z)| \begin{bmatrix} 0 & -1 \\ 2 & 0 \end{bmatrix}_8 &= 2^4 (2z^2)^{-8} \left(\eta\left(-\frac{1}{2z}\right) \eta\left(-\frac{1}{z}\right) \right)^8 \\ &= (2z^2)^{-4} \left(\sqrt{\frac{2z}{i}} \eta(2z) \sqrt{\frac{z}{i}} \eta(z) \right)^8 = (\eta(z)\eta(2z))^8 = f(z), \end{aligned}$$

where we have used the functional equation (3.11). So f is also invariant under $[ST^2S]_8$.

iii. The coset representatives for Γ modulo $\Gamma_0(2)$ are $I, S, ST^{-1}S$. So $\Gamma_0(2)$ has only one cusp at 0. Using the transformation (3.11), we see immediately that f vanishes at 0.

The proposition now follows. □

We recall the following definition

Definition 3.2.2.8. *A* ***Dirichlet character*** *mod m is defined to be a function $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ with the following properties*

i. $\chi(ab) = \chi(a)\chi(b)$ *for all* $a, b \in \mathbb{Z}$.

ii. $\chi(a) = \chi(b)$ *if* $a \equiv b \pmod{m}$.

iii. $\chi(a) \neq 0 \Longleftrightarrow \gcd(a, m) = 1$.

The ***conductor*** *of χ is the smallest positive integer n such that $\chi(a)$ depends only on a* mod n *when* $\gcd(a, n) = 1$. *The character χ is called* ***primitive*** *if $m = n$.*

For details about Dirichlet characters, see [Cop09]. Next, we will consider several ways to construct new modular forms out of given ones. In what follows, we denote χ to be a Dirichlet character and

$$\mathrm{M}_k(N, \chi) := \left\{ f \in \mathrm{M}_k(\Gamma_1(N)) : f|[\gamma]_k = \chi(d) f \quad \forall \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \right\}. \tag{3.12}$$

It is easy to see that $\mathrm{M}_k(N, \chi)$ is a subspace of $\mathrm{M}_k(\Gamma_1(N))$. A special case is when χ is trivial

$$\mathrm{M}_k(N, \chi_{\mathrm{triv}}) = \mathrm{M}_k(\Gamma_0(N)).$$

Let $\mathrm{GL}_2^+(\mathbb{Q})$ be a subgroup of $\mathrm{GL}_2(\mathbb{Q})$ consisting of all matrices of positive determinants. We now extend weight k operator $[\gamma]_k$ to be defined for all $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$.

$$f(z)|[\gamma]_k := (\mathrm{det}\gamma)^{k/2}(cz + d)^{-k} f(\gamma(z)), \quad \gamma \in \mathrm{GL}_2^+(\mathbb{Q}).$$

Proposition 3.2.2.9. ([Kob84], Proposition 17, p.127)

(a) *Let $\Gamma' \subset \Gamma$ be a congruence subgroup and $\alpha \in GL_2^+(\mathbb{Q})$. Set $\Gamma'' = \alpha^{-1}\Gamma'\alpha \cap \Gamma$. Then $\Gamma'' \subset \Gamma$ is a congruence subgroup. The map $f \longmapsto f|[\alpha]_k$ takes $\mathrm{M}_k(\Gamma')$ to $\mathrm{M}_k(\Gamma'')$ and takes $\mathrm{S}_k(\Gamma')$ to $\mathrm{S}_k(\Gamma'')$. In particular, if $f \in \mathrm{M}_k(\Gamma)$ and $g(z) = f(Nz)$, then $g \in \mathrm{M}_k(\Gamma_0(N))$.*

(b) *Let χ and χ_1 be Dirichlet characters modulo M and N respectively. If $f(z) = \sum_{n=0}^{\infty} a_n q^n \in \mathrm{M}_k(M, \chi)$ and define $f_{\chi_1}(z) := \sum_{n=0}^{\infty} a_n \chi_1(n) q^n$, then $f_{\chi_1} \in \mathrm{M}_k(MN^2, \chi\chi_1^2)$. If f is a cusp form, then so is f_{χ_1}.*

We usually refer to f_{χ_1} in the above proposition as the *twist of f by Dirichlet character χ_1*.

Proposition 3.2.2.10. ([Kob84], Proposition 28, p.137)

$$\mathrm{M}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathrm{M}_k(N, \chi),$$

where the sum is over all Dirichlet characters modulo N.

Later we will often work with the space $\mathrm{M}_k(\Gamma_1(4))$ and $\mathrm{M}_k(\Gamma_0(4))$. So it is convenient to state some of their properties here. We obtained the dimension formulae for $\mathrm{M}_k(\Gamma_1(4))$ and $\mathrm{M}_k(\Gamma_0(4))$ below by working out special cases of Theorem 3.5.1 and Theorem 3.6.1 in [Dia05]. These two general theorems contains several ideas which are too involved to discuss here. For details, see Chapter 3 of [Dia05].

Proposition 3.2.2.11. ([Kob84], Proposition 29, p.138) *Let k be a positive integer. Then*

$$\mathrm{M}_k(\Gamma_1(4)) = \begin{cases} \mathrm{M}_k(4,\chi_{\mathrm{triv}}) & \textit{if } k \textit{ is even} \\ \mathrm{M}_k(4,\chi) & \textit{if } k \textit{ is odd} \end{cases},$$

where χ_{triv} is the trivial character modulo 4 and χ is the unique non-trivial character modulo 4.

Proposition 3.2.2.12. *Let k be an integer. If $k \le 0$, then* $\dim\mathrm{M}_k(\Gamma_1(4)) = 0$. *If $k > 0$, then*

$$\dim\mathrm{M}_k(\Gamma_1(4)) = \begin{cases} \frac{k+2}{2} & \textit{if } k \textit{ is even} \\ \frac{k+1}{2} & \textit{if } k \textit{ is odd} \end{cases}.$$

Proposition 3.2.2.13. *Let k be an integer. Then*

$$\dim\mathrm{M}_k(\Gamma_0(4)) = \begin{cases} \frac{k+2}{2} & \textit{if } k \in 2\mathbb{N}\cup\{0\} \\ 0 & \textit{otherwise} \end{cases}.$$

3.2.3 Hecke operators

In previous subsections, we treated modular forms for Γ and its congruence subgroups separately. So it is natural to do the same here in defining Hecke operators on modular forms. However, on noting that

$$\Gamma = \Gamma(1) = \Gamma_1(1) = \Gamma_0(1),$$

we only need to define Hecke opertors on congruence subgroups of Γ. In what follows, we will denote Γ_1, Γ_2 to be congruence subgroups of Γ.
We start with a definition

Definition 3.2.3.1. *Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. The* ***double coset*** *$\Gamma_1\alpha\Gamma_2$ in $\mathrm{GL}_2^+(\mathbb{Q})$ is defined to be*

$$\Gamma_1\alpha\Gamma_2 := \{\gamma_1\alpha\gamma_2 \in \mathrm{GL}_2^+(\mathbb{Q}) : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}.$$

We now let Γ_1 act on the double coset $\Gamma_1\alpha\Gamma_2$ by left multiplication, which partitions it into orbits. The set of such orbits is called the *orbit space*. Next we will show that the orbit space has finite cardinality.

Proposition 3.2.3.2. ([Dia05], Lemmas 5.1.1, 5.1.2, p.164) *Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 \le \Gamma_2$. Define*

$$\begin{aligned} h : \Gamma_2 &\longrightarrow \Gamma_1\alpha\Gamma_2 \\ \gamma_2 &\longmapsto \alpha\gamma_2. \end{aligned}$$

Then h induces a bijection from the set of cosets of $\Gamma_3 \setminus \Gamma_2$ to the orbit space $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$.

