# ON A CERTAIN TRIPLE SYSTEM, ELLIPTIC CURVES AND GAUSS THEORY OF QUADRATIC FORMS

by

Shuai Wang

A dissertation submitted to the Johns Hopkins University in conformity with the requirements for the degree of Doctor of Philosophy

Baltimore, Maryland

April, 2008

## ABSTRACT

Inspired by the important result that the space of cusp forms is generated by Poincaré sums, a triple system $(\mathcal{G}, (G, M))$ is proposed in general and we are interested in whether analogous results hold in other circumstances. First I consider the case $(\mathcal{G}, (\mathrm{SL}_m(\mathbb{Z}), \mathrm{sl}_m(\mathbb{Z})))$ with $\mathcal{G}$ a cyclic group. In order to compute it, I generalize the core theorem in Gauss theory of quadratic forms from quadratic extensions to $n$-dimensional algebraic extensions and from over the integers to over any ring of integers which is a PID. By that generalization, I get analogous results to that of cusps forms for good cocycles. Second I consider the case $(\mathcal{G}, (\Gamma(N), M))$ with $\mathcal{G}$ a cyclic group and the congruence subgroup $\Gamma(N)$ in $\mathrm{SL}_m(\mathbb{Z})$. In order to compute it and others which might occur in the future, I generalize that core theorem in Gauss theory of quadratic forms even more to what I call polynomial cohomology. Third I consider the case $(\mathcal{G}, (\mathcal{O}^\times, \mathcal{O}))$ to explore more about the circumstance with $\mathcal{G}$ infinite, where $\mathcal{G}$ is the universal covering group for the elliptic curve $E_\tau$ associated with an element $\tau$ in the upper half plane and $\mathcal{O}$ is the ring of holomorphic functions over $\mathbb{C}$. From the results there for the elliptic curve case and those for the original modular form case, I try to formulate a good definition for a triple system when $\mathcal{G}$ is countable. Under that definition, in that elliptic curve case, we get analogous results to that of cusps forms for all the cocycles.


**Advisor**: Professor Takashi Ono.

## ACKNOWLEDGEMENT

Give thanks to the LORD, for He is good. His love endures forever.

Give thanks to my advisor, Professor Takashi Ono, for his insight, advice, encouragement, kindness and patience throughout my research. This project would not have been possible without his guidance.

Give thanks to Professor Qiao Zhang, Professor Stefan Kühnlein and Professor Florin Spinu, for their great assistance and helpful comments on this project.

Give thanks to my friends Yen-Yi Ho, Thomas Wright and Xiaozhen Lv for their advice, encouragement and assistance for me on this project.

Give thanks to my parents, my parents in law, and my brother for their constant support. In particular, give special thanks to my wife Wei Luo for her love and encouragement, and to my endearing daughter Shelley Enqi Wang.

# Contents

# 1 Introduction

One important result about modular forms is that the space of cusp forms is generated by Poincaré sums ([7]). Inspired by it, Ono proposes a setting of a certain triple system $(\mathcal{G}, (G, M))$ ([24]), which is more general than the one proposed by Shafarevich ([28]) and Ono ([21]). Under that setting, the result mentioned above about cusp forms becomes the statement that $M_c$ is generated by Poincaré sums.

It is then interesting to know if similar phenomenon occurs in other circumstances. In finite Galois extension case, Ono has settled that problem ([21], [22], [13], [23]), while I consider it for the case of cyclic actions of a matrix and the case of elliptic curves over $\mathbb{C}$. I will explain them in more detail later.

Now I introduce the triple system $(\mathcal{G}, (G, M))$. Let $G$ be a group and $M$ be a left $G$-module. Consider a finite group $\mathcal{G}$ which acts naturally on $(G, M)$. In other words, we assume that $G$ is a left $\mathcal{G}$-group, $M$ is a left $\mathcal{G}$-module so that ${}^{\sigma}(sx) = {}^{\sigma}s\,{}^{\sigma}x$, $\forall \sigma \in \mathcal{G}, s \in G, x \in M$. Define the cohomology set $H^1(\mathcal{G}, G)$ to be the quotient $Z^1(\mathcal{G}, G)/\sim$, where $Z^1(\mathcal{G}, G) = \{c : \mathcal{G} \to G | c_{\sigma\tau} = c_\sigma {}^{\sigma}c_\tau, \forall \sigma, \tau \in \mathcal{G}\}$ is the set of cocycles, and the equivalence relation $\sim$ is defined as: $c \sim c' \iff \exists u \in G$, such that $c'_\sigma = u^{-1} c_\sigma {}^{\sigma}u, \forall \sigma \in G$. Moreover, for a cocycle $c$, we associate two $\mathbb{Z}$-modules as the following:

$$M_c = \{x \in M : c_\sigma {}^{\sigma}x = x, \forall \sigma \in \mathcal{G}\}$$

and

$$P_c = \left\{ p_c(x) = \sum_{\tau \in \mathcal{G}} c_\tau {}^{\tau}x, x \in M \right\}.$$

It is easy to see that $P_c$ is the submodule of $M_c$ generated by Poincaré sums. Moreover, $M_c/P_c$ depends only on the class of $c$, i.e., $M_c/P_c \simeq M_{c'}/P_{c'}$ if $c \sim c'$. For $c = 1$, we get $M_1 = M^{\mathcal{G}}, P_1 = N_{\mathcal{G}} M$ and $M_1/P_1 = M^{\mathcal{G}}/N_{\mathcal{G}} M = \hat{H}^0(\mathcal{G}, M)$. Thus for a general $\gamma = [c] \in H^1(\mathcal{G}, G)$, we can think of $M_c/P_c$ as $\hat{H}^0(\mathcal{G}, M)_\gamma$, the Tate group twisted by $\gamma$.

To investigate the triple system in other circumstances, it is very natural to begin with a cyclic group $\mathcal{G}$. So first I examine a triple system $(\mathcal{G}, (G, M))$ with $\mathcal{G} =< \theta >$, a cyclic group of order two. Now let $G = \mathrm{SL}_2(\mathbb{Z})$, and $M = \mathrm{sl}_2(\mathbb{Z})$, the Lie algebra of $G$. Let $G$ act on $M$ by conjugation, $g \circ x = gxg^{-1}$, $\forall g \in G$, $x \in M$. And the action of $\mathcal{G}$ on $M_2(\mathbb{Z})$ is

given by:

$$^{\theta}x = x^{*t} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}, \text{ if } x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$$

where $x^*$ is the companion matrix of $x$, and $x^t$ is its transpose.

In this case, we can get that $H^1(\mathcal{G}, G) = \{c \in G | c = c^t\}/\sim$, where the equivalence relation is given by congruence in $G$. Then by the well-known core theorem of Gauss theory of quadratic forms in [6], which we will refer to as Gauss Correspondence (or abbreviated as G.C.), $H^1(\mathcal{G}, G)$ can be calculated out as $\{[I], [-I]\}$. Thus we only need to compute $M_c/P_c$ for $c = I, -I$. Those computations are easy, and we can get $M_c/P_c = 1$, for $c = I$ or $-I$.

$M_c/P_c = 1$ means that $M_c$ is generated by Poincaré sums, so we get the desired result in this case. What about it in a more general case, say $(\mathcal{G}, (\mathrm{SL}_m(\mathbb{Z}), \mathrm{sl}_m(\mathbb{Z})))$ where $\mathcal{G}$ is any cyclic group and $m$ is any integer? When I explore in that direction, I find myself in a position to generalize the Gauss Correspondence, otherwise I will have difficulty in calculating $H^1(\mathcal{G}, G)$. So I generalized it to fit my need, and that new generalization problem seems to me more interesting and important than the one above about $(\mathcal{G}, (\mathrm{SL}_m(\mathbb{Z}), \mathrm{sl}_m(\mathbb{Z})))$.

Actually I feel like that the Gauss Correspondence is a somewhat artificial and inflexible statement, although it is well-known and ingenious. I wonder why one does not try to find a more natural rule behind it.

Recently Manjul Bhargava ([1]) generalized the Gauss composition theory of quadratic forms to higher degree forms which involves three-dimensional boxes, not (two-dimensional) matrices. Actually, his equivalence relation is no longer given by congruences but by actions of certain matrix groups. His method, however, does not work for algebraic extensions of degree more than five. So I have not been satisfied with his generalization.[1]

After studying the paper [1] for some time, I find that G.C. is actually a special case of Latimer-MacDuffee-Taussky Theorem (see [12], [29]) (or LMT Theorem, for short). This generalization works for any algebraic number field and is much closer to the original G.C. than the method in [1].

Now let me introduce my work on the generalization. First remind you the well-known Gauss Correspondence. Let $m$ ($\neq 0, 1$) be a square-free integer and $K = \mathbb{Q}(\sqrt{m})$. Denote by $\Delta_K$ the discriminant of $K$, by $I_K$ the group of fractional ideals of $K$, by $P_K$ the subgroup of principal ideals in $I_K$ and put $P_K^+ = \{\mathbf{a} = (\alpha) \in P_K : N_{K|\mathbb{Q}}(\alpha) > 0\}$. Then we define

[1] I express my thanks to Professor Qiao Zhang for telling me the existence of [1].

$H_K = I_K/P_K$, $H_K^+ = I_K/P_K^+$. $H_K$ is the ideal class group of $K$ and $H_K^+$ is the ideal class group of $K$ in the narrow sense.

A quadratic form is a form $f(z) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$, where $z = (x, y)^t$. Its discriminant is defined as $\Delta_f = b^2 - 4ac$. An equivalence relation $\overset{+}{\sim}$ is defined on the set of all quadratic forms as the following: for any two quadratic forms $f$ and $g$, $f \overset{+}{\sim} g$ if and only if $\exists \gamma \in \mathrm{SL}_2(\mathbb{Z})$, such that $g(z) = f(\gamma z)$.

Consider the following quotient for a fixed quadratic field $K$:

$$Q(\Delta_K) = \left\{ f = ax^2 + bxy + cy^2 : \begin{array}{l} a, b, c \in \mathbb{Z}, \\ \Delta_f = \Delta_K (f > 0 \text{ if } \Delta_K < 0) \end{array} \right\} \Big/ \overset{+}{\sim}$$

Then the Gauss Correspondence can be expressed as:

**Theorem 4.1.1.** (Gauss, [6]) There is a bijection $i_K : H_K^+ \overset{\sim}{\to} \tilde{Q}(\Delta_K)$.

How to generalize this theorem? First it is obvious that any quadratic form $ax^2 + bxy + cy^2$ is associated with a matrix $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$. So if we let $f(t) = t^2 - p\,t + q$ be an irreducible polynomial in $\mathbb{Z}[t]$ with discriminant $\Delta_f = p^2 - 4q$, then $\tilde{Q}(\Delta_K)$ can be rewritten as

$$\tilde{Q}(f) = \left\{ A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in M_2(\mathbb{Q}) : \begin{array}{l} a, b, c \in \mathbb{Z}, b \equiv p \pmod 2 \\ \det(A) = -\frac{\Delta_f}{4} \\ (A > 0 \text{ if } \Delta_f < 0) \end{array} \right\} \Big/ \overset{c}{\sim}$$

for $f(t) = t^2 - m$, when $m \equiv 2, 3 \pmod 4$, and for $f(t) = t^2 - t + \frac{1-m}{4}$, when $m \equiv 1 \pmod 4$, where the equivalence relation $\overset{c}{\sim}$ is given by congruence in $\mathrm{SL}_2(\mathbb{Z})$, i.e., for $\forall A, B \in M_2(\mathbb{Z})$, $A \overset{c}{\sim} B$ if and only if $\exists T \in \mathrm{SL}_2(\mathbb{Z})$, such that $B = TAT^t$. We also define two other equivalence relations $\overset{+}{\sim}$ and $\sim$ on $M_2(\mathbb{Z})$ as the following: $\forall A, B \in M_2(\mathbb{Z})$, $A \overset{+}{\sim} B$ if and only if $\exists T \in \mathrm{SL}_2(\mathbb{Z})$, such that $B = TAT^{-1}$, and $A \sim B$ if and only if $\exists T \in \mathrm{GL}_2(\mathbb{Z})$, such that $B = TAT^{-1}$.

Then here comes the breakthrough:

**Theorem 4.3.1.** If $f(t) = t^2 - p\,t + q$ is an irreducible polynomial in $\mathbb{Z}[t]$, then there is a bijection $\lambda$:

$$\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : \begin{array}{l} f(A) = 0 \\ (b > 0 \text{ if } \Delta_f < 0) \end{array} \right\} \Big/ \overset{+}{\sim} \overset{\sim}{\longrightarrow} \tilde{Q}(f) \qquad (1)$$

The map $\lambda$ is given by $\lambda([A]) = [(A - \frac{p}{2})J^{-1}]$, for any $[A]$ in the left hand side of (1), where $J$ is the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. It is just a linear transformation.

Theorem 4.3.1 is quite simple, but it has far reaching impacts. It tells us that, skewed after a linear transformation, $\tilde{Q}(\Delta_K)$ can be viewed as the set of matrix solutions of an irreducible polynomial, a totally new point of view of quadratic forms.

By the Latimer-MacDuffee-Taussky Theorem [2] ([12], [29]), we know there is a bijection between $\{A \in M_2(\mathbb{Z}) : f(A) = 0\}/\sim$ and $H_K$ when $m \equiv 2, 3 \pmod 4$ and $f(t) = t^2 - m$, or when $m \equiv 1 \pmod 4$ and $f(t) = t^2 - t + \frac{1-m}{4}$. The bijection map is induced by assigning a matrix to the ideal generated over $\mathbb{Z}$ by the entries of its eigenvector. Combining it with Theorem 4.3.1 above, we find another way to get the Gauss Correspondence. Although there is some sign difference between the map we get and the one Gauss used, they are essentially the same. However, the new point of view of Gauss Correspondence allows us to generalize it to higher degree algebraic extensions and over any ring of integers which is a PID.

I will introduce the LMT Theorem in more generality. Let $k$ be a number field (local or global), and $\mathcal{O}_k$ be its ring of integers. Introduce two equivalence relations on $M_n(\mathcal{O}_k)$ as follows: $\forall A, B \in M_n(\mathcal{O}_k)$, $A \sim B$ if and only if $\exists T \in \mathrm{GL}_n(\mathcal{O}_k)$ such that $B = TAT^{-1}$, and $A \overset{+}{\sim} B$ if and only if $\exists T \in \mathrm{SL}_n(\mathcal{O}_k)$, such that $B = TAT^{-1}$, where $\mathrm{GL}_n(\mathcal{O}_k) = \{X \in M_n(\mathcal{O}_k) : \det(X) \in \mathcal{O}_k^\times\}$, and $\mathrm{SL}_n(\mathcal{O}_k) = \{X \in M_n(\mathcal{O}_k) : \det(X) = 1\}$.

For a fixed monic irreducible polynomial $f \in \mathcal{O}_k[t]$ of degree $n$ over $k$, consider $M_n(\mathcal{O}_k; f) = \{A \in M_n(\mathcal{O}_k) : f(A) = 0\}$, and define $\tilde{M}_n(\mathcal{O}_k; f) = M_n(\mathcal{O}_k; f)/\sim$, $\tilde{M}_n^+(\mathcal{O}_k; f) = M_n(\mathcal{O}_k; f)/\overset{+}{\sim}$.