Corollary 3.2.3.3. *Let Γ_1 act on $\Gamma_1\alpha\Gamma_2$ by left multiplication. Then the number of orbits is finite.*

Proof. Let Γ_3 be defined as in Proposition 3.2.3.2. Since $\alpha^{-1}\Gamma_1\alpha \cap \Gamma, \Gamma_2$ are congruence subgroups, so is $\Gamma_3 = (\alpha^{-1}\Gamma_1\alpha \cap \Gamma) \cap \Gamma_2$. In particular,

$$[\Gamma : \Gamma_2] < \infty, \quad [\Gamma : \Gamma_3] < \infty.$$

It follows that

$$[\Gamma_2 : \Gamma_3] = \frac{[\Gamma : \Gamma_3]}{[\Gamma : \Gamma_2]} < \infty.$$

□

Definition 3.2.3.4. *Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and $f \in \mathrm{M}_k(\Gamma_1)$. We define the weight k* double coset operator $[\Gamma_1\alpha\Gamma_2]_k$ *on f to be*

$$f|[\Gamma_1\alpha\Gamma_2]_k := \sum_j f|[\beta_j]_k,$$

where β_j runs through the set of orbit representatives for $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$.

It is not straightforward to see that the above definition is well-defined, as the sum might depend on the set of representatives. So we spend some time in showing that it is in fact not the case.
Now suppose that $\Gamma_1\beta_{j_1} = \Gamma_1\beta_{j_2}$ for $\beta_{j_1} = \gamma_{1,j_1}\alpha\gamma_{2,j_1}$ and $\beta_{j_2} = \gamma_{1,j_2}\alpha\gamma_{2,j_2}$ $(\gamma_{i,j_k} \in \Gamma_i)$. Then $\alpha\gamma_{2,j_1} \in \Gamma_1\alpha\gamma_{2,j_2}$. Since $f \in M_k(\Gamma_1)$, we have

$$f|[\beta_{j_1}]_k = f|[\alpha\gamma_{2,j_1}]_k = f|[\alpha\gamma_{2,j_2}]_k = f|[\gamma_{1,j_2}\alpha\gamma_{2,j_2}]_k = f|[\beta_{j_2}]_k.$$

as expected.

Proposition 3.2.3.5. *If $f \in \mathrm{M}_k(\Gamma_1)$, then $f|[\Gamma_1\alpha\Gamma_2]_k \in \mathrm{M}_k(\Gamma_2)$. If $f \in \mathrm{S}_k(\Gamma_1)$, then $f|[\Gamma_1\alpha\Gamma_2]_k \in \mathrm{S}_k(\Gamma_2)$.*

Proof. We will prove the first statement only. The second follows by a similar argument. Let $\gamma \in \Gamma_2$. If $\{\beta_j\}$ is the set of representatives of $\Gamma_1\alpha\Gamma_2$ modulo Γ_1, then so is $\{\beta_j\gamma\}$. Hence

$$(f|[\Gamma_1\alpha\Gamma_2]_k)\,|[\gamma]_k = \sum_j f|[\beta_j\gamma]_k = f|[\Gamma_1\alpha\Gamma_2]_k.$$

□

Three special cases of double coset operators are

1. $\Gamma_1 \supset \Gamma_2$: Let $\alpha = I$. Then $f|[\Gamma_1\alpha\Gamma_2]_k = f$. This gives an *inclusion* which injects $\mathrm{M}_k(\Gamma_1)$ into $\mathrm{M}_k(\Gamma_2)$.

2. $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$: Here $f|[\Gamma_1\alpha\Gamma_2]_k = f|[\alpha_k]$. This gives a *translation* from $\mathrm{M}_k(\Gamma_1)$ to $\mathrm{M}_k(\Gamma_2)$. It follows that this is also an isomorphism.

3. $\Gamma_1 \subset \Gamma_2$: Let $\alpha = I$ and $\{\gamma_j\}$ be the set of representatives for $\Gamma_1 \setminus \Gamma_2$. Then $f|[\Gamma_1\alpha\Gamma_2]_k = \sum_j f|[\gamma_j]_k$. This is a *trace map* which projects $\mathrm{M}_k(\Gamma_1)$ onto its subspace $\mathrm{M}_k(\Gamma_2)$.

The following argument shows that the general double coset operator is a composition of the above special ones. Let $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$, $\Gamma_4 = \alpha\Gamma_3\alpha^{-1} = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$. We have $\Gamma_1 \supset \Gamma_4$, $\alpha^{-1}\Gamma_4\alpha = \Gamma_3$ and $\Gamma_3 \subset \Gamma_2$. It follows from Proposition 3.2.3.2 that the following composition is the general double coset operator

$$f \longmapsto f \longmapsto f|[\alpha]_k \longmapsto \sum_j f|[\gamma_j]_k.$$

Next, we will define the first type of Hecke operator.

Definition 3.2.3.6. *Let N be a positive integer, $d \in (\mathbb{Z}/N\mathbb{Z})^*$ and $f \in \mathrm{M}_k(\Gamma_1(N))$. Let $\alpha \in \Gamma_0(N)$ be such that $\alpha \equiv \begin{bmatrix} * & * \\ * & d \end{bmatrix}$* (mod N). *The* ***diamond operator*** *$\langle d \rangle$ is the double coset operator $f|[\Gamma_1(N)\alpha\Gamma_1(N)]_k$.*

As noted before, $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$. Therefore, the $\langle d \rangle$ is a translation from $\mathrm{M}_k(\Gamma_1(N))$ to itself. So we can rewrite $\langle d \rangle$ as

$$\langle d \rangle f = f|[\alpha]_k, \quad \alpha \in \Gamma_0(N),\, \alpha \equiv \begin{bmatrix} * & * \\ * & d \end{bmatrix} \pmod{N}.$$

It follows that the space $\mathrm{M}_k(N.\chi)$ defined by (3.12) can be rewritten as

$$\mathrm{M}_k(N,\chi) = \{f \in \mathrm{M}_k(\Gamma_1(N)) : \langle d \rangle f = \chi(d)f, d \in \mathbb{Z}\}.$$

This means that $\mathrm{M}_k(N.\chi)$ is a χ-eigenspace of $\langle d \rangle$. Hence, $\langle d \rangle$ preserves the decomposition $\mathrm{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathrm{M}_k(N,\chi)$. Now we consider the second type of Hecke operator.

Definition 3.2.3.7. *Let N be a positive integer and let $f \in \mathrm{M}_k(\Gamma_1(N))$. The* ***$T_p$ operator*** *is defined by*

$$T_p f = f \left|\left[\Gamma_1(N) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma_1(N)\right]_k\right., \quad p \text{ prime.}$$

Proposition 3.2.3.8. ([Dia05], Proposition 5.2.4, p.173) *Let $d, e \in \mathbb{Z}/N\mathbb{Z}$ and p, q be primes. Then*

i. $\langle d \rangle T_p = T_p \langle d \rangle$.

ii. $\langle d \rangle \langle e \rangle = \langle e \rangle \langle d \rangle$.

iii. $T_p T_q = T_q T_p$.

Let N be a positive integer. So far we have defined two types of Hecke operators: $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^*$ and T_p for p a prime number. Now we will extend these to operators $\langle n \rangle$ and T_n for any $n \in \mathbb{Z}_+$.
For $n \in \mathbb{Z}_+$ with $\gcd(n, N) = 1$, the definition for $\langle n \rangle$ is the same as the case $n \in (\mathbb{Z}/N\mathbb{Z})^*$.

If $\gcd(n, N) > 1$, then $\langle n\rangle = 0$. It follows from Proposition 3.2.3.8 that $\langle n\rangle$ is completely multiplicative.
Next we define T_n for arbitrary $n \in \mathbb{Z}_+$. Set

$$\begin{aligned} &T_1 = 1, \\ &T_p^r = T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}, \quad r \geq 2, \\ &T_n = \prod T_{p_i^{e_i}}, \quad n = \prod p_i^{e_i}. \end{aligned}$$

It also follows from Proposition 3.2.3.8 that T_n is multiplicative (not completely). The effect of T_n on $\mathrm{M}_k(\Gamma_1(N))$ is as follows

Proposition 3.2.3.9. ([Dia05], Proposition 5.3.1, p.179) *Let $f \in \mathrm{M}_k(\Gamma_1(N))$ whose q-expansion is $f(z) = \sum_{n=0}^{\infty} a_n q^n$ and $n, d \in \mathbb{Z}_+$. Suppose $T_n f(z) = \sum_{m=0}^{\infty} b_m q^m$ and $\langle d\rangle f = \sum_{m=0}^{\infty} a_m^{(d)} q^m$. Then*

$$b_m = \sum_{d|\gcd(m,n)} d^{k-1} a^{(d)}_{mn/d^2}.$$

Suppose further that $f \in \mathrm{M}_k(N, \chi)$. Then $T_n f \in \mathrm{M}_k(N, \chi)$ and

$$b_m = \sum_{d|\gcd(m,n)} \chi(d) d^{k-1} a_{mn/d^2}.$$

The definition of T_{p^r} is chosen so that the generating function for T_n captures the Euler product factorisation as that of the Riemann zeta function. In particular,

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_p \frac{1}{1 - T_p p^{-s} + \langle p\rangle p^{k-1-2s}}.$$

For details, see [Kob84], pp.156 - 158 and [Dia05], p.179.

One of the most important results is the following proposition which we will use extensively later.

Proposition 3.2.3.10. ([Kob84], Proposition 40, p.163) *Suppose $f \in \mathrm{M}_k(N, \chi)$ is an eigenform for all of the operators T_n with eigenvalues $\lambda_n, n \in \mathbb{Z}_+$. Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$. Then $a_n = \lambda_n a_1$ for $n \in \mathbb{Z}_+$. In addition, $a_1 \neq 0$ unless $k = 0$ in which case f is constant. If $a_0 \neq 0$, then λ_n is given by*

$$\lambda_n = \sum_{d|n} \chi(d) d^{k-1}.$$

As preparation for the next subsection, we will prove the following lemma

Lemma 3.2.3.11. *Let $\Gamma' \subset \Gamma_1(N)$ be a congruence subgroup, $f \in \mathrm{M}_k(\Gamma')$ and $n \in \mathbb{Z}_+$. Let $\{f_1, \dots, f_s\}$ be the set of all basis eigen-forms for T_2. Suppose $T_2 f_i = \lambda_i f_i$ for all $i \in \{1, \dots, s\}$ and the eigen-values λ_i's are distinct. Then f_i is an eigenform for T_n for all $i \in \{1, \dots, s\}$.*

Proof. Let p be a prime. Then $T_2 T_p f_i = T_p T_2 f_i = T_p(\lambda_i f_i) = \lambda_i T_p f_i$. So $T_p f_i \in \mathrm{span}\{f_1, \dots, f_s\}$, say $T_p f_i = \sum_{j=1}^{s} c_j f_j$, where $c_j \in \mathbb{C}$. We then have $T_2 T_p f_i = T_2(\sum_j c_j f_j) = \sum_j c_j \lambda_j f_j$. So $\lambda_i(\sum_j c_j f_j) = \sum_j c_j \lambda_j f_j$. It follows that $\sum_j c_j(\lambda_i - \lambda_j) f_j = 0$. Since the f_j's are linearly independent and λ_j's are distinct, we must have $c_j = 0$ for $j \neq i$. Therefore, f_i is an eigenform for T_p. Similarly, f_i is an eigenform for all diamond operators $\langle p\rangle$. Thus f_i is an eigenform for T_n, where $n \in \mathbb{N}$ is arbitrary. □

3.2.4 The theta function and applications to sums of even squares

Definition 3.2.4.1. *The **theta function** is defined by*

$$\theta(z) := \sum_{n\in\mathbb{Z}} q^{n^2}, \quad z \in \mathfrak{H}, q = e^{2\pi i z}.$$

Now suppose

$$\theta^k(z) = \sum_{n\in\mathbb{Z}} c_n q^n.$$

Let $r_k(n)$ denote the number of ways that n can be represented as the sum of k squares. Then clearly, $r_k(n) = c_n$. So the problem of finding $r_k(n)$ boils down to calculating c_n. In principle, we can do this using the theory of modular forms, in particular the theta function. In this subsection, we give explicit formulae for the cases when $k = 2, 4$. The proofs are based on Koblitz's ideas in [Kob84]. We note that more elementary proofs are also available for these facts (see [Nat00] or [Mor06]).

We first introduce some notation. We use $\left(\frac{c}{d}\right)$ to denote the Kronecker symbol and define

$$\epsilon_d := \sqrt{\left(\frac{-1}{d}\right)}, \quad d \text{ odd},$$

where $\sqrt{}$ is the principal branch of square root.

Finally, we define the *factor of automorphy* to be

$$j(\gamma, z) := \left(\frac{c}{d}\right)\epsilon_d^{-1}\sqrt{cz+d}, \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(4),\ z \in \mathfrak{H}.$$

Theorem 3.2.4.2. ([Kob84], Theorem, p.148) *Let $\gamma \in \Gamma_0(4)$ and $z \in \mathfrak{H}$. The theta function satisfies the transformation*

$$\theta(\gamma z) = j(\gamma, z)\theta(z),$$

where $j(\gamma, z)$ is the automorphy factor.

Corollary 3.2.4.3.

$$\theta^{2k} \in \mathrm{M}_k(4, \chi_{-1}^k),$$

where χ_{-1} is the Dirichlet character modulo 4 defined by

$$\chi_{-1}(n) := \left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$

Proof. Clearly, $\theta^{2k} \in M_k(\Gamma_1(4))$. Now let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(4)$. Using Theorem 3.2.4.2, we have

$$\theta^{2k}(\gamma z) = j^{2k}(\gamma, z)\theta^{2k}(z) = \left(\frac{c}{d}\right)^{2k}\left(\frac{-1}{d}\right)^{k}(cz+d)^k\theta^{2k}(z) = \chi_{-1}^k(d)(cz+d)^k\theta^{2k}(z).$$

□

Proposition 3.2.4.4. *Let n be a positive integer. Then*

$$r_2(n) = 4 \sum_{\substack{d|n \\ d \text{ odd}}} \left(\frac{-1}{d}\right).$$

Proof. By Corollary 3.2.4.3, $\theta^2 \in \mathrm{M}_1(4, \chi_{-1})$. Note that $\mathrm{M}_1(4, \chi_{-1}) = \mathrm{M}_1(\Gamma_1(4))$ by Proposition 3.2.2.11. But $\mathrm{M}_k(\Gamma_1(4))$ is one dimensional by Proposition 3.2.2.12. It follows that $\mathrm{M}_k(\Gamma_1(4))$ is spanned by θ^2 and θ^2 is an eigenform for all Hecke operator T_n. The q-expansion for θ^2 for the first few terms is

$$\theta^2 = 1 + 4q + \dots .$$

So that $a_0 = 1 \neq 0$ and $a_1 = 4$. Let $N = 4$ and $\chi(d) = \chi_{-1}$ for d odd in Proposition 3.2.3.10, we have

$$r_2(n) = 4 \sum_{d|n} \chi(d) d^{k-1} = 4 \sum_{\substack{d|n \\ d \ odd}} \left(\frac{-1}{d}\right).$$