On the other side, let $\theta \in \overline{\mathcal{O}_k}$ satisfying $f(\theta) = 0$, where $\overline{\mathcal{O}_k}$ is an integral closure of $\mathcal{O}_k$. Take $K = k(\theta)$, let $\mathcal{O} = \mathcal{O}_k[\theta]$ be an order in $\mathcal{O}_K$, and denote by $I_\mathcal{O}$ the set of all integral ideals of $\mathcal{O}$. Introduce an equivalence relation in $I_\mathcal{O}$ as follows: for any $\mathbf{a}$, $\mathbf{b}$ in $I_\mathcal{O}$, $\mathbf{a} \sim \mathbf{b}$ if and only if $\exists \alpha, \beta \in \mathcal{O}, \alpha \neq 0, \beta \neq 0$, such that $\alpha\mathbf{a} = \beta\mathbf{b}$. Then define $\tilde{I}_\mathcal{O} = I_\mathcal{O}/\sim$. It is the ideal class group $H_K$ when $\mathcal{O} = \mathcal{O}_K$.

**Theorem 4.2.1.** (Latimer-MacDuffee-Taussky, [12], [29]) If $\mathcal{O}_k$ is a PID, then we have a bijection $\varphi : \tilde{M}_n(\mathcal{O}_k; f) \xrightarrow{\sim} \tilde{I}_\mathcal{O}$.

Using this theorem, we can generalize the Gauss Correspondence.

[2] Thanks a lot to my advisor Prof. Takashi Ono for telling me the LMT theorem.

Let $P \in M_n(\mathcal{O}_k)$ with $f(P) = 0$ be a fixed matrix, then we have the following:

**Theorem 4.4.1.** There is an exact sequence of pointed sets:

$$1 \to C_P(\mathrm{SL}_n(\mathcal{O}_k)) \xrightarrow{\iota} C_P(\mathrm{GL}_n(\mathcal{O}_k)) \xrightarrow{\det} \mathcal{O}_k^\times \xrightarrow{\delta} \tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{i} \tilde{M}_n(\mathcal{O}_k; f) \to 1$$

where $C_P(\mathrm{SL}_n(\mathcal{O}_k))$ and $C_P(\mathrm{GL}_n(\mathcal{O}_k))$ are the centralizers of $P$ in $\mathrm{SL}_n(\mathcal{O}_k)$ and $\mathrm{GL}_n(\mathcal{O}_k)$ respectively, and we consider $[P]$ as the distinguished element in both $\tilde{M}_n^+(\mathcal{O}_k; f)$ and $\tilde{M}_n(\mathcal{O}_k; f)$ when we talk about its exactness. Moreover, when $\mathcal{O}_K = \mathcal{O}_k[\theta]$, we have a bijection $i_f$:

$$\tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{\sim} \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times \tilde{M}_n(\mathcal{O}_k; f)$$

So if in addition, $\mathcal{O}_k$ is a PID, by LMT, $i_f$ becomes

$$\tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{\sim} \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times H_K$$

Theorem 4.4.1 generalizes the Gauss Correspondence from quadratic extensions to $n$-dimensional algebraic extensions, and from over the integers to over any ring of integers which is a PID. One can then verify the classical Gauss Correspondence from Theorem 4.4.1. (It is not so straightforward, and we need some proof there.)

Equipped with the generalization of Gauss Correspondence, we can now turn back to the general case $(\mathcal{G}, (\mathrm{SL}_m(\mathbb{Z}), \mathrm{sl}_m(\mathbb{Z})))$ where $\mathcal{G}$ is any cyclic group and $m$ is any positive integer. To be more specific, I consider the cyclic action of a matrix on a matrix algebra by conjugation, which generalizes the case we talked about before, where $\mathcal{G}$ is cyclic of order two.

Let $m \in \mathbb{Z}$ be a positive integer, the matrix be some $P \in \mathrm{SL}_m(\mathbb{Z})$ and the matrix algebra be $M_m(\mathbb{Z})$. Suppose the order of this action of $P$ on $\mathrm{SL}_m(\mathbb{Z})$ is $h$, and this action is irreducible, i.e., $P$ satisfies $f(P) = 0$ for some irreducible polynomial $f(t) \in \mathbb{Z}[t]$. Let $\mathcal{G} = \mathbb{Z}/h\mathbb{Z}$, $G = \mathrm{SL}_m(\mathbb{Z})$, $M = \mathrm{sl}_m(\mathbb{Z})$ and consider the triple system $(\mathcal{G}, (G, M))$.

To signify this action is given by $P$, we denote the corresponding $H^1(\mathbb{Z}, G)$, $M_c$ and $P_c$ by $H^1(\mathbb{Z}, G)_P$, $M_{c,P}$ and $P_{c,P}$ respectively. In those notations, we have the following result:

If the actions of two fixed $P, Q \in G$ have the same order $h$, then there is a bijection $i'_{PQ}$ between $H^1(\mathcal{G}, G)_P$ and $H^1(\mathcal{G}, G)_Q$. In addition, if $i'_{PQ}([c]) = [d]$, then $M_{c,P} \simeq M_{d,Q}$ for $h = 0$, and $M_{c,P}/P_{c,P} \simeq M_{d,Q}/P_{d,Q}$ for $h \neq 0$.

This result tells us that if there is a cyclic action of order $h$, then we can just proceed to choose any $P$ to do our computation.

For $h = 0$ case, $H^1(\mathcal{G}, G)$ can be identified with $G/\sim$, where the equivalence relation is given by conjugation in $G$. And for every $[c] \in H^1(\mathcal{G}, G)_P$, $M_c = C_{(c_1 P)}(M)$, the centralizer of $c_1 P$ in $M$.

For $h \neq 0$ case, we use the generalization of Gauss Correspondence to do the computation. One can try to use this method for any positive integer $m$, but I focus on the $m = 2$ case to illustrate this method, in which case I determine completely $H^1(\mathcal{G}, G)$ and $M_c/P_c$ without assuming irreducible action in the beginning. The result in the $m = 2$ case is as follows:

The cyclic action is always irreducible, and $h$ can only be $1, 2$ or $3$. When $h = 1$, $H^1(\mathcal{G}, G) = 1$ and $M_1/P_1 = 1$. When $h = 2$, $H^1(\mathcal{G}, G) = \{[I], [-I]\}$, and $M_c/P_c = 1$ for either $[c] \in H^1(\mathcal{G}, G)$. When $h = 3$, $H^1(\mathcal{G}, G) = \{[P^{-1}], [I], [P]\}$ where $P = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$, $M_c/P_c = (\mathbb{Z}/3\mathbb{Z})^3$ for $[c] = [P^{-1}]$, and $M_c/P_c = 1$ for $[c] = [I]$ or $[P]$.

During the computation, one might have the feeling that in order for $M_c/P_c = 1$, the cocycle $c$ must be "irreducible" in some sense.

After $(\mathcal{G}, (\mathrm{SL}_m(\mathbb{Z}), \mathrm{sl}_m(\mathbb{Z})))$, it is very natural to think about congruence subgroups. In this case, the generalization of Gauss Correspondence is not enough for our need. For this need and other needs which might occur in the future, I generalize the Gauss Correspondence to the greatest generality I can.

Let $G$ be a group, $R$ be a commutative ring and $\mathcal{A}$ be an $R$-algebra. $f(t) \in R[t]$ is a polynomial. For a multiplicative subset $M \subseteq \mathcal{A}$, if $G$ acts on the subset of $M$, $M^f = \{A \in M : f(A) = 0\}$, we define $H^1(f, M; G) = \{A \in M : f(A) = 0\}/G$ to be the set of the $G$-orbits of $M^f$. When $1 \in M$, denote $M^\times$ be the set of all the invertible elements in $M$, then it is a group. If it acts on $M^f$, we simply denote $H^1(f, M; M^\times)$ by $H^1(f, M)$.

Take a multiplicative set $S$ with unity, and assume $M$ contains the multiplicative unity of $\mathcal{A}$ too. Let us abuse the notation, and denote those two unities by the same expression 1. Let $\pi : M \to S$ be a surjective map with $\pi(1) = 1$ and $\pi(AB) = \pi(A)\pi(B)$, $\forall A, B \in M$. Also assume $\Gamma = \ker(\pi) = \{A \in M : \pi(A) = 1\}$ be a group. So we have the following exact sequence of pointed sets:

$$1 \to \Gamma \to M \xrightarrow{\pi} S \to 1 \tag{2}$$

Let $M^\times$, $S^\times$ act by conjugation on $M$, $S$ respectively. And for any $P \in M$, denote $C_P(\Gamma) = \{A \in \Gamma : AP = PA\}$, $C_P(M^\times) = \{A \in M^\times : AP = PA\}$ and $C_{\pi(P)}(S^\times) = \{a \in$

$S^\times : a\pi(P) = \pi(P)a\}$. Then the following theorem tells us that we can get a long exact sequence from the short exact sequence (2).

**Theorem 4.5.1.** For any $P \in M^f$, $\Gamma$ acts by conjugation on $(\pi^{-1} \circ \pi(P))^f$, and we have the following long exact sequence of pointed sets:

$$1 \to C_P(\Gamma) \xrightarrow{\iota} C_P(M^\times) \xrightarrow{\pi} C_{\pi(P)}(S^\times) \xrightarrow{\delta_P} H^1(f, \pi^{-1} \circ \pi(P); \Gamma) \xrightarrow{i} H^1(f, M) \tag{3}$$

Moreover, if $S$ is contained in a $R$-algebra $\mathcal{B}$, and their unities coincide, and if $\pi$ is defined as a map $\pi : \mathcal{A} \to \mathcal{B}$, $\pi|_M$ is the $\pi$ above, and it satisfies $\pi(0) = 0$, $\pi(aA) = a\pi(A)$ and $\pi(A + B) = \pi(A) + \pi(B)$, $\forall a \in R$, $\forall A, B \in M$, then we have the following long exact sequence of pointed sets:

$$1 \to C_P(\Gamma) \xrightarrow{\iota} C_P(M^\times) \xrightarrow{\pi} C_{\pi(P)}(S^\times) \xrightarrow{\delta_P}$$

$$\xrightarrow{\delta_P} H^1(f, \pi^{-1} \circ \pi(P); \Gamma) \xrightarrow{i} H^1(f, M) \xrightarrow{\pi} H^1(f, S) \tag{4}$$

Here when we talk about the exactnesses of (3) and (4), we consider $[P]$ as the distinguished element in both $H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$ and $H^1(f, M)$, and consider $[\pi(P)]$ as the distinguished element in $H^1(f, S)$. And if $\{P_i \in (\pi^{-1} \circ \pi(P))^f : i \in \mathcal{I}\}$ is a set of representatives of $i(H^1(f, \pi^{-1} \circ \pi(P); \Gamma))$, we have a bijection $i_f$:

$$H^1(f, \pi^{-1} \circ \pi(P); \Gamma) \xrightarrow{\sim} \coprod_{i \in \mathcal{I}} \pi(C_{P_i}(M^\times)) \backslash C_{\pi(P)}(S^\times)$$

which splits $H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$ into a disjoint union of the sets of right cosets of $\pi(C_{P_i}(M^\times))$ in $C_{\pi(P)}(S^\times)$.

I call this generalization as polynomial cohomology. We can apply it to the case of $\Gamma(N) = \{A \in \mathrm{SL}_m(\mathbb{Z}) : A \equiv I \pmod N\}$, the congruence subgroup of $\mathrm{SL}_m(\mathbb{Z})$.

Take $m = \phi(e)$ for a positive integer $e \geq 3$. Take an element $\theta \in \mathrm{GL}_m(\mathbb{Z})$, and let it act cyclically on $M_m(\mathbb{Z})$ by conjugation. Suppose this action is irreducible and finite, and $\theta$ satisfies $\Phi_e(\theta) = 0$. Then we can show that $\theta$ is actually an element in $\mathrm{SL}_m(\mathbb{Z})$. Denote $\overline{\theta} = \mathrm{mod}_N(\theta)$, the matrix got from $\theta$ by modulo $N$ for each entry, and let $K = \mathbb{Q}(\zeta)$ for a primitive $e$-th root of unity $\zeta$. Consider the triple system $(\mathcal{G}, (\Delta, M))$ with $\mathcal{G} =< \theta >= \mathbb{Z}/e\mathbb{Z}$, $\Delta = \Gamma(N)$.

When $N$ is prime, it has already been studied by Prof. Kühnlein ([10]). However, in the view point of polynomial cohomology, his proof can be made more organized and clearer.

Assuming $N$ does not divide $e$, $N \geq 3$ and denoting $\Gamma = \mathrm{GL}_m(\mathbb{Z})$ as what Prof. Kühnlein did, I explained my approach to this problem in this paper, and get an equivalent result, a bijection:

$$H^1(\mathcal{G}, \Delta) \xrightarrow{\sim} H_K \times (C_\theta(\Gamma)\Delta/\Delta)\backslash C_{\overline{\theta}}(\Gamma/\Delta)$$

For the case when $N$ is not prime, I denote $\Gamma$ for $\mathrm{SL}_m(\mathbb{Z})$ instead of $\mathrm{GL}_m(\mathbb{Z})$, which is more natural. In this case, I can only get an injection:

$$H^1(\Phi_e, \Delta\theta; \Delta) \hookrightarrow H_K \times \{\pm 1\} \times (C_\theta(\Gamma)\Delta/\Delta)\backslash C_{\overline{\theta}}(\Gamma/\Delta)$$

The story above are all about triple systems $(\mathcal{G}, (G, M))$ with $\mathcal{G}$ finite. But what should the definition be for $\mathcal{G}$ infinite? Especially how should the Poincaré sums be defined? We already have an example in the modular forms, from which our motivation starts. But I want to look at one more example.

I consider the case where $M$ is taken as $\mathcal{O}$, the ring of holomorphic functions over $\mathbb{C}$, $G$ as $\mathcal{O}^\times$, the group of invertible elements in $\mathcal{O}$, and $\mathcal{G}$ as $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$, the universal covering group for the elliptic curve $E_\tau$ associated with an element $\tau$ in the upper half plane. The action of $L_\tau$ on $\mathbb{C}$ is given by: ${}^\omega z = z + \omega, \forall z \in \mathbb{C}, \omega \in L_\tau$. Then $L_\tau$ has a natural left action on $\mathcal{O}$: ${}^\omega f(z) = f({}^{\omega^{-1}} z) = f(z - \omega), \forall f \in \mathcal{O}, z \in \mathbb{C}, \omega \in L_\tau$.

In this case, I obtain explicit expressions of all the cocycle classes in $H^1(\mathcal{G}, G)$, and for every cocycle $c$, I get that $M_c$ is still generated by Poincaré sums.

For simplicity, I use $\mathbf{e}(z)$ instead of $\exp(2\pi i z)$. Then the elements in $H^1(\mathcal{G}, G)$ are described by the following theorem:

**Theorem 6.2.2.** Any cocycle is equivalent to a cocycle $c$ having the following form:

$$c_\omega = \mathbf{e}(na(z - \frac{n}{2}\tau) + nb) \tag{5}$$

where $\omega = m + n\tau \in L_\tau, m, n \in \mathbb{Z}, a = a(\tau) \in \mathbb{Z}, b = b(\tau) \in \mathbb{C}$. Conversely, for any $a = a(\tau) \in \mathbb{Z}, b = b(\tau) \in \mathbb{C}$, (5) gives a cocycle in $H^1(L_\tau, \mathcal{O}^\times)$. Any two cocycles $c, c'$ having the form (5) are equivalent if and only if $a = a'$, and $b - b' \in \mathbb{Z} + \mathbb{Z}\tau = L_\tau$, where $a', b'$ are the corresponding parameters to $c'$ as that of $a, b$ to $c$.

For every cocycle $c$, we can get its corresponding $\mathbb{C}$-vector space $M_c$ as follows:

**Theorem 6.3.1.** For any cocycle $c$ of the form (5), with $a \in \mathbb{Z}, b \in \mathbb{C}$, we have the following:

1. If $a \neq 0$, then $\dim M_c = |a|$, and the basis can be given by $\sum_{k\in\mathbb{Z}} c_{k\tau}\mathbf{e}(r(z-k\tau)), r = 0, \ldots, |a|-1$;
2. If $a = 0$ and $b \notin L_\tau$, then $M_c = 0$;
3. If $a = 0$ and $b \in L_\tau$, then $\dim M_c = 1$, and the basis can be given by $\mathbf{e}(rz)$, where $b = r' + r\tau \in L_\tau, r, r' \in \mathbb{Z}$.

From the above theorem, it seems that the elements in $M_c$ are still generated by Poincaré sums. To proclaim it, we need to formulate a general definition for the triple system $(\mathcal{G}, (G, M))$ when $\mathcal{G}$ is countable. A new $P_c$ and a new Poincaré sum is proposed as follows. For each cocycle $c \in Z^1(\mathcal{G}, G)$, let $P_c = \{a \in M : a = p_{c,H}(x) = \sum_{s\in\mathcal{G}/H} c_s{}^s x$, for some subgroup $H \subseteq \ker(c) \subseteq \mathcal{G}$, some $x \in M^H$, and it converges absolutely$\}$. Furthermore, $P_c$ can be characterized by $K = \ker(c)$ only, as $P_c = \{a \in M : a = p_c(x) = \sum_{s\in G/K} c_s{}^s x$, for some $x \in M^K$, and it converges absolutely$\}$. We can see immediately that the Poincaré sums we encountered in the two countable group cases we have investigated are just two specific examples of this general definition, which confirms that our definition is good. Under that definition, Theorem 6.3.1 can be translated into the statement $M_c/P_c = 1$, i.e., $M_c$ is generated by Poincaré sums, for any cocycle $c$.

# 2 Preliminaries

## 2.1 Cohomology

The concepts of cohomology groups and nonabelian cohomology are introduced in [27], [26] and [15], which we refer to for definitions and basic properties of cohomology throughout this section.

Let $G$ be a group and $A$ be a left $G$-module. The action of $G$ on $A$ is given by $(s, a) \mapsto {}^s a$, $\forall s \in G, a \in A$. We have ${}^1 a = a$, ${}^s(a + b) = {}^s a + {}^s b$, and ${}^{st}a = {}^s({}^t a)$, where $1 \in G$ is the identity element in the group $G$. Let $A^G$ be the submodule of all the elements fixed by $G$.

Denote by $C^n(G, A)$ the set of $n$-cochains, i.e., the set of all maps of $G^n$ to $A$. If $G$ and $A$ are topological groups, cochains are further required to be continuous. $C^0(G, A)$ is defined to be $\{1\}$, the identity element of $G$. And the coboundary maps are defined as:

$$d_{n+1} : C^n(G, A) \longrightarrow C^{n+1}(G, A)$$

with

$$\begin{aligned}(d_{n+1}f)(s_1,\cdots,s_{n+1}) &= {}^{s_1}f(s_2,\cdots,s_{n+1}) \\ &\quad +\sum_{i=1}^{n}(-1)^i f(s_1,\cdots,s_is_{i+1},\cdots,s_{n+1}) \\ &\quad +(-1)^{n+1}f(s_1,\cdots,s_n).\end{aligned}$$

We have $d_{n+1}\circ d_n = 0$ and $\operatorname{im} d_n \subseteq \ker d_{n+1}$. Let $Z^n(G,A) = \ker d_{n+1}$ be the group of cocycles, and $B^n(G,A) = \operatorname{im} d_n$ be the group of coboundaries, then the $n$-th cohomology group is defined by $H^n(G,A) = Z^n(G,A)/B^n(G,A)$.

It is easy to see that $H^0(G,A) = A^G$, and $H^1(G,A) = Z^1(G,A)/B^1(G,A)$ with

$$Z^1(G,A) = \{f : G \to A | f(st) = f(s) + {}^sf(t)\}$$

$$B^1(G,A) = \{f : G \to A | f(s) = {}^sb - b \text{ for some } b \in A\}.$$

Thus $H^1(G,A)$ is the group of equivalent classes of crossed-homomorphisms of $G$ into $A$. For $H^2(G,A)$, $H^2(G,A) = Z^2(G,A)/B^2(G,A)$, where

$$Z^2(G,A) = \{f : G \to A | f(st,u) + f(s,t) = f(s,tu) + {}^sf(s,t)\}$$

$$B^2(G,A) = \{f : G \to A | f(s,t) = g(s) - g(st) + {}^sg(t) \text{ for some 1-cochain } g\}.$$

Given an exact sequence of $G$-groups

$$1 \to A \to B \to C \to 1$$

we can get a long exact sequence of cohomology groups:

$$1 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to$$

$$\to H^1(G,B) \to H^1(G,C) \to H^2(G,A) \to H^2(G,B) \to H^2(G,C) \to \cdots$$

Now let us turn to the case when $A$ is nonabelian. Let the action of $G$ on $A$ be a left action. In this case, we can only define $H^0(G,A)$ and $H^1(G,A)$.

$H^0(G,A)$ is defined again as the group $A^G$ of all the elements of $A$ fixed by $G$. Now define a cocycle as a map $c : G \to A$ with $s \mapsto c_s$, such that $c_{st} = c_s{}^sc_t$, $\forall s,t \in G$. Denote by $Z^1(G,A)$ the set of all cocycles. Call two cocycles $c$ and $c'$ cohomologous, or equivalent, denoted by $c \sim c'$, if there exists $u \in A$ such that $c'_s = u^{-1}c_s{}^su$ for all $s \in G$. It is an

equivalence relation on $Z^1(G, A)$. Then the cohomology set of $G$ with value in $A$ is defined as the quotient set:

$$H^1(G, A) = Z^1(G, A)/\sim$$

If $A$ is abelian, this definition coincides with the definition of the first cohomology group for the abelian case. Notice that $Z^1(G, A)$ and $H^1(G, A)$ may not be groups if $A$ is nonabelian. However, there is a distinguished element, which is the class of the unit cocycle $c$ with $c_s = 1$, $\forall s \in G$, and we regard $H^1(G, A)$ as a pointed set.

A $G$-group homomorphism $f : A \to B$ induces the following maps:

$$f_0 : H^0(G, A) \to H^0(G, B)$$

$$f_1 : H^1(G, A) \to H^1(G, B)$$

where $f_0$ is the restriction of $f$ to $A^G$, and $f_1$ is defined by $f_1([c]) = [f_1(c)]$ with $f_1(c)_s = f(c_s)$, $\forall s \in G$. One can show that they are well-defined.

$f_0$ is a group homomorphism but $f_1$ is a morphism of pointed sets, which means that $f_1$ sends the distinguished element of $H^1(G, A)$ to the distinguished element of $H^1(G, B)$. We can also consider an exact sequence of pointed sets, if we define kernel of a morphism of pointed sets as the pre-image of the distinguished element.

**Proposition 2.1.1.** ([26],p.125) Let $1 \to A \to B \to C \to 1$ be an exact sequence on nonabelian $G$-groups. Then we have the following exact sequence of pointed sets:

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

In general that exact sequence does not extend to $H^2$. However, if $A$ is in the center of $B$, then $A$ is abelian, so $H^2(G, A)$ is defined and the long exact sequence can be extended up to $H^2(G, A)$.

For a $G$-group $A$, we can define a new action of $G$ on $A$ twisted by a 1-cocycle. Take any $c \in Z^1(G, A)$, denote by ${}_cA$ the set $A$ on which $G$ acts by the formula

$${}^{s'}a = c_s {}^s a c_s^{-1}, \forall s \in G, a \in A$$

where ${}^{s'}a$ denotes the new action of $s$ on $a$. In this case, one says that ${}_cA$ is obtained by twisting $A$ using the cocycle $c$.

**Proposition 2.1.2.** ([27]) Let $c \in Z^1(G, A)$, and let $A' = {}_cA$. To each cocycle $d_s$ in $A'$ we associate $d_s c_s$, which is a cocycle of $G$ in $A$. Thus we have bijections

$$t_c : Z^1(G, A') \longrightarrow Z^1(G, A)$$

and

$$\tau_c : H^1(G, A') \longrightarrow H^1(G, A)$$

induced by $t_c$, mapping the neutral element of $H^1(G, A')$ into the class of $c$.

## 2.2 Poincaré Series

We can find the Poincaré's idea about Poincaré series in [7] and [28]. Now let us follow the definitions and theorems from Gunning's book ([7]). Denote the upper half plane by $\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im} z > 0\}$, and we know that the only conformal automorphisms of $\mathfrak{H}$ are the linear fractional transformations:

$$T : z \longmapsto \frac{az + b}{cz + d}$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix in $\mathrm{SL}_2(\mathbb{R})$. Define the inhomogeneous modular group $\Gamma$ to be the group of linear fractional transformations associated to integral matrices, then we have that $\Gamma$ is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$. Let $G$ be a subgroup of finite index in $\Gamma$. Call a transformation $T$ parabolic if it has only one fixed point on the real line or at $\infty$, and call a fixed point of a parabolic transformation in $G$ a parabolic vertex, or a cusp of $G$.

**Definition 2.2.1.** An unrestricted modular form of weight $2k$ for $G$ is a meromorphic function $f(z)$ on $\mathfrak{H}$ such that $f\left(\frac{az+b}{cz+d}\right) = (cz + d)^{2k} f(z)$ for any transformation $T \in G$ with $T(z) = \frac{az+b}{cz+d}$, where $k$ is an integer.

Denote $J_T(z) = \frac{dT}{dz} = (cz + d)^{-2}$, then we can write the above equation as $f(T(z)) = J_T(z)^{-k} f(z)$. The local coordinate at $i\infty$ is $\zeta = e^{2\pi i z/q}$, where $q$ is the least positive integer such that the translation $z \mapsto z+q$ is in $G$. Let $\hat{f}(\zeta) = f(z)$, then we call that an unrestricted modular form $f(z)$ is holomorphic at $\infty$ if $\hat{f}(\zeta)$ is holomorphic in $|\zeta| < 1$. Moreover, $\hat{f}(\zeta)$ admits a Taylor expansion in $\zeta$:

$$\hat{f}(\zeta) = \sum_{m=0}^{\infty} a_m \zeta^m$$

which induces a Fourier expansion for $f(z)$:

$$f(z) = \sum_{m=0}^{\infty} a_m e^{2\pi imz/q}.$$

For a parabolic fixed point $p$ of $G$, which is not $\infty$, $f(z)$ is called holomorphic at $p$ if $g(z)$ is holomorphic at $\infty$, where $g(z) = J_{S^{-1}}(z)^k f(S^{-1}z)$ with some $S \in \Gamma$ mapping $p$ to $\infty$.

**Definition 2.2.2.** A modular form is an unrestricted modular form which is holomorphic at all points of $\mathfrak{H}$ and at all parabolic vertices of the group.

**Definition 2.2.3.** The Poincaré series of weight $2k$ and of character $\nu$ for $G$ is the series

$$\phi_\nu(z) = \sum_{T \in \mathcal{R}} e^{2\pi i\nu T(z)/q} J_T(z)^k$$

where $\nu$ is nonnegative integer, $\mathcal{R}$ is the set of coset representatives of $G$ mod $G_0$, and $G_0$ is the infinite cyclic subgroup of translation in $G$, generated by the least translation $T : z \mapsto z + q$ in $G$.

**Definition 2.2.4.** A cusp form of weight $2k$ for $G$ is a modular form of weight $2k$ for $G$ which vanishes at all parabolic vertices (cusps).

It is known that the set of cusp forms of weight $k$ for $G$ forms a finite dimensional Hilbert space with the Petersson Inner Product:

$$< f, g >:= \int_D f(z)\overline{g(z)} y^{2(k-1)} dxdy$$

where $D$ is a fundamental domain for $G$.

**Theorem 2.2.1.** The Poincaré series

$$\phi_\nu(z) = \sum_{T \in \mathcal{R}} e^{2\pi i\nu T(z)/q} (cz + d)^{-2k}$$

converges absolutely and uniformly on compact subsets of $\mathfrak{H}$, for $\nu > 0$ and $k \geq 1$, and for $\nu = 0$ and $k > 1$. $\phi_\nu(z)$ converges absolutely and uniformly on every fundamental domain $D$ for $G$ and represents a modular form of weight $2k$ for $G$. Further,

- $\phi_0(z)$ is zero at all finite parabolic vertices, nonzero at $i\infty$.
- $\phi_\nu(z)$ is a cusp form for $\nu \geq 1$.

**Theorem 2.2.2.** Every cusp form is a linear combination of the Poincaré series $\phi_\nu(z)$, $\nu \geq 1$.

# 3 Triple System $(\mathcal{G}, (G, M))$

## 3.1 Triple System $(\mathcal{G}, (G, M))$

Now I introduce the triple system $(\mathcal{G}, (G, M))$, and will explain in the next section why it is a general setting for considering analogies to Theorem 2.2.2. Let $G$ be a group and $M$ be a left $G$-module. Consider a finite group $\mathcal{G}$ which acts naturally on $(G, M)$. In other words, we assume that $G$ is a left $\mathcal{G}$-group, $M$ is a left $\mathcal{G}$-module so that ${}^\sigma(sx) = {}^\sigma s\, {}^\sigma x$, $\forall \sigma \in \mathcal{G}, s \in G, x \in M$. Let $c$ be a cocycle of $\mathcal{G}$ in $G$. By definition, $c$ is a map $\mathcal{G} \to G$ such that $c_{\sigma\tau} = c_\sigma{}^\sigma c_\tau$, $\forall \sigma, \tau \in \mathcal{G}$. For a cocycle $c$, we associate a $\mathbb{Z}$-module $M_c$ by

$$M_c = \{x \in M : c_\sigma{}^\sigma x = x, \forall \sigma \in \mathcal{G}\}.$$

As the group $\mathcal{G}$ is finite, we can speak of a sum

$$p_c(x) = \sum_{\tau \in \mathcal{G}} c_\tau{}^\tau x, \quad x \in M.$$

We shall put

$$P_c = \{y = p_c(x) : x \in M\}.$$

One verifies that

$$|\mathcal{G}| M_c \subseteq P_c \subseteq M_c$$

where $|\mathcal{G}|$ is the order of $\mathcal{G}$. Denote by $Z^1(\mathcal{G}, G)$ the set of all cocycles of $\mathcal{G}$ in $G$. Two cocycles $c$, $c'$ are called equivalent $c \sim c'$ if there is a $u \in G$ such that $c'_\sigma = u^{-1} c_\sigma{}^\sigma u, \forall \sigma \in \mathcal{G}$. One verifies that the map $x \mapsto u^{-1}x$ induces an isomorphism of factor modules: $M_c/P_c \simeq M_{c'}/P_{c'}$. Consequently the structure of the module $M_c/P_c$ depends only on the cohomology class $\gamma = [c]$ in the (first) cohomology set $H^1(\mathcal{G}, G) = Z^1(\mathcal{G}, G)/\sim$.

If we put $c = 1$, we have

$$M_1 = M^{\mathcal{G}}, \quad P_1 = N(M)$$

and so

$$M_1/P_1 = \hat{H}^0(\mathcal{G}, M)$$

Then for a general $\gamma = [c] \in H^1(\mathcal{G}, G)$, we have a right to make identification

$$M_c/P_c = \hat{H}^0(\mathcal{G}, M)_\gamma$$

the Tate group twisted by $\gamma$.