□

Corollary 3.2.4.5. *Let p be an odd prime. Then*

$$r_2(p) = \begin{cases} 8 & \textit{if } p \equiv 1 \ (\textit{mod } 4), \\ 0 & \textit{if } p \equiv 3 \ (\textit{mod } 4). \end{cases}$$

Proof. We have

$$r_2(p) = 4\left(1 + \left(\frac{-1}{p}\right)\right) = \begin{cases} 8 & \text{if } p \equiv 1 \pmod 4, \\ 0 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

□

Proposition 3.2.4.6. *Let n be a positive integer. Then*

$$r_4(k) = \begin{cases} 8\sigma_1(n) & \textit{if } n \textit{ is odd}, \\ 24\sigma_1(m) & \textit{if } n = 2^s m \textit{ where } m \textit{ is odd, } s \in \mathbb{Z}_+. \end{cases}$$

Proof. First, we define

$$F(z) := \sum_{n \text{ odd}} \sigma_1(n) q^n = q + 4q^3 + \dots, \quad z \in \mathfrak{H}.$$

Also note that

$$\theta^4 = 1 + 8q + \dots \in \mathrm{M}_2(4, \chi_{-1}^2)$$

by Corollary 3.2.4.3. But $\mathrm{M}_2(4, \chi_{-1}^2) = \mathrm{M}_2(4, \chi_{\text{triv}}) = \mathrm{M}_2(\Gamma_0(4))$. So $\theta^4 \in \mathrm{M}_2(\Gamma_0(4))$. It can easily be shown that $F \in \mathrm{M}_2(\Gamma_0(4))$ and $\{F, \theta^4\}$ is linearly independent. But $\mathrm{M}_2(\Gamma_0(4))$ has dimension 2 by Proposition 3.2.2.12. It follows that $\{F, \theta^4\}$ is a basis for $\mathrm{M}_2(\Gamma_0(4))$. Applying Proposition 3.2.3.9, we have

$$T_2 F = 0,$$
$$T_2 \theta^4 = \theta^4 + 16F.$$

It follows that $\{F, \theta^4 + 16F\}$ forms an eigen-basis for T_2. Now we use Lemma 3.2.3.11 to deduce that these are also eigenforms for T_n, where n is arbitrary. Denote

$$\theta^4(z) + F(z) = \sum_{n=0}^{\infty} a_n q^n.$$

It follows that

$$a_n = \begin{cases} r_4(n) + 16\sigma_1(n) & \text{if } n \text{ is odd,} \\ r_4(n) & \text{if } n \text{ is even.} \end{cases}$$

When n is odd, $\lambda_n = \sigma_1(n)$. Apply Proposition 3.2.3.10 to $\theta^4 + 16F$, we have

$$r_4(n) + 16\sigma_1(n) = \lambda_1 a_1 = 24\sigma_1(n).$$

Thus,

$$r_4(n) = 8\sigma_1(n), \quad n \text{ odd.}$$

When $n = 2^s m$, $\lambda_n = \sigma_1(m)$. Apply Proposition 3.2.3.10 to $\theta^4 + 16F$, we have

$$r_4(n) = \lambda_1 a_1 = 24\sigma_1(m).$$

Now the proposition follows. □

Corollary 3.2.4.7. *The form $x^2 + y^2 + z^2 + t^2$ is universal. That is, it represents all natural numbers.*

Proof. It follows from the above proposition that $r_4(n) > 0$ for all $n \in \mathbb{N}$. □

3.3 Modular forms of half integral weights

3.3.1 Four-sheeted covering of $\mathbf{GL}_2^+(\mathbb{Q})$

Let T be the set of fourth-roots of unity, i.e, $T = \{\pm 1, \pm i\}$. We define

$$G := \left\{ (\alpha, \phi(z)) : \alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}), \phi(z)^2 = t\frac{cz+d}{\sqrt{\det \alpha}}, t \in \{\pm 1\} \right\}.$$

Loosely speaking, G is 4 times as big as $\mathrm{GL}_2^+(\mathbb{Q})$. It contains 4 branches of square-root of $\pm(cz+d)$. We call G the *four-sheeted covering of* $\mathrm{GL}_2^+(\mathbb{Q})$.
We define a binary relation on G as follows

$$(\alpha, \phi(z)) \cdot (\beta, \psi(z)) = (\alpha\beta, \phi(\beta z)\psi(z)).$$

It is straight-forward to check that $(G, \cdot)$ forms a group. Next, we define

$$P : G \longrightarrow \mathrm{GL}_2^+(\mathbb{Q}) : (\alpha, \phi(z)) \longmapsto \alpha,$$

which is a *projection* from G onto $\mathrm{GL}_2^+(\mathbb{Q})$. Clearly, P is a homomorphism. We denote

$$G^1 := P^{-1}(\Gamma),$$

where Γ is the full modular group $\mathrm{SL}_2(\mathbb{Z})$. Then G^1 is a subgroup of G.
Now let $\xi = (\alpha, \phi(z)) \in G$, we define the action of ξ on $\mathfrak{H}$ to be the same as α on $\mathfrak{H}$, i.e, $\xi z := \alpha z$. If f is a function on $\mathfrak{H}$ and $k \in \mathbb{Z}$, then an operator $[\xi]_{k/2}$ of weight $k/2$ is defined by

$$f(z)|[\xi]_{k/2} := f(\xi z)\phi(z)^{-k} = f(\alpha z)\phi(z)^{-k}.$$

It follows that

$$f|[\xi_1\xi_2]_{k/2} = \big(f|[\xi_1]_{k/2}\big)\,[\xi_2]_{k/2}.$$

This gives an action of G on the space of such functions.
Next, let $\Gamma' \subset \Gamma_0(4)$ be a subgroup, so that the automorphy factor $j(\gamma, z)$ is defined for $\gamma \in \Gamma'$. We define

$$\widetilde{\Gamma}' := \{(\gamma, j(\gamma, z)) : \gamma \in \Gamma'\} \leq G.$$

Note that $P|_{\Gamma'}$ is an isomorphism. In particular, $\widetilde{\Gamma}_0(4) \cong \Gamma_0(4)$. The inverse of $P|_{\widetilde{\Gamma}_0(4)}$ is then

$$L : \Gamma_0(4) \longrightarrow \widetilde{\Gamma}_0(4) : \gamma \longmapsto \widetilde{\gamma} = (\gamma, j(\gamma, z)),$$

which is called a *lifting* of P.
In the next subsection, we will use the above notions to define modular forms of half integral weight for $\widetilde{\Gamma}$ and congruence subgroup.

3.3.2 Modular forms of half integral weights

Definition 3.3.2.1. *Let k be an odd integer and Γ' be of finite index in $\Gamma_0(4)$. Let $\widetilde{\Gamma}', \widetilde{\Gamma}_0(4)$ be as in previous subsection. A function $f : \bar{\mathfrak{H}} \longrightarrow \hat{\mathbb{C}}$ which is meromorphic on $\mathfrak{H}$ is called a **weakly modular form of weight** $k/2$ for $\widetilde{\Gamma}'$ if*

$$f(z)|[\widetilde{\gamma}]_{k/2} = f(z), \quad \gamma = (\gamma, j(\gamma, z)) \in \widetilde{\Gamma}', \quad z \in \bar{\mathfrak{H}},$$

where $j(\gamma, z)$ is the automorphy factor.