### 3.2 Poincaré Series Revisited

Theorem 2.2.2 can be seen from the point of view of a triple system $(\mathcal{G}, (G, M))$. Let $\mathcal{O}(\mathfrak{H})$ be the ring of holomorphic functions on $\mathfrak{H}$, $\mathcal{G}$ be a subgroup of finite index in $\mathrm{PSL}_2(\mathbb{Z})$, $G$ be $\mathcal{O}(\mathfrak{H})^\times$, the group of invertible elements in $\mathcal{O}(\mathfrak{H})$, and $M$ be the subring of all the elements in $\mathcal{O}(\mathfrak{H})$ which vanish at all cusps. Then $\mathcal{G}$ has a natural action on either $M$ or $G$:

$${}^s f(z) = f({}^{s^{-1}}z) = f\left(\frac{az+b}{cz+d}\right), \forall f \in M \cup G, z \in \mathfrak{H}, s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathcal{G}.$$

For an integer $k$, define $c : \mathcal{G} \to G$ by $c_s(z) = (cz+d)^{-2k}$ for $\forall z \in \mathfrak{H}, s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathcal{G}$. Then $c$ is a 1-cocycle in $Z^1(\mathcal{G}, G)$. It is not hard to check. For any two elements in $\mathcal{G}$, $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$ and $t = \begin{pmatrix} e & f \\ g & h \end{pmatrix}^{-1}$, and any $z \in \mathfrak{H}$, we have

$$\begin{aligned} c_s(z)\ {}^s c_t(z) &= (cz+d)^{-2k}\ {}^s(gz+h)^{-2k} \\ &= (cz+d)^{-2k}\left(g\frac{az+b}{cz+d}+h\right)^{-2k} \\ &= (g(az+b)+h(cz+d))^{-2k} \\ &= ((ag+ch)z+(bg+dh))^{-2k} \\ &= c_{st}(z) \end{aligned}$$

because $(st)^{-1} = t^{-1}s^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ae+cf & be+df \\ ag+ch & bg+dh \end{pmatrix}$.

Now if we denote the space of cusp forms of weight $2k$ by $M_c$, we have

$$M_c = \left\{ f \in M \middle| (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) = f(z) \right\}.$$

Then the condition $(cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) = f(z)$ can be rewritten as $c_s\, {}^s f(z) = f(z)$. Therefore Theorem 2.2.2 just says that $M_c$ is generated by Poincaré sums.

Moreover, we notice that

$$\begin{aligned}\phi_\nu(z) &= \sum_{T\in\mathcal{R}} e^{2\pi i\nu T(z)/q}(cz+d)^{-2k} \\ &= \sum_{s\in\mathcal{R}} c_s(z)\ {}^s g(z)\end{aligned}$$

where $g(z) = e^{2\pi i\nu z/q}$, $\nu \geq 1$. This result may be needed in Section 6.4 to explore the general formulation of a triple system when $\mathcal{G}$ is countable.

### 3.3 A Simple Example

To investigate the triple system in other circumstances, it is very natural to begin with a cyclic group $\mathcal{G}$. So first I examine a triple system $(\mathcal{G}, (G, M))$ with $\mathcal{G} =< \theta >$, a cyclic group of order two. Now let $G = \mathrm{SL}_2(\mathbb{Z})$, and $M = \mathrm{sl}_2(\mathbb{Z})$, the Lie algebra of $G$. Let $G$ act on $M$ by conjugation, $g \circ x = gxg^{-1}$, $\forall g \in G$, $x \in M$. And the action of $\mathcal{G}$ on $M_2(\mathbb{Z})$ is given by:

$${}^\theta x = x^{*t} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}, \text{ if } x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$$

where $x^*$ is the companion matrix of $x$, and $x^t$ is its transpose.

If restricted to $G$, this action becomes ${}^\theta x = x^{-t}$, $\forall x \in G$. It is easy to see that ${}^\theta(xy) = {}^\theta x {}^\theta y$, ${}^{\theta\theta}x = x$, ${}^\theta G = G$, ${}^\theta M = M$.

What is its $H^1(\mathcal{G}, G)$ then? It is obvious that $Z^1(\mathcal{G}, G) = \{c \in G | c^\theta c = 1\}$. $\forall c \in G$, $c^\theta c = 1 \iff cc^{-t} = 1 \iff c = c^t$. Thus $Z^1(\mathcal{G}, G) = \{c \in G | c = c^t\}$. For $\forall c, c' \in Z^1(\mathcal{G}, G)$, $c \sim c' \iff \exists g \in G, c' = g^{-1}c^\theta g \iff \exists u \in G, c' = u^t cu$, by putting $u = {}^\theta g$. Thus $H^1(\mathcal{G}, G) = \{c \in G | c = c^t\}/\sim$, where the equivalence relation is given by congruence in $G$.

Because symmetric matrices in $\mathrm{SL}_2(\mathbb{Z})$ can be identified with integral quadratic forms with discriminant $-4$, by Gauss Correspondence, there is a bijection

$$i_K : H_K^+ \xrightarrow{\sim} \{c \in G | c = c^t \text{ and } c \text{ is positive definite}\}/\sim$$

with $K = \mathbb{Q}(\sqrt{-1})$. But $H_K^+ = H_K = 1$ for $K = \mathbb{Q}(\sqrt{-1})$, thus $\forall c \in Z^1(\mathcal{G}, G) = \{c \in G | c = c^t\}$, either $c$ or $-c$ is positive definite and congruent to $I$. Hence $c$ is congruent to either $I$ or $-I$. Notice that any positive definite matrix is still positive definite after congruence, thus $I$ and $-I$ are not congruent to each other, so we get that $H^1(\mathcal{G}, G) = \{[I], [-I]\}$.

Now we can consider $M_c/P_c$ for $\forall[c] \in H^1(\mathcal{G}, G)$. But either for $c = I$ or $c = -I$, $c \circ x = x$, $\forall x \in M$. Thus for $\forall[c] \in H^1(\mathcal{G}, G)$, $M_c = \{x \in M | {}^\theta x = x\} = \{x = \begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix} \in M_2(\mathbb{Z})\} = J\mathbb{Z}$, where $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $P_c = \{x + {}^\theta x | x \in M\} = \{x = \begin{pmatrix} 0 & \beta - \gamma \\ \gamma - \beta & 0 \end{pmatrix} \in M_2(\mathbb{Z})\} = J\mathbb{Z}$. Therefore $M_c/P_c = 1$, $\forall[c] \in H^1(\mathcal{G}, G)$.

This example is only for $\mathrm{SL}_2(\mathbb{Z})$ and a cyclic group of order two. Can we get more general results? It is very natural to ask this kind of question. Notice that we use the Gauss Correspondence to solve the question, and in order to get more general results, we need to generalize the Gauss Correspondence. It is what I will talk about in the next chapter.

# 4 G.C. and LMT Theorem

## 4.1 Gauss Theory of Quadratic Forms

Before going to our generalization of the Gauss Correspondence, first let us recall some standard notions on quadratic fields and quadratic forms, and introduce the well known Gauss Correspondence. After that, in the next section, I will then introduce the LMT Theorem.

Let $m(\neq 0, 1)$ be a square-free integer and $K = \mathbb{Q}(\sqrt{m})$, where $\mathbb{Q}$ denotes the field of rational numbers. Denote by $\Delta_K$ the discriminant of $K$. If we put

$$\omega = \begin{cases} \sqrt{m}, & m \equiv 2, 3 \pmod 4 \\ (1 + \sqrt{m})/2, & m \equiv 1 \pmod 4 \end{cases}$$

,then $\{1, \omega\}$ form the canonical basis of the ring $\mathcal{O}_K$ of integers, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega = [1, \omega]$. We have

$$\Delta_K \stackrel{\text{def}}{=} \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2 = \begin{cases} 4m, & m \equiv 2, 3 \pmod 4 \\ m, & m \equiv 1 \pmod 4 \end{cases}$$

,where $\omega'$ is the conjugate of $\omega$. We denote by $I_K$ the group of fractional ideals of $K$, by $P_K$ the subgroup of $I_K$ of principal ideals. Furthermore, we put

$$P_K^+ = \{\mathbf{a} = (\alpha) \in P_K : N\alpha > 0\}.$$

We have

$$[P_K : P_K^+] = \begin{cases} 1, & m < 0 \text{ or } m > 0, \exists \varepsilon \in \mathcal{O}_K^\times, N\varepsilon = -1 \\ 2, & m > 0, N\varepsilon = 1, \forall \varepsilon \in \mathcal{O}_K^\times \end{cases} \tag{6}$$

Next, we define the factor groups:

$$H_K = I_K/P_K, \quad h_K = \#H_K;$$
$$H_K^+ = I_K/P_K^+, \quad h_K^+ = \#H_K^+.$$

Hence, $h_K^+ = h_K$ or $2h_K$ by (6). $h_K$ is the class number of $K$ and $h_K^+$ is the class number of $K$ in the narrow sense. We denote the equivalence of ideals mod $P_K$ (resp. mod $P_K^+$) by $\mathbf{a} \sim \mathbf{b}$ (resp. $\mathbf{a} \overset{+}{\sim} \mathbf{b}$).

Now, let us turn to quadratic forms. Consider a quadratic form

$$f = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}.$$

Assume that the discriminant $\Delta_f = b^2 - 4ac \neq 0$. One can write

$$f(z) = z^t F z, \text{ with } z = \begin{pmatrix} x \\ y \end{pmatrix}, F = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

We introduce two equivalence relations $\sim$ and $\overset{+}{\sim}$. Let $g = a'x^2 + b'xy + c'y^2$ be another integral quadratic form with the matrix $G$. The two equivalence relations are defined as follows:

$$f \sim g \overset{\text{def}}{\Longleftrightarrow} g(z) = f(\gamma z), \quad \exists \gamma \in GL_2(\mathbb{Z});$$
$$f \overset{+}{\sim} g \overset{\text{def}}{\Longleftrightarrow} g(z) = f(\gamma z), \quad \exists \gamma \in SL_2(\mathbb{Z}).$$

Obviously $f \overset{+}{\sim} g \Rightarrow f \sim g$, but the converse is not true.

For a fixed quadratic field $K$, consider the set

$$Q(\Delta_K) = \left\{ f = ax^2 + bxy + cy^2 : \begin{array}{l} a, b, c \in \mathbb{Z}, \\ \Delta_f = \Delta_K (f > 0 \text{ if } \Delta_K < 0) \end{array} \right\}.$$

Since the equivalence $\overset{+}{\sim}$ makes sense in $Q(\Delta_K)$, we can consider the quotient:

$$\tilde{Q}(\Delta_K) = Q(\Delta_K)/\overset{+}{\sim}.$$

Now we introduce the Gauss Correspondence.

**Theorem 4.1.1.** (Gauss, [6]) There is a bijection $i_K : H_K^+ \xrightarrow{\sim} \tilde{Q}(\Delta_K)$.

Here, the map $i_K$ is the following. We agree to orient a basis of an ideal $\mathbf{a} = [\alpha, \beta]$ by the rule:

$$\begin{cases} \begin{vmatrix} \beta & \beta' \\ \alpha & \alpha' \end{vmatrix} > 0 \quad \text{if } m > 0, \\ \\ \frac{1}{i} \begin{vmatrix} \beta & \beta' \\ \alpha & \alpha' \end{vmatrix} > 0 \quad \text{if } m < 0. \end{cases}$$

Then, $i_K$ is the one induced by

$$\mathbf{a} \mapsto f_{\mathbf{a}} = \frac{N(x\alpha + y\beta)}{N\mathbf{a}}$$

Thanks to $i_K$, one can define a group structure in the set $\tilde{Q}(\Delta_K)$. Gauss (1801) defined directly a group structure in $\tilde{Q}(\Delta_K)$ (the composition theory of quadratic forms, see [6]). The notion of ideals was introduced by Dedekind (1871, see [4]).

## 4.2 Latimer-MacDuffee-Taussky Theorem

The Latimer-MacDuffee-Taussky Theorem (LMT Theorem, see [12],[29]) was originally stated over the ring $\mathbb{Z}$. But actually it is also true over any ring of integers, when it is a PID. In the following, I will state it and prove it in this general setting.

Let $k$ be a number field (local or global), and $\mathcal{O}_k$ be its ring of integers. Let $f(t) \in \mathcal{O}_k[t]$ be a monic irreducible polynomial of degree $n$ over $k$. Consider the matrix algebra $M_n(\mathcal{O}_k)$.

**Lemma 4.2.1.** For any matrix $A \in M_n(\mathcal{O}_k)$ satisfying $f(A) = 0$, its minimal polynomial and characteristic polynomial are both equal to $f$.

**Pf.** Suppose the minimal polynomial of $A$ is $q(t)$, then $q|f$ over $k$, for $f(A) = 0$. But $f$ is irreducible and they are both monic, so $q = f$. Notice that we also proved that $q(t) \in \mathcal{O}_k[t]$ here.

Let $\chi(t) = \det(tI - A)$ be the characteristic polynomial of $A$. Then we have $\chi(A) = 0$, and then $q|\chi$. In view of $\deg(q) = \deg(f) = n = \deg(\chi)$, we get $q = \chi$, because $\chi$ is also monic. $\square$

Now we introduce two equivalence relations on $M_n(\mathcal{O}_k)$. Let $A, B \in M_n(\mathcal{O}_k)$, the equivalence relations are defined as follows:

$$A \sim B \overset{\text{def}}{\Longleftrightarrow} B = TAT^{-1}, \quad \exists T \in GL_n(\mathcal{O}_k)$$

$$A \overset{+}{\sim} B \overset{\text{def}}{\Longleftrightarrow} B = TAT^{-1}, \quad \exists T \in SL_n(\mathcal{O}_k)$$

where $GL_n(\mathcal{O}_k) = \{X \in M_n(\mathcal{O}_k) : \det(X) \in \mathcal{O}_k^{\times}\}$, and $SL_n(\mathcal{O}_k) = \{X \in M_n(\mathcal{O}_k) : \det(X) = 1$.

Of course when $A \sim B$, the characteristic polynomial of $A$ and $B$ are the same. And if further $f(A) = 0$, then $f(B) = 0$.

For a fixed monic irreducible polynomial $f$, consider the set

$$M_n(\mathcal{O}_k; f) = \{A \in M_n(\mathcal{O}_k) : f(A) = 0\}.$$

Since the equivalences $\sim$, $\overset{+}{\sim}$ defined above make sense in $M_n(\mathcal{O}_k; f)$, we can consider the quotients $M_n(\mathcal{O}_k; f)/\sim$ and $M_n(\mathcal{O}_k; f)/\overset{+}{\sim}$. Denote

$$\tilde{M}_n(\mathcal{O}_k; f) = M_n(\mathcal{O}_k; f)/\sim$$

$$\tilde{M}_n^{+}(\mathcal{O}_k; f) = M_n(\mathcal{O}_k; f)/\overset{+}{\sim}$$

On the other side, let $\theta \in \overline{\mathcal{O}_k}$ satisfying $f(\theta) = 0$, where $\overline{\mathcal{O}_k}$ is an integral closure of $\mathcal{O}_k$. Take $K = k(\theta)$, then $[K : k] = n$. And let $\mathcal{O} = \mathcal{O}_k[\theta]$ be an order in $\mathcal{O}_K$. Denote by $I_{\mathcal{O}}$ the set of all integral ideals of $\mathcal{O}$. Again we introduce an equivalence relation in $I_{\mathcal{O}}$. Let $\mathbf{a}, \mathbf{b}$ be any two ideals contained in $\mathcal{O}$, the equivalence relation is defined as the following:

$$\mathbf{a} \sim \mathbf{b} \overset{\text{def}}{\Longleftrightarrow} \exists \alpha, \beta \in \mathcal{O}, \alpha \neq 0, \beta \neq 0, s.t. \quad \alpha\mathbf{a} = \beta\mathbf{b}$$

Then the ideal class set of the order $\mathcal{O}$ is defined as:

$$\tilde{I}_{\mathcal{O}} = I_{\mathcal{O}}/\sim$$

It is the ideal class group $H_K$ when $\mathcal{O} = \mathcal{O}_K$.

Now, it is the time to introduce the generalized form of the Latimer-MacDuffee-Taussky Theorem.

**Theorem 4.2.1.** (Latimer-MacDuffee-Taussky, [12], [29]) If $\mathcal{O}_k$ is a PID, then we have a bijection $\varphi : \tilde{M}_n(\mathcal{O}_k; f) \xrightarrow{\sim} \tilde{I}_{\mathcal{O}}$.

**Pf.** Given any $[A] \in \tilde{M}_n(\mathcal{O}_k; f)$, let the characteristic polynomial of $A$ be $\chi(t) = \det(tI - A)$. Then by Lemma 4.2.1, we know $f(t) = \chi(t) = \det(tI - A)$. But $f(\theta) = 0$, so we have

$$\det(\theta I - A) = 0$$

Thus $\theta$ is an eigenvalue of $A$. So we have

$$\exists\, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{O}^n, x \neq 0, s.t. \quad Ax = \theta x.$$

Here we know there exists such an eigenvector $x$ in $K^n$. But after multiplying an appropriate number in $\mathcal{O}_k$, it can be taken from $\mathcal{O}^n$.

Such an eigenvector is unique up to a multiple of an element in $K$. The reason is as follows. The polynomial $f(t)$ is irreducible, thus $f(t)$ and $f'(t)$ are coprime, and $f(t)$ does not have any multiple root. So $\theta$ is an eigenvalue of multiplicity one of $A$, and the eigenspace of $\theta$ is one dimensional over $K$.

Define $\varphi([A]) = [\mathbf{a}]$, where $\mathbf{a} = [x_1, \ldots, x_n]_{\mathcal{O}_k} \subseteq \mathcal{O}$. $\mathbf{a}$ is an ideal in $\mathcal{O}$, for we have $Ax = \theta x$. If any $[B] = [A] \in \tilde{M}_n(\mathcal{O}_k; f)$, then $\exists\, T \in GL_n(\mathcal{O}_k)$, such that $B = TAT^{-1}$. So we have $T^{-1}BT = A$, and $T^{-1}BTx = Ax = \theta x$, thus $BTx = \theta Tx$. Let $y = (y_1, \ldots, y_n)^t = Tx$, then we have $By = \theta y$, and $\varphi([B]) = [y_1, \ldots, y_n]_{\mathcal{O}_k} = [x_1, \ldots, x_n]_{\mathcal{O}_k} = \mathbf{a}$. So the definition of $\varphi$ doesn't depend on the choice of $A$.

The definition of $\varphi$ doesn't depend on the choice of $x$, too. As we mentioned before, the choice of $x$ is unique up to a multiple of an element in $K$. So if we have $x = (x_1, \ldots, x_n)^t, y = (y_1, \ldots, y_n)^t \in \mathcal{O}^n, x \neq 0, y \neq 0$ and $Ax = \theta x$, $Ay = \theta y$, then there exists some nonzero $\gamma \in K$, such that $y = \gamma x$. Let $\gamma = \alpha/\beta$, with $\alpha, \beta \in \mathcal{O}$, then $\alpha \neq 0, \beta \neq 0$, and $\alpha x = \beta y$, i.e., $(\alpha x_1, \ldots, \alpha x_n)^t = (\beta y_1, \ldots, \beta y_n)^t$. So we have $\alpha[x_1, \ldots, x_n]_{\mathcal{O}_k} = \beta[y_1, \ldots, y_n]_{\mathcal{O}_k}$, i.e., $[x_1, \ldots, x_n]_{\mathcal{O}_k} \sim [y_1, \ldots, y_n]_{\mathcal{O}_k}$.

In all, the definition of $\varphi$ doesn't depend on the choice of $A$ and $x$. Hence $\varphi$ is well-defined.

Now we are going to prove the mapping $\varphi$ is bijective.

- $\varphi$ is injective.

  Suppose $\varphi([A]) = \mathbf{a} = [x_1, \ldots, x_n]_{\mathcal{O}_k}$, $\varphi([B]) = \mathbf{b} = [y_1, \ldots, y_n]_{\mathcal{O}_k}$, with $x = (x_1, \ldots, x_n)^t, y = (y_1, \ldots, y_n)^t \in \mathcal{O}^n$, and $Ax = \theta x$, $By = \theta y$. If $[\mathbf{a}] = [\mathbf{b}]$, then there exist $\alpha, \beta \in \mathcal{O}$, $\alpha \neq 0, \beta \neq 0$, such that $\alpha\mathbf{a} = \beta\mathbf{b}$, i.e., $[\alpha x_1, \ldots, \alpha x_n]_{\mathcal{O}_k} = [\beta y_1, \ldots, \beta y_n]_{\mathcal{O}_k}$. Then $\{\alpha x_1, \ldots, \alpha x_n\}$ and $\{\beta y_1, \ldots, \beta y_n\}$ are two integral bases for the same integral ideal in $\mathcal{O}$. So the transformation matrix from one basis to the other

is in $GL_n(\mathcal{O}_k)$. Denote the transformation matrix from the former to the latter by $U \in GL_n(\mathcal{O}_k)$, we have

$$\beta y = U\alpha x \tag{7}$$

Multiply both sides of (7) by $B$ to the left, we get

$$B\beta y = BU\alpha x = \beta By = \beta\theta y = \theta\beta y$$

Multiply both sides of (7) by $\theta$, we get

$$\theta\beta y = \theta U\alpha x = U\alpha\theta x = U\alpha Ax = UA\alpha x$$

Combining the above two, we get

$$BU\alpha x = UA\alpha x$$

i.e.

$$BUx = UAx \tag{8}$$

where $x = (x_1, \ldots, x_n)^t$.

Remind that $\{x_1, \ldots, x_n\}$ forms an integral basis for $\mathbf{a}$, it is linearly independent over $\mathcal{O}_k$. So from (8), we have

$$BU = UA$$

i.e., $B = UAU^{-1}$, $A \sim B$.

- $\varphi$ is surjective.

  For any $[\mathbf{a}] \in \tilde{I}_{\mathcal{O}}$, where $\mathbf{a}$ is an integral ideal in $\mathcal{O}$, $\mathbf{a}$ is a lattice over $\mathcal{O}_k$, for $\mathbf{a} \subseteq \mathcal{O}$, and $\mathcal{O}_k$ is a PID. And $\mathrm{rank}_{\mathcal{O}_k}(\mathbf{a}) = n$, for there exists an injection from $\mathcal{O}$ to $\mathbf{a}$. Let $\{x_1, \ldots, x_n\}$ be an integral basis for $\mathbf{a}$. Then for $i = 1, 2, \ldots, n$, $\theta x_i \in \mathbf{a}$, and it can be expressed as a linear combination of $\{x_1, \ldots, x_n\}$. Using matrix notation, the above statement becomes

  $$\exists\, A \in M_n(\mathcal{O}_k), \text{s.t. } \theta x = Ax$$

  Further, we have

  $$f(\theta)x = f(A)x = 0$$

Remind that $\{x_1, \ldots, x_n\}$ forms an integral basis for $\mathbf{a}$, by the same argument as before, we get

$$f(A) = 0$$

It is the $A$ that we want, with it satisfying $\varphi([A]) = [\mathbf{a}]$. $\square$

From this theorem, one can define a group structure in the set $\tilde{M}_n(\mathcal{O}_k; f)$ as what one has done for $\tilde{Q}(\Delta_K)$ when $\mathcal{O} = \mathcal{O}_K$. But no one has defined such a group structure yet.

When $k = \mathbb{Q}$, $\mathcal{O}_k = \mathbb{Z}$. Take $f(t) = t^2 - m$, where $m(\neq 0, 1)$ is a square-free integer and $m \equiv 2, 3 \pmod 4$. Then $f(t)$ is irreducible by Eisenstein Criterion. Let $\theta = \sqrt{m}$, then $K = \mathbb{Q}(\sqrt{m})$, $\mathcal{O} = \mathbb{Z}[\sqrt{m}] = \mathcal{O}_K$, and $\tilde{I}_{\mathcal{O}} = H_K$. So LMT tells us that there is a bijection between $\tilde{M}_n(\mathbb{Z}; f)$ and $H_K$, which is quite similar to Gauss Correspondence.

If we take $f(t) = t^2 - t + \frac{1-m}{4}$, where $m(\neq 0, 1)$ is a square-free integer and $m \equiv 1 \pmod 4$. We know $f(t)$ is irreducible because neither of its roots is in $\mathbb{Q}$. Let $\theta = (1 + \sqrt{m})/2$ be one of its roots, then $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{m})$, $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{m})/2] = \mathcal{O}_K$, and $\tilde{I}_{\mathcal{O}} = H_K$. In this case LMT still tells us that there is a bijection between $\tilde{M}_n(\mathbb{Z}; f)$ and $H_K$, which is again quite similar to Gauss Correspondence.

From those, one may know there should be some link between Gauss Correspondence and LMT Theorem. As I will explain in the next section, Gauss Correspondence is basically a skewed form of LMT Theorem in some special circumstances.

As this section is coming to a close, I need quote here a lemma, which we will use afterwards.

**Lemma 4.2.2.** ([30]) Let $A$ be a matrix with entries in some field. If the characteristic polynomial of $A$ has no multiple roots, the only matrices commuting with it are scalar polynomials in $A$.

## 4.3 Link between G.C. and LMT Theorem

That Gauss Correspondence essentially becomes LMT in $2 \times 2$ matrix case is due to a special matrix:

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{9}$$

This matrix is special because of the following special property:

**Lemma 4.3.1.** Let $R$ be a commutative ring with unity, and let $J \in M_2(R)$ be the matrix in (9), then for any matrix $A \in M_2(R)$, we have $JAJ^{-1} = A^{*t}$, where $A^*$ is the companion matrix of $A$. Moreover, if $A \in SL_2(R) = \{A \in M_2(R) : \det(A) = 1\}$, then $JAJ^{-1} = A^{-t}$.

**Pf.** $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, so $J^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Take any matrix $A \in M_2(R)$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in R$. Then

$$JAJ^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}^t = A^{*t}$$

If $A \in SL_2(R)$, then $AA^* = \det(A) = I$, $A^* = A^{-1}$, so $JAJ^{-1} = A^{-t}$. $\square$

Now we are going to change the form of quadratic forms to the form of matrices. We use the notation $A \overset{c}{\sim} B$ to mean that $\exists T \in SL_2(\mathbb{Z})$, such that $B = TAT^t$, for $\forall A, B \in M_2(\mathbb{Z})$.

As before, let $m(\neq 0, 1)$ be a square-free integer and $K = \mathbb{Q}(\sqrt{m})$. First consider the case $m \equiv 2, 3 \pmod 4$.

**Lemma 4.3.2.** When $m \equiv 2, 3 \pmod 4$, there is a bijection $j$:

$$\tilde{Q}(\Delta_K) \overset{\sim}{\to} \left\{ A \in M_2(\mathbb{Z}) : \begin{array}{l} A = A^t, \\ \det(A) = -m \ (A > 0 \text{ if } m < 0) \end{array} \right\} \Big/ \overset{c}{\sim} \qquad (10)$$

We still denote the right hand side of (10) by $\tilde{Q}(\Delta_K)$.

**Pf.** In this case, $\Delta_K = 4m$. $\forall\, [f] \in \tilde{Q}(\Delta_K)$, $f = ax^2 + b'xy + cy^2$, $a, b', c \in \mathbb{Z}$. Then $\Delta_f = b'^2 - 4ac = \Delta_K = 4m$, so $4|b'^2$, $2|b'$. Put $b = b'/2 \in \mathbb{Z}$. Define $j([f]) = [A]$, where $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$.

Obviously $A \in M_2(\mathbb{Z})$ and $A = A^t$. $b = b'/2$, thus $b' = 2b$, $b'^2 - 4ac = 4b^2 - 4ac = 4m$, so $\det(A) = ac - b^2 = -m$. In view of $\Delta_K = 4m$, we have $\Delta_K < 0 \Leftrightarrow m < 0$. Also we know that $f > 0 \Leftrightarrow A > 0$. So $[A]$ is in the right hand side of (10).

$\forall\, [f], [g] \in \tilde{Q}(\Delta_K)$, $f = ax^2 + 2bxy + cy^2$, $g = a'x^2 + 2b'xy + c'y^2$, and $j([f]) = [A]$, $j([g]) = [B]$, with $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, $B = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$. Then we know that $f \overset{+}{\sim} g \Leftrightarrow A \overset{c}{\sim} B$. So $j$ is well-defined and injective.

Given any $[A]$ in the right hand side of (10), $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, let $f = ax^2 + 2bxy + cy^2$. Note $\det(A) = ac - b^2 = -m$, so $\Delta_f = (2b)^2 - 4ac = 4b^2 - 4ac = 4m = \Delta_K$. As before, for $\Delta_K = 4m$, we have $\Delta_K < 0 \Leftrightarrow m < 0$, and also $f > 0 \Leftrightarrow A > 0$. So we know $[f] \in \tilde{Q}(\Delta_K)$, and $j([f]) = [A]$. $j$ is surjective. $\square$

Now we turn to the case $m \equiv 1 \pmod 4$.

**Lemma 4.3.3.** When $m \equiv 1 \pmod 4$, there is a bijection $j$:

$$\tilde{Q}(\Delta_K) \xrightarrow{\sim} \left\{ A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in M_2(\mathbb{Q}) : \begin{array}{l} a, b, c \in \mathbb{Z}, b \text{ odd} \\ \det(A) = -\frac{m}{4} \\ (A > 0 \text{ if } m < 0) \end{array} \right\} \Big/ \overset{c}{\sim} \tag{11}$$

We still denote the right hand side of (11) by $\tilde{Q}(\Delta_K)$.

**Pf.** In this case, $\Delta_K = m$. $\forall [f] \in \tilde{Q}(\Delta_K)$, $f = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$. Then $\Delta_f = b^2 - 4ac = \Delta_K = m \equiv 1 \pmod 4$, so $b^2 \equiv 1 \pmod 4$, $b$ odd. Define $j([f]) = [A]$, where $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$.

Obviously $A \in M_2(\mathbb{Q})$. We know $\Delta_f = b^2 - 4ac = \Delta_K = m$, so $\det(A) = ac - b^2/4 = -m/4$. For $\Delta_K = m$, we have $\Delta_K < 0 \Leftrightarrow m < 0$. Also we know that $f > 0 \Leftrightarrow A > 0$. So $[A]$ is in the right hand side of (11).

$\forall [f], [g] \in \tilde{Q}(\Delta_K)$, $f = ax^2 + bxy + cy^2$, $g = a'x^2 + b'xy + c'y^2$, and $j([f]) = [A]$, $j([g]) = [B]$, with $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$, $B = \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix}$. Then we know that $f \overset{+}{\sim} g \Leftrightarrow A \overset{c}{\sim} B$. So $j$ is well-defined and injective.

Given any $[A]$ in the right hand side of (11), $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$, let $f = ax^2 + bxy + cy^2$. Note $\det(A) = ac - b^2/4 = -m/4$, so $\Delta_f = b^2 - 4ac = m = \Delta_K$. As before, for $\Delta_K = m$, we have $\Delta_K < 0 \Leftrightarrow m < 0$, and also $f > 0 \Leftrightarrow A > 0$. So we know $[f] \in \tilde{Q}(\Delta_K)$, and $j([f]) = [A]$. $j$ is surjective. $\square$

Next, I am going to show the link between Gauss Correspondence and LMT in a more general setting. Let $f(t) = t^2 - p\,t + q$ be an irreducible polynomial in $\mathbb{Z}[t]$. Its discriminant is $\Delta_f = p^2 - 4q$. Define

$$\tilde{Q}(f) = \left\{ A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in M_2(\mathbb{Q}) : \begin{array}{l} a, b, c \in \mathbb{Z}, b \equiv p \pmod 2 \\ \det(A) = -\frac{\Delta_f}{4} \\ (A > 0 \text{ if } \Delta_f < 0) \end{array} \right\} \Big/ \overset{c}{\sim}$$

It is a generalization of those $\tilde{Q}(\Delta_K)$ before, which can be seen as follows:

- When $m \equiv 2, 3 \pmod 4$, let $f(t) = t^2 - m$. It is irreducible by Eisenstein's Criterion. And its discriminant is $\Delta_f = 4m$. Comparing their definition, obviously $\tilde{Q}(\Delta_K)$ in this case is the same as $\tilde{Q}(f)$.