To define modular form of half integral weight, as before, we need the notions of holomorphicity and vanishing at infinity. Since we have a slightly different definition for weakly modular forms, some explanation will be needed for these notions.
Note that the condition $[\Gamma_0(4) : \Gamma'] < \infty$ implies $[\Gamma : \Gamma'] < \infty$. If we denote

$$\widetilde{\Gamma}'_\infty := \{\widetilde{\gamma} \in \widetilde{\Gamma}' : \widetilde{\gamma}\infty = \infty\},$$

then there must be some $M \in \mathbb{Z}_+$ such that

$$\widetilde{\Gamma}'_\infty = \begin{cases} \left\{\left(\pm\begin{bmatrix} 1 & M \\ 0 & 1\end{bmatrix}^k, 1\right)\right\}_{k\in\mathbb{Z}} & \text{if } -1 \in \Gamma', \\ \left\{\left(\begin{bmatrix} 1 & M \\ 0 & 1\end{bmatrix}^k, 1\right)\right\}_{k\in\mathbb{Z}} \text{ or } \left\{\left(-\begin{bmatrix} 1 & M \\ 0 & 1\end{bmatrix}^k, 1\right)\right\}_{k\in\mathbb{Z}} & \text{if } -1 \notin \Gamma'. \end{cases}$$

But

$$f(z)\left|\left[\left(\pm\begin{bmatrix} 1 & M \\ 0 & 1\end{bmatrix}, 1\right)\right]_{k/2} = \Big(f(z)|[\pm\widetilde{1}]_{k/2}\Big)\right|\left[\left(\begin{bmatrix} 1 & M \\ 0 & 1\end{bmatrix}, 1\right)\right]_{k/2} = f(z+M).$$

So in both cases, f is invariant under the translation $z \longmapsto z + M$. So by Fourier analysis, f has a q_M expansion

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q_M^n, \quad q_M = e^{2\pi i z/M}. \tag{3.13}$$

Definition 3.3.2.2. *The function f is said to be holomorphic (resp. vanishes) at infinity if $a_n = 0$ for $n < 0$ (resp. $n \leq 0$) in the q_M-expansion* (3.13).

With the above definition, we can now proceed as in Subsection 3.2.2.

Definition 3.3.2.3. *Let f be a meromorphic function on $\mathfrak{H}$ and let Γ' be of finite index in $\Gamma_0(4)$. Let $\widetilde{\Gamma}', \widetilde{\Gamma}_0(4), G^1$ be as in the previous subsection. Let k be an odd integer. Then f is called a* ***modular form of weight*** *$k/2$ for $\widetilde{\Gamma}'$ if f satisfies the following conditions*

i. *f is holomorphic on $\mathfrak{H}$.*

ii. *f is weakly modular of weight k for $\widetilde{\Gamma}'$.*

iii. *$f|[\widetilde{\gamma}]_k$ is holomorphic at ∞ for all $\widetilde{\gamma} \in G^1$.*

The set of all modular forms of weight $k/2$ for $\widetilde{\Gamma}'$ is denoted by $\mathrm{M}_{k/2}(\widetilde{\Gamma}')$. Moreover, if condition (iii) *is replaced by*

iii'. *$f|[\widetilde{\gamma}]_k$ vanishes at ∞ for all $\widetilde{\gamma} \in G^1$,*

then f is called a ***cusp form of weight*** *$k/2$ for $\widetilde{\Gamma}'$. The set of all cusp forms of weight $k/2$ for $\widetilde{\Gamma}'$ is denoted by $\mathrm{S}_{k/2}(\widetilde{\Gamma}')$.*

Note that for each cusp $s \in \mathbb{Q} \cup \{\infty\}$, there is a $\widetilde{\gamma} \in G^1$ such that $s = \widetilde{\gamma}\infty$. Using similar arguments as before, we can show that the conditions (iii) and (iii') above depend only on the $\widetilde{\Gamma}'$-equivalence class of s (see [Kob84], Proposition 2, p.181).
The following proposition relates the spaces $\mathrm{M}_{k/2}(\widetilde{\Gamma}_0(4), \chi)$ and $\mathrm{S}_{k/2}(\widetilde{\Gamma}_0(4), \chi)$ when $k \in 2\mathbb{Z}$ to familiar spaces from the previous section.

Proposition 3.3.2.4. ([Kob84], Proposition 3, p.183) *Let $4 \mid N$ and $k \in 2\mathbb{Z}$. Then*

$$\mathrm{M}_{k/2}(\widetilde{\Gamma}_0(4), \chi) = \mathrm{M}_{k/2}(N, \chi_{-1}^{k/2}\chi), \quad \mathrm{S}_{k/2}(\widetilde{\Gamma}_0(4), \chi) = \mathrm{S}_{k/2}(N, \chi_{-1}^{k/2}\chi).$$

Next, we will describe the structure of $\mathrm{M}_{k/2}(\widetilde{\Gamma}_0(4))$. If $P \in \mathbb{C}[X_1, \dots, X_n]$ and each X_i are assigned to weight w_i, then the monomial $X_1^{k_1} \dots X_n^{k_n}$ is said to have weight $w = \sum_{i=1}^n k_i w_i$, and we say P has pure weight w if each monomial in P has weight w.

Proposition 3.3.2.5. ([Kob84], Proposition 4, p.184) *Let $\theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2}$ and $F(z) = \sum_{n=1}^{\infty} \sigma_1(n) q^n$, where $q = e^{2\pi i z}$. Assign weight $1/2$ to θ and weight 2 to F. Then $\mathrm{M}_{k/2}(\widetilde{\Gamma}_0(4))$ is the space of all polymonials in $\mathbb{C}[\theta, F]$ having pure weight $k/2$.*

Corollary 3.3.2.6. ([Kob84], Corollary, p.184)

$$\dim \mathrm{M}_{k/2}(\widetilde{\Gamma}_0(4)) = 1 + \left\lfloor \frac{k}{4} \right\rfloor.$$

Now we will modify the definition for normalised Eisenstein series from Subsection 3.2.1 to give an example of modular forms of half integral weight. Recall that the normalised Eisenstein series is defined by

$$E_k(z) := \sum_{\substack{m,n\in\mathbb{Z}\\ \gcd(m,n)=1}} (mz+n)^{-k}, \quad k \in 2\mathbb{Z},\, k \geq 4. \tag{3.14}$$

For each pair $(m,n) \in \mathbb{Z}^2$ with $\gcd(m,n) = 1$, we can complete it to a matrix $\gamma = \begin{bmatrix} a & b \\ m & n \end{bmatrix} \in \Gamma$. We denote $\Gamma_\infty := \left\{\pm \begin{bmatrix} 1 & j \\ 0 & 1 \end{bmatrix}, j \in \mathbb{Z}\right\}$ and define an equivalence relation on Γ as follows: $\gamma_1, \gamma_2 \in \Gamma$ are equivalent iff $\gamma_1 = \alpha\gamma_2$ for some $\alpha \in \Gamma_\infty$. This simply means that γ_1, γ_2 have the same bottom row (m,n) up to a sign. We can now rewrite (3.14) as

$$E_k(z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} J_k(\gamma,z)^{-1}, \quad k \in 2\mathbb{Z},\, k \geq 4,$$

where $J_k(\gamma, z) := (mz+n)^k$, which is the automorphy factor of modular forms of integral weight k. The condition $\gamma \in \Gamma_\infty \setminus \Gamma$ says that the sum is over all equivalence classes of γ. Notice that $\Gamma_0(4)_\infty = \Gamma_\infty$. We are now ready to modify the normalised Eisenstein series (3.14) to construct an example of modular forms of half integral weights.

Definition 3.3.2.7. *Let k be an odd integer and $k \geq 5$. We define*

$$E_{k/2}(z) := \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(4)} J_k(\gamma,z)^{-1}.$$

We also define

$$F_{k/2}(z) := E_{k/2}\left|\left[\left(\begin{bmatrix} 0 & -1 \\ 4 & 0 \end{bmatrix}, \sqrt{2z}\right)\right]_{k/2}\right. .$$

and call $F_{k/2}$ the *companion Eisenstein series* of $E_{k/2}$.