- When $m \equiv 1 \pmod 4$, let $f(t) = t^2 - t + \frac{1-m}{4}$. It is a polynomial in $\mathbb{Z}[t]$. It is irreducible, because neither of its roots is rational. And its discriminant is $\Delta_f = m$. Comparing their definition, obviously $\tilde{Q}(\Delta_K)$ in this case is still the same as $\tilde{Q}(f)$.

Recall that for $\forall A, B \in M_2(\mathbb{Z})$, we use the notation $A \overset{+}{\sim} B$ to mean that $\exists\, T \in SL_2(\mathbb{Z})$, such that $B = TAT^{-1}$.

Now we are ready to prove the following theorem:

**Theorem 4.3.1.** If $f(t) = t^2 - p\,t + q$ is an irreducible polynomial in $\mathbb{Z}[t]$, then there is a bijection $\lambda$:

$$\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : \begin{array}{l} f(A) = 0 \\ (b > 0 \text{ if } \Delta_f < 0) \end{array} \right\} \Big/ \overset{+}{\sim} \xrightarrow{\sim} \tilde{Q}(f) \tag{12}$$

**Pf.** Given any $[A]$ in the left hand side of (12), define $\lambda([A]) = [(A - \frac{p}{2})J^{-1}]$, where $J$ is the matrix in (9). It is just a linear transformation.

For $A \in M_2(\mathbb{Z})$, $J^{-1} \in M_2(\mathbb{Z})$, so $(A - \frac{p}{2})J^{-1} \in M_2(\mathbb{Q})$. $f$ is irreducible, and $A$ satisfies $f(A) = 0$, so by Lemma 4.2.1, $f(t)$ is its characteristic polynomial. Thus $\mathrm{tr}(A) = p$, $\det(A) = q$. $A$ can be written as $A = \begin{pmatrix} a & b \\ c & p-a \end{pmatrix}$, then $\det(A) = a(p-a) - bc = ap - a^2 - bc = q$. Note $(A - \frac{p}{2})J^{-1} = \begin{pmatrix} b & p/2 - a \\ p/2 - a & -c \end{pmatrix}$, where $p/2 - a = (p-2a)/2$, and $p - 2a \in \mathbb{Z}$, $p - 2a \equiv p \pmod 2$. Also we have $\det((A - \frac{p}{2})J^{-1}) = -bc - (p/2 - a)^2 = -bc - a^2 + ap - p^2/4 = q - p^2/4 = -\Delta_f/4$.

Now consider the special condition when $\Delta_f < 0$. We know $A = \begin{pmatrix} a & b \\ c & p-a \end{pmatrix}$. If $b > 0$, then the (1,2)-entry of its conjugate $TAT^{-1}$ for any $T \in SL_2(\mathbb{Z})$ is still positive. The reason is as follows. Suppose $T = \begin{pmatrix} r & s \\ u & v \end{pmatrix}$, then the (1,2)-entry of $TAT^{-1}$ is $br^2 + (p-2a)rs - cs^2 > 0$, for its discriminant is $\Delta = (p-2a)^2 + 4bc = p^2 - 4ap + 4a^2 + 4bc = p^2 - 4q = \Delta_f < 0$.

Under the condition $\Delta_f < 0$, we also have $b > 0 \Leftrightarrow (A-\frac{p}{2})J^{-1} > 0$, because $(A-\frac{p}{2})J^{-1} = \begin{pmatrix} b & p/2-a \\ p/2-a & -c \end{pmatrix}$, and $\det((A-\frac{p}{2})J^{-1}) = -\Delta_f/4 > 0$.

Given any two $[A], [B]$ in the left hand side of (12), $\lambda([A]) = [(A-\frac{p}{2})J^{-1}]$, $\lambda([B]) = [(B-\frac{p}{2})J^{-1}]$. $\forall\, T \in SL_2(\mathbb{Z})$, we have

$$\begin{aligned} B = TAT^{-1} &\Leftrightarrow \quad (B-\tfrac{p}{2}) = T(A-\tfrac{p}{2})T^{-1} \\ &\Leftrightarrow \quad (B-\tfrac{p}{2})J^{-1} = T(A-\tfrac{p}{2})T^{-1}J^{-1} \end{aligned}$$

By Lemma 4.3.1, we have

$$\begin{aligned} T(A-\frac{p}{2})T^{-1}J^{-1} &= T(A-\frac{p}{2})J^{-1}JT^{-1}J^{-1} \\ &= T(A-\frac{p}{2})J^{-1}(T^{-1})^{-t} \\ &= T(A-\frac{p}{2})J^{-1}T^{t} \end{aligned}$$

Thus

$$B = TAT^{-1} \Leftrightarrow (B-\frac{p}{2})J^{-1} = T(A-\frac{p}{2})J^{-1}T^{t}$$

i.e.

$$A \overset{+}{\sim} B \Leftrightarrow (A-\frac{p}{2})J^{-1} \overset{c}{\sim} (B-\frac{p}{2})J^{-1}$$

Hence, the map $\lambda$ is well-defined and injective. Now we are going to show it is surjective. For any $[A] \in \tilde{Q}(f)$, consider the matrix $AJ + \frac{p}{2}$. Suppose $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$, then $AJ + \frac{p}{2} = \begin{pmatrix} \frac{p-b}{2} & a \\ -c & \frac{p+b}{2} \end{pmatrix}$. $AJ + \frac{p}{2} \in M_2(\mathbb{Z})$, for $b \equiv p \pmod 2$. Also $\mathrm{tr}(AJ + \frac{p}{2}) = p$, $\det(AJ + \frac{p}{2}) = (p^2 - b^2)/4 + ac = q$, for $\det(A) = ac - b^2/4 = -\Delta_f/4$. So the characteristic polynomial of $AJ + \frac{p}{2}$ is $t^2 - p\,t + q = f(t)$. Thus we have $f(AJ + \frac{p}{2}) = 0$. When $\Delta_f < 0$, $A > 0$ implies $a > 0$. So $[AJ + \frac{p}{2}]$ is in the left hand side of (12), and $\lambda([AJ + \frac{p}{2}]) = [A]$. $\lambda$ is surjective. $\square$

## 4.4 Generalization of Gauss Correspondence

The bijection in (12) gives us a link between the Gauss Correspondence and the LMT. But the conjugation there is the conjugation by an element in $SL_2(\mathbb{Z})$. If we need generalize the Gauss Correspondence, we need to get the LMT in $SL_n$ version. That is what we are going to do next.

As in section 4.2, let $k$ be a number field (local or global), and $\mathcal{O}_k$ be its ring of integers. Let $f(t) \in \mathcal{O}_k[t]$ be a monic irreducible polynomial of degree $n$ over $k$. Let $P \in M_n(\mathcal{O}_k)$ with $f(P) = 0$ be a fixed matrix. From Lemma 4.2.1, we know $f(t)$ is the characteristic polynomial for $P$. Fix one of its eigenvalues, and denote it by $\theta$. Of course $\theta \in \overline{\mathcal{O}_k}$ and satisfies $f(\theta) = 0$. As before, take $K = k(\theta)$, then $[K : k] = n$. Also define $H_K$, $H_K^+$, $\mathcal{O}$, $I_{\mathcal{O}}$, $\tilde{I}_{\mathcal{O}}$, $M_n(\mathcal{O}_k; f)$, $\tilde{M}_n(\mathcal{O}_k; f)$ and $\tilde{M}_n^+(\mathcal{O}_k; f)$ as before. Then we have the following generalization of Gauss Correspondence:

**Theorem 4.4.1.** There is an exact sequence of pointed sets:

$$1 \to C_P(\mathrm{SL}_n(\mathcal{O}_k)) \xrightarrow{\iota} C_P(\mathrm{GL}_n(\mathcal{O}_k)) \xrightarrow{\det} \mathcal{O}_k^\times \xrightarrow{\delta} \tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{i} \tilde{M}_n(\mathcal{O}_k; f) \to 1 \tag{13}$$

where $C_P(\mathrm{SL}_n(\mathcal{O}_k))$ and $C_P(\mathrm{GL}_n(\mathcal{O}_k))$ are the centralizers of $P$ in $\mathrm{SL}_n(\mathcal{O}_k)$ and $\mathrm{GL}_n(\mathcal{O}_k)$ respectively, and we consider $[P]$ as the distinguished element in both $\tilde{M}_n^+(\mathcal{O}_k; f)$ and $\tilde{M}_n(\mathcal{O}_k; f)$ when we talk about its exactness. Moreover, when $\mathcal{O}_K = \mathcal{O}_k[\theta]$, we have a bijection $i_f$:

$$\tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{\sim} \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times \tilde{M}_n(\mathcal{O}_k; f) \tag{14}$$

So if in addition, $\mathcal{O}_k$ is a PID, by LMT, $i_f$ becomes

$$\tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{\sim} \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times H_K \tag{15}$$

Here, I think I should point out that any of the bijections in (14) and (15) doesn't depend on $P$.

**Pf.** In (13), we define $\iota$ to be the inclusion map, "det" to be the determinant map, $i$ to be the map induced by identity map. And we define $\delta$ as follows: $\forall a \in \mathcal{O}_k^\times$, take any $A \in GL_n(\mathcal{O}_k)$ with $\det(A) = a$, then define $\delta(a) = [A^{-1}PA] \in \tilde{M}_n^+(\mathcal{O}_k; f)$.

The definition of $\delta$ is well-defined. First, $f(A^{-1}PA) = A^{-1}f(P)A = 0$. And if we choose another matrix $B \in GL_n(\mathcal{O}_k)$ with $\det(B) = a$, then $\det(B^{-1}A) = 1$ and $B^{-1}A \in SL_n(\mathcal{O}_k)$. So $B^{-1}PB = B^{-1}AA^{-1}PAA^{-1}B = (B^{-1}A)A^{-1}PA(B^{-1}A)^{-1}$, thus $[B^{-1}PB] = [A^{-1}PA]$. The definition of $\delta$ does not depend on the choice of $A$.

Now we are going to show the exactness of (13). $\iota$ is the inclusion map, so it is injective. $\forall A \in C_P(SL_n(\mathcal{O}_k))$, we know $\det(A) = 1$, so $\det \circ \iota(A) = 1$. $\forall A \in C_P(GL_n(\mathcal{O}_k))$, if $\det(A) = 1$, then $A \in C_P(SL_n(\mathcal{O}_k))$. So (13) is exact at $C_P(SL_n(\mathcal{O}_k))$ and $C_P(GL_n(\mathcal{O}_k))$.

$\forall A \in C_P(GL_n(\mathcal{O}_k))$, suppose $\det(A) = a$, then $\delta(a) = [A^{-1}PA]$, because we can still take the $A$ in the definition of $\delta$ to be this $A$. But $A \in C_P(GL_n(\mathcal{O}_k))$, so $\delta \circ \det(A) =$

$[A^{-1}PA] = [A^{-1}AP] = [P]$. And $\forall a \in \mathcal{O}_k^\times$, if $\delta(a) = [P]$, then by the definition of $\delta$, choose any $A \in GL_n(\mathcal{O}_k)$ with $\det(A) = a$, $\delta(a) = [A^{-1}PA]$. So we have $[A^{-1}PA] = [P]$. It means that there exists some $T \in SL_n(\mathcal{O}_k)$, such that $A^{-1}PA = TPT^{-1}$. Thus, $P(AT) = (AT)P$, $AT \in C_P(GL_n(\mathcal{O}_k))$ and $\det(AT) = \det(A) = a$. So (13) is exact at $\mathcal{O}_k^\times$.

$\forall a \in \mathcal{O}_k^\times$, by the definition of $\delta$, $\delta(a) = [A^{-1}PA]$, if choosing some $A \in GL_n(\mathcal{O}_k)$ with $\det(A) = a$. Of course $[A^{-1}PA] = [P]$ in $\tilde{M}_n(\mathcal{O}_k; f)$. And $\forall\, [A] \in \tilde{M}_n^+(\mathcal{O}_k; f)$, if $[A] = [P]$ in $\tilde{M}_n(\mathcal{O}_k; f)$, then there is some $T \in GL_n(\mathcal{O}_k)$, such that $TAT^{-1} = P$. So $A = T^{-1}PT$. Let $a = \det(T) \in \mathcal{O}_k^\times$, then $\delta(a) = [T^{-1}PT] = [A]$, if taking the $A$ in the definition of $\delta$ to be $T$. So (13) is exact at $\tilde{M}_n^+(\mathcal{O}_k; f)$.

The surjectivity of $i$ is obvious. So all in all, we get that (13) is an exact sequence of pointed sets.

Now we are going to show that $N_{K|k}(\mathcal{O}_k[\theta])^\times \subseteq \mathrm{Im}(\det)$. Note that we denote $\mathcal{O} = \mathcal{O}_k[\theta]$. Because $\theta$ is an eigenvalue of $P$, we have

$$\exists\, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{O}^n, x \neq 0, s.t. \quad Px = \theta x.$$

As before, here there exists such an eigenvector $x$ in $K^n$. But after multiplying an appropriate number in $\mathcal{O}_k$, it can be taken from $\mathcal{O}^n$.

Let $\mathbf{a} = [x_1, \ldots, x_n]_{\mathcal{O}_k}$, then $\mathbf{a}$ is an integral ideal in $\mathcal{O}$, for $\theta x = Px$. So $\{x_1, \ldots, x_n\}$ is linearly independent over $k$ and it forms a basis for $K$ over $k$. For any $g(\theta) \in (\mathcal{O}_k[\theta])^\times$, where $g(t) \in \mathcal{O}_k[t]$, in view of $Px = \theta x$, we have $g(P)x = g(\theta)x$. Because $\{x_1, \ldots, x_n\}$ forms a basis for $K$ over $k$, we get $\det(g(P)) = N_{K|k}(g(\theta))$. For $g(\theta) \in (\mathcal{O}_k[\theta])^\times \subseteq \mathcal{O}_K^\times$, so $\det(g(P)) = N_{K|k}(g(\theta)) \in \mathcal{O}_k^\times$, $g(P) \in GL_n(\mathcal{O}_k)$. Obviously, $g(P) \in C_P(GL_n(\mathcal{O}_k))$. So $N_{K|k}(g(\theta)) = \det(g(P)) \in \mathrm{Im}(\det)$, and $N_{K|k}(\mathcal{O}_k[\theta])^\times \subseteq \mathrm{Im}(\det)$.

When $\mathcal{O}_K = \mathcal{O}_k[\theta]$, we have the inverse inclusion: $\mathrm{Im}(\det) \subseteq N_{K|k}\mathcal{O}_K^\times$. As we know, the polynomial $f(t)$ is irreducible, thus $f(t)$ and $f'(t)$ are coprime, and $f(t)$ does not have any multiple root. But $f(t)$ is the characteristic polynomial for $P$, so $P$ has no multiple roots. By Lemma 4.2.2, we get that, for any $A \in C_P(GL_n(\mathcal{O}_k))$, $A = g(P)$, where $g(t) \in k[t]$. As mentioned before, $\theta$ is an eigenvalue of $P$, and $x \in \mathcal{O}^n$ is the corresponding eigenvector with $Px = \theta x$. Thus $Ax = g(P)x = g(\theta)x$. So $g(\theta)$ is an eigenvalue for $A$, and it satisfies the characteristic polynomial of $A$. Hence it is integral over $\mathcal{O}_k$. Note $g(\theta) \in K$, thus

$g(\theta) \in \mathcal{O}_K = \mathcal{O}_k[\theta]$. Therefore there exists a polynomial $h(t) \in \mathcal{O}_k[t]$, such that $g(\theta) = h(\theta) \in \mathcal{O}_K$. Thus we have $Ax = h(\theta)x$. As mentioned before, $\{x_1, \ldots, x_n\}$ is linearly independent over $k$ and it forms a basis for $K$ over $k$. So $N_{K|k}(h(\theta)) = \det(A) \in \mathcal{O}_k^\times$. Then we get $h(\theta) \in \mathcal{O}_K^\times$, and $\det(A) = N_{K|k}(h(\theta)) \in N_{K|k}\mathcal{O}_K^\times$. Hence we get the inverse inclusion, $\mathrm{Im}(\det) \subseteq N_{K|k}\mathcal{O}_K^\times$.

All in all, when $\mathcal{O}_K = \mathcal{O}_k[\theta]$, we have $\mathrm{Im}(\det) = N_{K|k}\mathcal{O}_K^\times$. In this case, from (13), we get the following exact sequence of pointed sets:

$$1 \to \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \xrightarrow{\delta} \tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{i} \tilde{M}_n(\mathcal{O}_k; f) \to 1 \tag{16}$$

Here $\delta$ is the map induced from the $\delta$ before. This $\delta$ is well-defined. The reason is as follows: $\forall\, [a] \in \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times$, where $a \in \mathcal{O}_k^\times$, take any $au \in [a]$ with $u \in N_{K|k}\mathcal{O}_K^\times = \mathrm{Im}(\det)$. There exist $A \in GL_n(\mathcal{O}_k)$ with $\det(A) = a$ and $U \in C_P(GL_n(\mathcal{O}_k))$ with $\det(U) = u$. Thus $\det(UA) = ua = au$ and then by definition of $\delta$ in (13), $\delta(au) = [A^{-1}U^{-1}PUA] = [A^{-1}PA] = \delta(a)$, for $U \in C_P(GL_n(\mathcal{O}_k))$. So $\delta([a]) = \delta(a)$ is well-defined.

The $\delta$ in (16) is injective. For $\forall\, [a], [b] \in \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times$, $a, b \in \mathcal{O}_k^\times$, let $A, B \in GL_n(\mathcal{O}_k)$ with $\det(A) = a$, $\det(B) = b$, then by definition of $\delta$ above, we have $\delta([a]) = \delta(a) = [A^{-1}PA]$ and $\delta([b]) = \delta(b) = [B^{-1}PB]$. If $\delta([a]) = \delta([b])$, then $[A^{-1}PA] = [B^{-1}PB]$. There exists some $T \in SL_n(\mathcal{O}_k)$, such that $B^{-1}PB = TA^{-1}PAT^{-1}$. Then $PBTA^{-1} = BTA^{-1}P$, $BTA^{-1} \in C_P(GL_n(\mathcal{O}_k))$. Thus $ba^{-1} = \det(BTA^{-1}) \in \mathrm{Im}(\det) = N_{K|k}\mathcal{O}_K^\times$, $[a] = [b]$.

Denote the $\delta$ in (16) by $\delta_P$ to signify that the definition of $\delta$ there depends on the choice of $P$. But the definition of $i$ in (16) does not depend on $P$. If we take any element $[A] \in \tilde{M}_n(\mathcal{O}_k; f)$, we have $A \in M_n(\mathcal{O}_k)$ and $f(A) = 0$. By Lemma 4.2.1, we know $f(t)$ is the characteristic polynomial for $A$ again. And we can still fix the same $\theta$ as its eigenvalue and get the same $K$ as before. Then the story above for $P$ works for $A$ too, and we get another exact sequence of pointed sets:

$$1 \to \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \xrightarrow{\delta_A} \tilde{M}_n^+(\mathcal{O}_k; f) \xrightarrow{i} \tilde{M}_n(\mathcal{O}_k; f) \to 1 \tag{17}$$

where we consider $[A]$ as the distinguished element in both $\tilde{M}_n^+(\mathcal{O}_k; f)$ and $\tilde{M}_n(\mathcal{O}_k; f)$ in (17) when we talk about its exactness.

By the exactness of (17), we get $\mathrm{Im}(\delta_A) = i^{-1}([A])$. From the injectivity of $\delta_A$, we get the bijection $\delta_A^{-1} : i^{-1}([A]) \to \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times$.

Let $\{A_i \in M_n(\mathcal{O}_k; f) : i \in \mathcal{I}\}$ be a fixed set of the representatives of $\tilde{M}_n(\mathcal{O}_k; f)$. Define

$$\begin{aligned} i_f : \quad \tilde{M}_n^+(\mathcal{O}_k; f) &\longrightarrow \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times \tilde{M}_n(\mathcal{O}_k; f) \\ [A] &\longmapsto (\delta_{A_i}^{-1}([A]), [A]) \\ &\qquad \text{if } [A] = [A_i] \in \tilde{M}_n(\mathcal{O}_k; f) \text{ for some } i \in \mathcal{I} \end{aligned}$$

- $i_f$ is well-defined.

  $\forall\, [A] \in \tilde{M}_n^+(\mathcal{O}_k; f)$, $i([A]) = [A] \in \tilde{M}_n(\mathcal{O}_k; f)$, so $[A] = [A_i]$ for some $i \in \mathcal{I}$, because $\{A_i \in M_n(\mathcal{O}_k; f) : i \in \mathcal{I}\}$ is a set of the representatives of $\tilde{M}_n(\mathcal{O}_k; f)$. Then $[A] \in i^{-1}([A_i])$, and the definition of $i_f$ makes sense. If $[B] \in \tilde{M}_n^+(\mathcal{O}_k; f)$, with $[B] = [A]$ in $\tilde{M}_n^+(\mathcal{O}_k; f)$, then $[B] = [A] = [A_i]$ in $\tilde{M}_n(\mathcal{O}_k; f)$. And we have $\delta_{A_i}^{-1}([A]) = \delta_{A_i}^{-1}([B])$, because $[A] = [B] \in i^{-1}([A_i]) \subseteq \tilde{M}_n^+(\mathcal{O}_k; f)$. $i_f$ is well-defined.

- $i_f$ is injective.

  If $[A], [B] \in \tilde{M}_n^+(\mathcal{O}_k; f)$, with $i_f[A] = i_f[B]$, then $[A] = [B]$ in $\tilde{M}_n(\mathcal{O}_k; f)$. Thus there is some $i \in \mathcal{I}$ such that $[A] = [B] = [A_i]$ in $\tilde{M}_n(\mathcal{O}_k; f)$. Again from $i_f[A] = i_f[B]$, we also have $\delta_{A_i}^{-1}([A]) = \delta_{A_i}^{-1}([B])$, and then $[A] = [B]$ in $\tilde{M}_n^+(\mathcal{O}_k; f)$.

- $i_f$ is surjective.

  Take any $([a], [A]) \in \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times \tilde{M}_n(\mathcal{O}_k; f)$, $[A] \in \tilde{M}_n(\mathcal{O}_k; f)$, then there is some $i \in \mathcal{I}$, such that $[A] = [A_i]$ in $\tilde{M}_n(\mathcal{O}_k; f)$. Let $[B] = \delta_{A_i}([a]) \in \mathrm{Im}(\delta_{A_i}) = i^{-1}([A_i]) \subseteq \tilde{M}_n^+(\mathcal{O}_k; f)$, then $i([B]) = [B] = [A_i] = [A]$ in $\tilde{M}_n(\mathcal{O}_k; f)$, and $\delta_{A_i}^{-1}([B]) = [a]$ for $\delta_{A_i}^{-1}$ is a bijection. Hence $i_f([B]) = ([a], [A])$.

So we get the required bijection. □

Now we are going to show why Theorem 4.4.1 is considered as a generalization of Gauss Correspondence.

When $k = \mathbb{Q}$, and $f(t) = t^2 - p\,t + q$ is an irreducible polynomial in $\mathbb{Z}[t]$, we have $\Delta_f = p^2 - 4q$, and its roots are $(p \pm \sqrt{\Delta_f})/2$. Take $\theta$ be one of its roots, fixed, thus $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{\Delta_f})$, and $\mathcal{O}_k^\times = \{\pm 1\}$. We have the following cases:

- Case $\Delta_f > 0$:

First, we notice that in this case $K$ is a real quadratic field. Comparing with (6), we have

$$|\mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times| = [P_K : P_K^+] = \begin{cases} 1, & \exists \varepsilon \in \mathcal{O}_K^\times, N_{K|k}\varepsilon = -1 \\ 2, & N_{K|k}\varepsilon = 1, \forall \varepsilon \in \mathcal{O}_K^\times \end{cases}$$

So we have a bijection:

$$\mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times H_K \xrightarrow{\sim} H_K^+$$

Thus by (15), we have

$$\tilde{M}_2^+(\mathbb{Z}; f) \xrightarrow{\sim} \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times H_K \xrightarrow{\sim} H_K^+ \tag{18}$$

On the other side, in view of $\Delta_f > 0$, the left hand side of (12) becomes $\tilde{M}_2^+(\mathbb{Z}; f)$. So combining with (12), (18) implies

$$H_K^+ \xrightarrow{\sim} \tilde{Q}(f)$$

By the argument in section 4.3, we know it implies the classical Gauss Correspondence.

- Case $\Delta_f < 0$:

  In this case, the left hand side of (12) becomes

$$\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : f(A) = 0 \text{ and } b > 0 \right\} \Big/ \overset{+}{\sim}$$

  We denote it by $\tilde{M}_2^+(\mathbb{Z}; f; +)$. Accordingly, we denote

$$\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : f(A) = 0 \text{ and } b < 0 \right\} \Big/ \overset{+}{\sim}$$

  by $\tilde{M}_2^+(\mathbb{Z}; f; -)$.

  The definition of $\tilde{M}_2^+(\mathbb{Z}; f; -)$ is meaningful as that of $\tilde{M}_2^+(\mathbb{Z}; f; +)$ when $\Delta_f < 0$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{M}_2^+(\mathbb{Z}; f; -)$, $f(A) = 0$, so by Lemma 4.2.1, $f$ is the characteristic polynomial for $A$. Thus $a+d = p$, $d = p-a$. If $b < 0$, then the (1,2)-entry of its conjugate $TAT^{-1}$ for any $T \in SL_2(\mathbb{Z})$ is still negative. The reason is as follows. Suppose $T = \begin{pmatrix} r & s \\ u & v \end{pmatrix}$, then the (1,2)-entry of $TAT^{-1}$ is $br^2 + (p-2a)rs - cs^2 < 0$, for its discriminant is $\Delta = (p-2a)^2 + 4bc = p^2 - 4ap + 4a^2 + 4bc = p^2 - 4q = \Delta_f < 0$.

For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$, if $f(A) = 0$, then $b \neq 0$. Otherwise, by Lemma 4.2.1, we know, the characteristic polynomial of $A$ is $f(t) = (t-a)(t-d)$, not irreducible any more. Therefore, $\tilde{M}_2^+(\mathbb{Z}; f)$ can be split into a disjoint union of $\tilde{M}_2^+(\mathbb{Z}; f; +)$ and $\tilde{M}_2^+(\mathbb{Z}; f; -)$ as follows:

$$\tilde{M}_2^+(\mathbb{Z}; f) = \tilde{M}_2^+(\mathbb{Z}; f; +) \coprod \tilde{M}_2^+(\mathbb{Z}; f; -) \tag{19}$$

We have the following lemma:

**Lemma 4.4.1.** If $f(t) = t^2 - p\,t + q$ is an irreducible polynomial in $\mathbb{Z}[t]$ with discriminant $\Delta_f < 0$, then there is a bijection $t$ induced by transposition:

$$\tilde{M}_2^+(\mathbb{Z}; f; +) \xrightarrow{\sim} \tilde{M}_2^+(\mathbb{Z}; f; -)$$

**Pf.** For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{M}_2^+(\mathbb{Z}; f)$, we have $bc < 0$. The reason is as follows. $f(A) = 0$, so by Lemma 4.2.1, $f$ is the characteristic polynomial for $A$. Thus $p = \mathrm{tr}(A) = a + d$, $q = \det(A) = ad - bc$. The discriminant of $f$ is $\Delta_f = p^2 - 4q = (a+d)^2 - 4(ad - bc) = (a-d)^2 + bc < 0$. Thus $bc < 0$.

$\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{M}_2^+(\mathbb{Z}; f; +) \subseteq \tilde{M}_2^+(\mathbb{Z}; f)$, $A^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Because $b > 0$ and $bc < 0$, we get $c < 0$. Also from $f(A) = 0$, we get $f(A^t) = 0$. So $[A^t] \in \tilde{M}_2^+(\mathbb{Z}; f; -)$.

Given any two $[A], [B] \in \tilde{M}_2^+(\mathbb{Z}; f; +)$. $\forall\, T \in SL_2(\mathbb{Z})$, we have

$$\begin{aligned} B = TAT^{-1} \quad &\Leftrightarrow \quad B^t = T^{-t}A^tT^t \\ &\Leftrightarrow \quad B^t = T^{-t}A^t(T^{-t})^{-1} \end{aligned}$$

So $t$ is well-defined and injective.

For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{M}_2^+(\mathbb{Z}; f; -) \subseteq \tilde{M}_2^+(\mathbb{Z}; f)$, $A^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Then, for $b < 0$, $bc < 0$, we get $c > 0$. And for $f(A) = 0$, $f(A^t) = 0$. So $[A^t] \in \tilde{M}_2^+(\mathbb{Z}; f; +)$, and $t([A^t]) = [A]$. $t$ is surjective. Hence, $t$ is a bijection. $\square$

From this lemma and the decomposition (19), we have the following bijection:

$$\tilde{M}_2^+(\mathbb{Z}; f) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \tilde{M}_2^+(\mathbb{Z}; f; +)$$

Notice that the left hand side of (12) is just $\tilde{M}_2^+(\mathbb{Z}; f; +)$, we get

$$\tilde{M}_2^+(\mathbb{Z}; f) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \tilde{Q}(f) \tag{20}$$

On the other side, from (15), we have

$$\tilde{M}_2^+(\mathbb{Z}; f) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times H_K$$

because the nontrivial conjugation over $K$ is just the complex conjugation and the norm function always has positive values. In view of (20), we get

$$H_K^+ = H_K \xrightarrow{\sim} \tilde{Q}(f)$$

Again, by the argument in section 4.3, we know it implies the classical Gauss Correspondence.

## 4.5 Polynomial Cohomology

Inspired by Theorem 4.4.1, one may want to get a more generalized result and apply it in some other circumstances. That is what I am going to do now.

Let $G$ be a group, $R$ be a commutative ring and $\mathcal{A}$ be an $R$-algebra. $f(t) \in R[t]$ is a polynomial. For a multiplicative subset $M \subseteq \mathcal{A}$, if $G$ acts on the subset of $M$, $M^f = \{A \in M : f(A) = 0\}$, we define

$$H^1(f, M; G) = \{A \in M : f(A) = 0\}/G$$

to be the set of $G$-orbits of $M^f$. When $1 \in M$, denote $M^\times$ be the set of all the invertible elements in $M$, then it is a group. If it acts on $M^f$, we simply denote $H^1(f, M; M^\times)$ by $H^1(f, M)$.

Take a multiplicative set $S$ with unity, and assume $M$ contains the multiplicative unity of $\mathcal{A}$ too. Let us abuse the notation, and denote those two unities by the same expression 1. Let $\pi : M \to S$ be a surjective map with $\pi(1) = 1$ and $\pi(AB) = \pi(A)\pi(B)$, $\forall A, B \in M$. Also assume $\Gamma = \ker(\pi) = \{A \in M : \pi(A) = 1\}$ be a group. So we have the following exact sequence of pointed sets:

$$1 \to \Gamma \to M \xrightarrow{\pi} S \to 1 \tag{21}$$

Let $M^\times$, $S^\times$ act by conjugation on $M$, $S$ respectively. And for any $P \in M$, denote $C_P(\Gamma) = \{A \in \Gamma : AP = PA\}$, $C_P(M^\times) = \{A \in M^\times : AP = PA\}$ and $C_{\pi(P)}(S^\times) = \{a \in$

$S^\times : a\pi(P) = \pi(P)a\}$. Then the following theorem tells us that we can get a long exact sequence from (21).