Proposition 3.3.2.8. ([Kob84], pp.186 – 187)

$$E_{k/2}, F_{k/2} \in \mathrm{M}_{k/2}(\widetilde{\Gamma}_0(4)).$$

Definition 3.3.2.9. *A **Dirichlet L-series** is a function of the form*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where χ is a Dirichlet character.

Definition 3.3.2.10. *A **quadratic field** is a field of the form $\mathbb{Q}(\sqrt{l})$, where $l \in \mathbb{Z}$. The **discriminant** of $\mathbb{Q}(\sqrt{l})$ is defined by*

$$D := \begin{cases} l & \text{if } l \equiv 1 \pmod 4, \\ 4l & \text{otherwise.} \end{cases}$$

*The **corresponding character** for $\mathbb{Q}(\sqrt{l})$ is defined by*

$$\chi_D(\cdot) := \left(\frac{D}{\cdot}\right),$$

where $\left(\frac{a}{b}\right)$ is the Kronecker symbol.

Proposition 3.3.2.11. ([Kob84], Proposition 6, p.193) *Let $\lambda = (k-1)/2 \geq 2$. Then*

$$H_{k/2} := \zeta(1-2\lambda)(E_{k/2} + (1+i^k)2^{-k/2}F_{k/2}) \in \mathrm{M}_{k/2}(\widetilde{\Gamma}_0(4))$$

has the following property: if $D = (-1)^\lambda l$ or $(-1)^\lambda 4l, l > 0$, is the discriminant of a quadratic field and χ_D is the corresponding character, then the $|D|$-th q-expansion coefficient of $H_{k/2}$ equals $L(1-\lambda, \chi_D)$.

Corollary 3.3.2.12. *Let D be the discriminant of a real quadratic field and χ_D the corresponding character. Then*

$$r_5(D) = 120L(-1,\chi_D) + 20 \sum_{\substack{|j|<\sqrt{D} \\ D-j^2 \text{ odd}}} \sigma_1(D-j^2).$$

Proof. We consider the space $\mathrm{M}_{5/2}(\widetilde{\Gamma}_0(4))$. By Corollary 3.3.2.6, $\mathrm{M}_{5/2}(\widetilde{\Gamma}_0(4))$ has dimension 2. By Theorem 3.2.4.2, $\theta^5 \in \mathrm{M}_{5/2}(\widetilde{\Gamma}_0(4))$. Note also that $\theta F \in \mathrm{M}_{5/2}(\widetilde{\Gamma}_0(4))$. But θ^5 and θF are linearly independent. So $\{\theta^5, \theta F\}$ forms a basis for $\mathrm{M}_{5/2}(\widetilde{\Gamma}_0(4))$. By Proposition 3.3.2.11, the function $H_{5/2} \in \mathrm{M}_{5/2}(\widetilde{\Gamma}_0(4))$. Therefore,

$$H_{5/2} = a\theta^5 + b\theta F$$

for some $a, b \in \mathbb{C}$. We have

$$\begin{aligned} H_{5/2}(z) &= \frac{1}{120} - \frac{1}{6}q + \dots \\ \theta^5(z) &= 1 + 10q + \dots \\ (\theta F)(z) &= q + 2q^2 + \dots. \end{aligned}$$

On comparing the constant coefficients and the coefficients of the first powers of q, we derive

$$H_{5/2} = \frac{1}{120}\theta^5 - \frac{1}{6}\theta F.$$

Next we use Proposition 3.3.2.11 to obtain

$$L(-1,\chi_D) = \frac{1}{120}r_5(D) - \frac{1}{6} \sum_{\substack{|j|<\sqrt{D} \\ D-j^2 \ odd}} \sigma_1(D-j^2).$$

The proposition now follows. □

The following is the counterpart of Proposition 3.2.2.9.

Proposition 3.3.2.13. ([Geh11], Fact $9, 10$, p.11) *Let k be an odd integer, $N \in 4\mathbb{Z}$ and $f = \sum_{n=0}^{\infty} a_n q^n \in \mathrm{M}_{k/2}(N, \chi)$. Then*

i. *$f(Mz) \in \mathrm{M}_{k/2}(NM, \left(\frac{4M}{\cdot}\right)\chi)$.*

ii. *If ψ is a primitive character of conductor M, then $f_\psi(z) := \sum_{n=0}^{\infty} \psi(n) a_n q^n \in \mathrm{M}_{k/2}(NM^2, \chi\psi^2)$.*

3.3.3 Hecke operators

With slight modification from Subsection 3.3.1, we are ready to define

Definition 3.3.3.1. *Let k be an odd integer. Let $\alpha \in G$, $\widetilde{\Gamma}_1, \widetilde{\Gamma}_2 \subset \widetilde{\Gamma}_0(4)$ be subgroups and $f \in \mathrm{M}_{k/2}(\widetilde{\Gamma}_1)$. We define the* ***weight** $k/2$ **double coset operator*** $[\widetilde{\Gamma}_1\alpha\widetilde{\Gamma}_2]_{k/2}$ *on f to be*

$$f|[\widetilde{\Gamma}_1\alpha\widetilde{\Gamma}_2]_{k/2} := \sum_j f|[\beta_j]_{k/2},$$

where β_j runs through the set of orbit representatives for $\widetilde{\Gamma}_1 \setminus \widetilde{\Gamma}_1\alpha\widetilde{\Gamma}_2$.

For our purpose, we will consider only the case $\widetilde{\Gamma}_1 = \widetilde{\Gamma}_2 = \widetilde{\Gamma}_1(N)$ and $\alpha = \xi_n := \left(\begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}, \sqrt[4]{n}\right)$, where $N, n \in \mathbb{Z}$.

Proposition 3.3.3.2. ([Kob84], Proposition 12, p.204) *If $n > 0$ is not a perfect square and* $\gcd(n, N) = 1$, *then*

$$f|[\widetilde{\Gamma}_1(N)\xi_n\widetilde{\Gamma}_1(N)]_{k/2} = 0.$$

Due to the above proposition, we only need to consider Hecke operators on $\mathrm{M}_{k/2}(\widetilde{\Gamma}_1)$ of index prime to N when that index is a perfect square. Some modifications to Hecke operators in Subsection 3.2.3 are needed to define Hecke operators of half integral weight. For details, see [Kob84]. Here we adopt the following definition

Definition 3.3.3.3. *Let p be a prime. We define the Hecke operator T_{p^2} to be*

$$T_{p^2} := p^{\frac{k}{2}-2} f|[\widetilde{\Gamma}_1(N)\xi_{p^2}\widetilde{\Gamma}_1(N)]_{k/2},$$

where $\xi_{p^2} = \left(\begin{bmatrix} 1 & 0 \\ 0 & p^2 \end{bmatrix}, \sqrt{p}\right)$.

Next, we examine the effect of T_{p^2} on the coefficients of a modular form.

Proposition 3.3.3.4. ([Kob84], Proposition 13, p.207) *Suppose that $4 \mid N$, χ is a Dirichlet character modulo $N, p \nmid N$ is a prime and $k = 2\lambda + 1$ is a positive odd integer. Let $f(z) \in \sum_{n=0}^{\infty} a_n q^n \in \mathrm{M}_{k/2}(\widetilde{\Gamma}_0(N), \chi)$. Then*

$$T_{p^2} f(z) = \sum_{n=0}^{\infty} b_n q^n,$$

where

$$b_n = a_{p^2 n} + \chi(p)\left(\frac{(-1)^\lambda n}{p}\right) p^{\lambda-1} a_n + \chi(p^2) p^{k-2} a_{n/p^2}.$$

Here we take $a_{n/p^2} = 0$ if $p^2 \nmid n$.

As an application of Hecke operators of half integral weight, we will prove the following recurrence relation of $r_3(n)$, which appeared in [Hir99], p.101.

Proposition 3.3.3.5. *Let p be an odd prime and $n \in \mathbb{Z}$. Then*

$$r_3(p^2n) = \left[p + 1 - \left(\frac{-n}{p}\right)\right] r_3(n) - pr_3(n/p^2),$$

where $\left(\frac{a}{b}\right)$ denotes the Legendre symbol. Here we take $r_3(n/p^2) = 0$ if $p^2 \nmid n$.

Proof. We consider the modular form θ^3. By Theorem 3.2.4.2, $\theta^3 \in \mathrm{M}_{3/2}(\widetilde{\Gamma}_0(4))$. By Corollary 3.3.2.6, $\mathrm{M}_{3/2}(\widetilde{\Gamma}_0(4))$ has dimension 1. Therefore, $\mathrm{M}_{3/2}(\widetilde{\Gamma}_0(4)) = \mathbb{C}\theta^3$. Note that T_p^2 preserves the space $\mathrm{M}_{3/2}(\widetilde{\Gamma}_0(4))$, so that $T_{p^2}\theta^3 = c\theta^3$ for some $c \in \mathbb{C}$. Using Proposition 3.3.3.4 and comparing the constant coefficients, we deduce that $c = p+1$. Using Proposition 3.3.3.4 again, we obtain the result. □

3.3.4 Application to ternary quadratic forms

This subsection presents Lehman's idea of finding all forms having the same genus in [Leh92]. We will go into details and work out 2 concrete examples. In these examples, the Brant-Intrau-Schiemann table is used.

Definition 3.3.4.1. *A matrix M of dimension k over $\mathbb{Z}$ is called **even** if its entries on the main diagonal are all even.*

Theorem 3.3.4.2. ([Leh92], Theorem, p.400) *Let $f(x_1, \dots, x_k) = \sum_{i=1}^n f_{ii}x_i^2 + \sum_{1 \le i < j \le n} f_{ij}x_ix_j$ be a positive definite quadratic form over $\mathbb{Z}$. Let*

$$A_f := \left[\frac{\partial^2 Q}{\partial x_i \partial x_j}\right]_{i,j=1,\dots,k}.$$

Define N to be the smallest integer so that NA^{-1} is an even matrix. Let

$$\theta_f(z) := \sum_{(m_1,\dots,m_k)\in\mathbb{Z}^n} q^{f(m_1,\dots,m_k)}, \quad q = e^{2\pi i z}.$$

Then

$$\theta_f \in \mathrm{M}_{k/2}(N, \chi_d),$$

where

$$d := \begin{cases} \det A & \text{if } k \equiv 0 \pmod 4, \\ -\det A & \text{if } k \equiv 2 \pmod 4, \\ \det A/2 & \text{if } k \text{ is odd}, \end{cases}$$

and $\chi_d(\cdot) := \left(\frac{D}{\cdot}\right)$, where $d = qr^2$ with q square-free and

$$D := \begin{cases} q & \text{if } q \equiv 1 \pmod 4, \\ 4q & \text{if } q \equiv 2, 3 \pmod 4). \end{cases}$$

Definition 3.3.4.3. *The integer N in the above theorem is called the **level** of the positive definite quadratic form f.*

Now let f, g be positive definite quadratic forms in k variables. Suppose that $g = tf$ for some $t \in \mathbb{Z}$. Then $\theta(g)$ has weight $k/2$ and level tN. Its character is χ_d if k is even and χ_{td} if k is odd. Also, the q-expansion of $\theta(g)$ is the same as that of $\theta(f)$ with all exponents multiplied by t. Therefore, in finding the level of a positive definite quadratic form, we can restrict ourselves to the case when f is *primitive*, i.e, when the greatest common divisor of the coefficients of f is 1.

Definition 3.3.4.4. *Let $M = [m_{ij}] \in \mathrm{M}_k(\mathbb{Z})$ and $s, t \in \{1, \ldots, k\}$. Let M_{st} be the submatrix of M formed by crossing out the s-th row and the t-th column. Then, the (s, t) co-factor of M is defined to be $(-1)^{s+t} M_{st}$.*

Definition 3.3.4.5. *Let f be a positive definite ternary quadratic form and A_f be defined as in Theorem 3.3.4.2. Let C_{ij} be the (i, j) co-factor of A_f. We define the* ***divisor*** *of f to be*

$$m := m_f := \gcd(C_{11}, C_{22}, C_{33}, 2C_{23}, 2C_{13}, 2C_{12}).$$

Let $\alpha = C_{11}/m, \beta = C_{22}/m, \gamma = C_{33}/m, \rho = 2C_{23}/m, \sigma = 2C_{13}/m$ and $\tau = 2C_{12}/m$. The ***reciprocal*** *of f is defined to be*

$$\phi(x, y, z) = \alpha x^2 + \beta y^2 + \gamma z^2 + \rho yz + \sigma xz + \tau xy.$$

Since we are interested in ternary quadratic forms, the following special case of Theorem 3.3.4.2 is useful.

Proposition 3.3.4.6. ([Leh92], pp.401 − 402) *Let f be a positive definite ternary quadratic form and A_f, N be as in Theorem 3.3.4.2. Let C_{ij} be the (i, j) co-factor of A_f. Then*

$$N = \frac{\det A_f}{2m},$$

where m is the divisor of f.

Definition 3.3.4.7. *Let f be a positive definite ternary quadratic form with divisor m. Let p run over all prime divisors of m. We define the symbol (f/p) as follows:*
If p is odd, then $(f/p) := (f_{11}/p)$, where (f_{11}/p) is the Legendre symbol.
If $p = 2$, then define $(f/4) := (-1)^{(a-1)/2}$ if $16|m$, and $(f/8) := (-1)^{(a^2-1)/8}$ if $32|m$.
Let ϕ be the reciprocal of f with divisor μ. Let p run over all prime divisors of μ. The symbol (ϕ/p) is defined as follows:
If p is odd, then $(\phi/p) := (\gamma/p)$, where (γ/p) is the Legendre symbol.
$(\phi/4)$ and $(\phi/8)$ are defined similarly as $(f/4)$ and $(f/8)$.
The set of symbols $\{(f/p) : p|m\} \cup \{(\phi/p) : p|\mu\}$ are called the ***collection of genus symbols*** *for f.*

To find all forms having the same genus, we need the following reformulation of Definition 2.2.3.1.

Proposition 3.3.4.8. ([Leh92], p.410) *Let f and g be primitive positive definite ternary quadratic forms. Then f, g are in the same genus if and only if they have the same determinant, level and the collection of genus symbols.*

Using the above proposition, we can now easily compute which ternary quadratic forms are in the same genus of a given one.

Example 3.3.4.9. In this example, we will find all ternary quadratic forms in the same genus as $f = x^2 + y^2 + 10z^2$. Note that $N(f) = D(f) = 40$ and the divisor of f is $m = 4$. The reciprocal for f is $\phi = 10x^2 + 10y^2 + z^2$ with divisor $\mu = 40$. The genus symbol for f is $(\phi/5) = (1/5) = 1$. Looking at the Brand-Intrau-Schiemann table, we know that there are 2 more primitive positive ternary quadratic forms of determinant 40, which are $g_1 = x^2 + 2y^2 + 5z^2$ and $g_2 = 2x^2 + 2y^2 + 3z^2 + 2yz$. Using Proposition 3.3.4.6, we compute the levels of these forms which are both 40. The reciprocal forms of g_1, g_2 are respectively $\phi_1 = 10x^2 + 5y^2 + 2z^2$ and $\phi_2 = 5x^2 + 6y^2 + 4z^2 + 4yz$. Let m_1, m_2, μ_1, μ_2 be the divisors of g_1, g_2, ϕ_1, ϕ_2 respectively. Then $m_1 = m_2 = 4, \mu_1 = \mu_2 = 40$. The genus symbol for g_1 is $(\phi_1/5) = (2/5) = -1$. The genus symbol for g_2 is $(\phi_2/5) = (4/5) = 1$. This gives $g_2 = 2x^2 + 2y^2 + 3z^2 + 2xz$ as the only form in the same genus with $f = x^2 + y^2 + 10z^2$.

Example 3.3.4.10. In this example, we will find all ternary quadratic forms in the same genus as $f = 2x^2 + 2y^2 + 3z^2 + 2yz + 2xz + 2xy$. Note that $N(f) = D(f) = 28$ and the divisor of f is $m = 4$. The reciprocal of f is $\phi = 5x^2 + 5y^2 + 3z^2 - 2yz - 2xz - 4xy$ with divisor $\mu = 28$. The genus symbol for f is $(\phi/7) = (3/7) = -1$. Looking at the Brand-Intrau-Schiemann table, we know that there are 2 more primitive positive ternary quadratic form of determinant 28, which are $g_1 = x^2+y^2+7z^2$ and $g_2 = x^2+2y^2+4z^2+2yz$. Using Proposition 3.3.4.6, we compute the levels of these forms which are both 28. The reciprocal forms of g_1, g_2 are respectively $\phi_1 = 7x^2+7y^2+2z^2$ and $\phi_2 = 7x^2+4y^2+2z^2+2yz$. Let m_1, m_2, μ_1, μ_2 be the divisors of g_1, g_2, ϕ_1, ϕ_2 respectively. Then $m_1 = m_2 = 4, \mu_1 = \mu_2 = 28$. The genus symbol for g_1 is $(\phi_1/7) = (2/7) = 1$. The genus symbol for g_2 is $(\phi_2/7) = (2/7) = 1$. This eliminates both g_1, g_2. So $f = 2x^2 + 2y^2 + 3z^2 + 2yz + 2xz + 2xy$ is in a genus of one class.

Chapter 4

Conclusion

Schiemann (1993) proved that if two positive definite ternary quadratic forms represent the same numbers with the same multiplicities, then they are the same. In the first half of this thesis, we consider the effect of having the same multiplicities of representation in the statement. Kaplansky (1997) conjectured that if two forms have the same set of representable numbers, then either both are regular or one is equivalent to $\langle s, t, t, t, 0, 0\rangle$, the other to $\langle s, t, 3t, 0, 0, 0\rangle$ or one is equivalent to $\langle t, t, t, s, s, s\rangle$, the other to $\langle t, 2t, -s, 2t + s, 0, 2s, 0\rangle$. We proved the conjecture holds when two forms are diagonal. Since there are only 102 regular diagonal forms, the result further implies that Schiemann's result does not hold even for the simplest case, but a near miss. The method we used to prove the results might by applicable if the two forms are increased by a term xy or xz, but will be time and effort consuming. So a subtler method is desirable. In the second half of the thesis, we study modular forms. This topic is mostly independent with the first part of the thesis. The emphasis is on modular forms of half integral weight due to their connection with ternary quadratic forms. The theory of modular forms has been used successfully to determine the number of ways an integer can be represented as sums of n square, where $n \in \mathbb{Z}_+ \setminus \{3\}$. Here we demonstrate the cases $n = 2$ and $n = 4$. We also present a recursive relation for sums of three squares by using Hecke operators, and an interesting relation between sums of five squares and Dirichlet L-series. In the last subsection of this part, we give an application of modular forms in finding all ternary quadratic forms being in the same genus as a given one.

Bibliography

[Apo90] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Springer, New York, 1990.

[Cas97] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, Germany, 1997.

[Cas08] J. W. S. Cassels, *Rational Quadratic Forms*, Dover, New York, 2008.

[Cop09] W. A. Coppel, *Number Theory: An Introduction to Mathematics*, Springer, New York, 2009.

[Cox89] D. A. Cox, *Primes of the form x^2+ny^2: Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons, Canada, 1989.

[Dia05] F. Diamond and J. Shurman, *A First Couse in Modular Forms*, Springer, USA, 2005.

[Dic27] L. E. Dickson, *Ternary Quadratic Forms and Congruences*, *The Annals of Mathematics*, Second Series, Vol. 28, No. 1/4, pp. 333-341, 1927.

[Dic39] L. E. Dickson, *Modern Elementary Theory of Numbers*, University of Chicago Press, New York, 1939.

[Dic92] L. E. Dickson, *History of the theory of numbers, Volume III: Quadratic and Higher Forms*, Chelsea Publishing Company, New York, 1992.

[Fre05] E. Freitag and R. Busam, *Complex Analysis*, Springer, Berlin, 2005.

[Gab12] G. Nebe and N. Sloane, *The Brandt-Intrau-Schiemann Table of Odd Ternary Quadratic Forms.* Retrieved 7/4/2012, from `www2.research.att.com/~njas/lattices/Brandt_1.html`.

[Geh11] A. Gehret, A. Kottmeyer and N. Salter, Computation of Modular Forms of Weight 3/2, Preprint, 2011.

[Gro85] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, New York, 1985.

[Hir99] M. D. Hirschhorn and J. A. Sellers, On representations of a number as a sum of three squares, *Discrete Mathematics*, Vol. 199, pp. 85-101, 1999.

[Hor90] N. R. A. Horn and C. R. Johnson, *Matrix analysis*, Cambridge University Press, Cambridege, 1990.

[Jag10] W. C. Jagy, *Integral Positive Ternary Quadratic Forms*, Preprint, 2010.

[Jag97] W. C. Jagy, I. Kaplansky and A. Chiemann, There are 913 regular ternary quadratic forms, *Mathematika*, Vol. 44, pp. 332-341, 1997.

[Jon28] B. W. Jones, *Representation by positive ternary quadratic forms*, PhD thesis, University of Chicago, 1928.

[Jon39] B. W. Jones and G. Pall, Regular and semi-regular positive ternary quadratic forms, *Acta Mathematica*, Vol.70, pp. 165-191, 1939.

[Kil08] L. J. P. Kilford, *Modular Forms: A classical and computational introduction*, Imperial College Press, Singapore, 2008.

[Kob84] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, New York, 1984.

[Leh92] J. L. Lehman, Levels of positive definite ternary quadratic forms, *American Mathematical Society*, Vol. 58, No. 197, pp. 399-417, 1992.

[Mor06] C. J. Moreno and S. S. Wagstaff, *Sums of Squares of Integers*, Taylor & Francis Group, USA, 2006.

[Nat00] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer, New York, 2000.

[Sch97] A. Schiemann, Ternary positive definite quadratic forms are determined by their theta series, *Mathematische Annalen*, Vol.308, pp. 507-517, 1997.

[Ser73] J. P. Serre, *A course in arithmetic*, Springer, New York, 1973.

[Shi73] G. Shimura, On modular forms of Half Integral Weight, *The Annals of Mathematics*, Second Series, Vol. 97, No. 3, pp. 440-481, 1973.

[Ste07] W. Stein, *Modular forms: A computational approach*, Graduate Studies in Mathematics, American Mathematical Society, 2007.

[Wat79] G. L. Watson, Determination of a binary quadratic form by its values at integer points, *Mathematika*, Vol. 26, pp. 72-75, 1979.

[Whi35] E. T. Whittaker and G. N. Watson, *A course of modern analysis*, Cambridge University Press, Cambridge, 1935.