**Theorem 4.5.1.** For any $P \in M^f$, $\Gamma$ acts by conjugation on $(\pi^{-1} \circ \pi(P))^f$, and we have the following long exact sequence of pointed sets:

$$1 \to C_P(\Gamma) \xrightarrow{\iota} C_P(M^\times) \xrightarrow{\pi} C_{\pi(P)}(S^\times) \xrightarrow{\delta_P} H^1(f, \pi^{-1} \circ \pi(P); \Gamma) \xrightarrow{i} H^1(f, M) \tag{22}$$

Moreover, if $S$ is contained in a $R$-algebra $\mathcal{B}$, and their unities coincide, and if $\pi$ is defined as a map $\pi : \mathcal{A} \to \mathcal{B}$, $\pi|_M$ is the $\pi$ above, and it satisfies $\pi(0) = 0$, $\pi(aA) = a\pi(A)$ and $\pi(A + B) = \pi(A) + \pi(B)$, $\forall a \in R$, $\forall A, B \in M$, then we have the following long exact sequence of pointed sets:

$$1 \to C_P(\Gamma) \xrightarrow{\iota} C_P(M^\times) \xrightarrow{\pi} C_{\pi(P)}(S^\times) \xrightarrow{\delta_P}$$

$$\xrightarrow{\delta_P} H^1(f, \pi^{-1} \circ \pi(P); \Gamma) \xrightarrow{i} H^1(f, M) \xrightarrow{\pi} H^1(f, S) \tag{23}$$

Here when we talk about the exactnesses of (22) and (23), we consider $[P]$ as the distinguished element in both $H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$ and $H^1(f, M)$, and consider $[\pi(P)]$ as the distinguished element in $H^1(f, S)$. And if $\{P_i \in (\pi^{-1} \circ \pi(P))^f : i \in \mathcal{I}\}$ is a set of representatives of $i(H^1(f, \pi^{-1} \circ \pi(P); \Gamma))$, we have a bijection $i_f$:

$$H^1(f, \pi^{-1} \circ \pi(P); \Gamma) \xrightarrow{\sim} \coprod_{i \in \mathcal{I}} \pi(C_{P_i}(M^\times)) \backslash C_{\pi(P)}(S^\times) \tag{24}$$

which splits $H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$ into a disjoint union of the sets of right cosets of $\pi(C_{P_i}(M^\times))$ in $C_{\pi(P)}(S^\times)$.

**Pf.** First, let me show that for any $P \in M^f$, $\Gamma$ acts by conjugation on $(\pi^{-1} \circ \pi(P))^f$. $\forall A \in (\pi^{-1} \circ \pi(P))^f$, $\gamma \in \Gamma$, we have $\gamma A \gamma^{-1} \in M$, and $\pi(\gamma A \gamma^{-1}) = \pi(\gamma)\pi(A)\pi(\gamma^{-1}) = \pi(A) = \pi(P)$, for $\pi(\gamma^{-1}) = \pi(\gamma)\pi(\gamma^{-1}) = \pi(\gamma\gamma^{-1}) = \pi(1) = 1$. Of course $f(\gamma A \gamma^{-1}) = \gamma f(A) \gamma^{-1} = 0$, so $\gamma A \gamma^{-1} \in (\pi^{-1} \circ \pi(P))^f$. Hence $\Gamma$ acts by conjugation on $(\pi^{-1} \circ \pi(P))^f$.

Next, note that from (21), we can get the following short exact sequence of groups:

$$1 \to \Gamma \to M^\times \xrightarrow{\pi} S^\times \to 1 \tag{25}$$

The reason is as follows. Because $\Gamma$ is a group, $\forall a \in \Gamma \subseteq M$, $\exists b \in \Gamma \subseteq M$, such that $ab = 1$, thus $a \in M^\times$, $\Gamma \subseteq M^\times$. For any $m \in M^\times$, there is some $m' \in M$, such that $mm' = 1$. Then $\pi(mm') = \pi(m)\pi(m') = \pi(1) = 1$. So $\pi(m) \in S^\times$. By definition of $\Gamma$, we know (25) is exact

at $M^\times$. For any $s \in S^\times$, there is some $s' \in S$, such that $ss' = 1$. For $s, s' \in S$, there are $m, m' \in M$, such that $\pi(m) = s$ and $\pi(m') = s'$. So $\pi(mm') = \pi(m)\pi(m') = ss' = 1$. Thus $mm' \in \Gamma$, $(mm')^{-1} \in \Gamma$, and $mm'(mm')^{-1} = 1$, so $m \in M^\times$, $\pi : M^\times \to S^\times$ is surjective.

Now we turn to prove the long exact sequences (22) and (23). In them, $\iota$ is the inclusion map, $i$ is the map induced by inclusion, and $\pi : H^1(f, M) \to H^1(f, S)$ is the map induced by $\pi$. And $\delta = \delta_P$ is defined as follows: $\forall a \in C_{\pi(P)}(S^\times)$, by (25), there is some $A \in M^\times$ with $\pi(A) = a$, then define $\delta(a) = [A^{-1}PA] \in H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$. Here we use the notation $\delta_P = \delta$ to signify that the definition of $\delta$ depends on the choice of $P$.

The definition of $\delta$ is well-defined. First, $A^{-1}PA \in M$, $f(A^{-1}PA) = A^{-1}f(P)A = 0$, and $\pi(A^{-1}PA) = \pi(A^{-1})\pi(P)\pi(A) = \pi(A^{-1})\pi(A)\pi(P) = \pi(A^{-1}A)\pi(P) = \pi(1)\pi(P) = \pi(P)$, for $\pi(A) = a \in C_{\pi(P)}(S^\times)$. Hence we have $[A^{-1}PA] \in H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$. If we choose another element $B \in M^\times$ with $\pi(B) = a$, then $\pi(B^{-1}A) = \pi(B)^{-1}\pi(A) = 1$ and $B^{-1}A \in \Gamma$. So $B^{-1}PB = B^{-1}AA^{-1}PAA^{-1}B = (B^{-1}A)A^{-1}PA(B^{-1}A)^{-1}$, thus $[B^{-1}PB] = [A^{-1}PA]$. The definition of $\delta$ does not depend on the choice of $A$.

$\iota$ is the inclusion map, so it is injective. $\forall A \in C_P(\Gamma)$, we know $\pi(A) = 1$, so $\pi \circ \iota\,(A) = 1$. $\forall A \in C_P(M^\times)$, if $\pi(A) = 1$, then $A \in C_P(\Gamma)$. So (22) and (23) are exact at $C_P(\Gamma)$ and $C_P(M^\times)$.

$\forall A \in C_P(M^\times)$, suppose $\pi(A) = a$, then $\delta(a) = [A^{-1}PA]$, because we can still take the $A$ in the definition of $\delta$ to be this $A$. But $A \in C_P(M^\times)$, so $\delta \circ \pi(A) = [A^{-1}PA] = [A^{-1}AP] = [P]$. And $\forall a \in C_{\pi(P)}(S^\times)$, if $\delta(a) = [P]$, then by the definition of $\delta$, choose any $A \in M^\times$ with $\pi(A) = a$, $\delta(a) = [A^{-1}PA]$. So we have $[A^{-1}PA] = [P]$. It means that there exists some $T \in \Gamma$, such that $A^{-1}PA = TPT^{-1}$. Thus, $P(AT) = (AT)P$, $AT \in C_P(M^\times)$ and $\pi(AT) = \pi(A)\pi(T) = a$. So (22) and (23) are exact at $C_{\pi(P)}(S^\times)$.

$\forall a \in C_{\pi(P)}(S^\times)$, by the definition of $\delta$, $\delta(a) = [A^{-1}PA]$, if choosing some $A \in M^\times$ with $\pi(A) = a$. Of course $[A^{-1}PA] = [P]$ in $H^1(f, M)$. And $\forall\, [A] \in H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$, if $[A] = [P]$ in $H^1(f, M)$, then there is some $T \in M^\times$, such that $TAT^{-1} = P$. So we get $TA = PT$. Thus $\pi(TA) = \pi(PT) = \pi(T)\pi(A) = \pi(P)\pi(T) = \pi(T)\pi(P)$, for $[A] \in H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$ and $\pi(A) = \pi(P)$. Let $a = \pi(T) \in S^\times$, then $a \in C_{\pi(P)}(S^\times)$. Also from above, we know $TAT^{-1} = P$, thus $A = T^{-1}PT$. So $\delta(a) = [T^{-1}PT] = [A]$, if taking the $A$ in the definition of $\delta$ to be $T$. So (22) and (23) are exact at $H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$.

Moreover, if $S$ is contained in a $R$-algebra $\mathcal{B}$, and their unities coincide, and if $\pi$ is defined

as a map $\pi : \mathcal{A} \to \mathcal{B}$, $\pi|_M$ is the $\pi$ as before, and it satisfies $\pi(0) = 0$, $\pi(aA) = a\pi(A)$ and $\pi(A + B) = \pi(A) + \pi(B)$, $\forall a \in R$, $\forall A, B \in M$, then (23) is exact at $H^1(f, M)$. The reason is as follows. $\forall\, [A] \in H^1(f, M)$, we have $\pi(A) \in S$ and $f(\pi(A)) = \pi(f(A)) = \pi(0) = 0$. So the map $\pi : H^1(f, M) \to H^1(f, S)$ is well-defined. Also $\forall\, [A] \in H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$, we have $\pi(A) = \pi(P)$ and $\pi \circ i([A]) = [\pi(A)] = [\pi(P)]$. For any $[A] \in H^1(f, M)$, if $\pi([A]) = [\pi(A)] = [\pi(P)]$ in $H^1(f, S)$, then there exists some $s \in S^\times$, such that $s\pi(A)s^{-1} = \pi(P)$. By (25), there is some $m \in M^\times$, such that $\pi(m) = s$. So we have $s\pi(A)s^{-1} = \pi(m)\pi(A)\pi(m)^{-1} = \pi(mAm^{-1}) = \pi(P)$. Let $B = mAm^{-1} \in M$, then from above we know $\pi(B) = \pi(P)$. Also $f(B) = f(mAm^{-1}) = mf(A)m^{-1} = 0$, thus $[B] \in H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$ and $i([B]) = [mAm^{-1}] = [A]$ in $H^1(f, M)$. Hence (23) is exact at $H^1(f, M)$.

For any $a, b \in C_{\pi(P)}(S^\times)$, we have

$$ab^{-1} \in \pi(C_P(M^\times)) \Longleftrightarrow \delta(a) = \delta(b)$$

The reason is as follows. For any $a, b \in C_{\pi(P)}(S^\times)$, if $c = ab^{-1} \in \pi(C_P(M^\times))$, then by (25), there are $B \in M^\times$ and $C \in C_P(M^\times)$ with $\pi(B) = b$ and $\pi(C) = c$. Let $A = CB \in M^\times$, then $\pi(A) = \pi(C)\pi(B) = cb = a$. So we have $A^{-1}PA = B^{-1}C^{-1}PCB = B^{-1}C^{-1}CPB = B^{-1}PB$, thus by the definition of $\delta$, $\delta(a) = [A^{-1}PA] = [B^{-1}PB] = \delta(b)$. On the other side, if $\delta(a) = \delta(b)$, then by the definition of $\delta$, there exist $A, B \in M^\times$ with $\pi(A) = a$ and $\pi(B) = b$, and $\delta(a) = [A^{-1}PA] = [B^{-1}PB] = \delta(b)$ in $H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$. So there is some $T \in \Gamma$, such that $A^{-1}PA = TB^{-1}PBT^{-1}$. Then $PATB^{-1} = ATB^{-1}P$, $ATB^{-1} \in C_P(M^\times)$ and $\pi(ATB^{-1}) = \pi(A)\pi(T)\pi(B^{-1}) = ab^{-1} \in \pi(C_P(M^\times))$. Therefore, for any $a, b \in C_{\pi(P)}(S^\times)$, $\delta(a) = \delta(b)$ if and only if $a$ and $b$ are in the same right coset in $\pi(C_P(M^\times))\backslash C_{\pi(P)}(S^\times)$.

By the above argument, and from (22), we can get the following exact sequence of pointed sets:

$$1 \to \pi(C_P(M^\times))\backslash C_{\pi(P)}(S^\times) \xrightarrow{\delta_P} H^1(f, \pi^{-1} \circ \pi(P); \Gamma) \xrightarrow{i} \mathrm{Im}(i) \to 1 \tag{26}$$

where $\delta_P$ is an injection.

In view of the exactness of (26) and the injectivity of $\delta_P$, we get $\mathrm{Im}(\delta_P) = i^{-1}([P])$ and the bijection $\delta_P^{-1} : i^{-1}([P]) \to \pi(C_P(M^\times))\backslash C_{\pi(P)}(S^\times)$.

The arguments before are all valid for an arbitrary element $P \in M^f$. So if let $\{P_i \in (\pi^{-1} \circ \pi(P))^f : i \in \mathcal{I}\} \subseteq M^f$ be a set of representatives of $i(H^1(f, \pi^{-1} \circ \pi(P); \Gamma))$, then

$\pi(P_i) = \pi(P)$, $H^1(f, \pi^{-1} \circ \pi(P_i); \Gamma) = H^1(f, \pi^{-1} \circ \pi(P); \Gamma)$, $\forall i \in \mathcal{I}$. And we have the following bijection $i_f = \coprod_{i \in \mathcal{I}} \delta_{P_i}^{-1}$:

$$H^1(f, \pi^{-1} \circ \pi(P); \Gamma) = \coprod_{i \in \mathcal{I}} i^{-1}([P_i]) \xrightarrow{\sim} \coprod_{i \in \mathcal{I}} \pi(C_{P_i}(M^\times)) \backslash C_{\pi(P)}(S^\times)$$

where the restriction of $\coprod_{i \in \mathcal{I}} \delta_{P_i}^{-1}$ to each $i^{-1}([P_i])$ is $\delta_{P_i}^{-1}$, $\forall i \in \mathcal{I}$. $\square$

Theorem 4.5.1 is a generalization of Theorem 4.4.1. In Theorem 4.5.1, if we take

- The commutative ring $R$ to be $\mathcal{O}_k$, the ring of integers of a number field $k$;
- The polynomial $f$ to be irreducible;
- The $R$-algebra $\mathcal{A}$ to be $M_n(\mathcal{O}_k)$, where $n$ is the degree of $f$;
- The multiplicative subset $M$ to be $\mathcal{A}$;
- the $R$-algebra $\mathcal{B}$ to be $R$;
- The multiplicative subset $S$ to be $R$;
- The map $\pi$ to be the determinant map;

then $M^\times = GL_n(\mathcal{O}_k)$, $S^\times = \mathcal{O}_k^\times$, $\Gamma = SL_n(\mathcal{O}_k)$, $C_{\pi(P)}(S^\times) = \mathcal{O}_k^\times$ and $H^1(f, M) = \tilde{M}_n(\mathcal{O}_k; f)$.

Also we have $(\pi^{-1} \circ \pi(P))^f = M_n(\mathcal{O}_k; f)$. First it is obvious that $(\pi^{-1} \circ \pi(P))^f \subseteq M_n(\mathcal{O}_k; f)$. On the other side, for any $A \in M_n(\mathcal{O}_k; f)$, then $f(A) = 0$. In view of $P \in M^f$, we also have $f(P) = 0$. By Lemma 4.2.1, $f$ is the characteristic polynomial for both $A$ and $P$, thus $\det(A) = \det(P)$, $A \in (\pi^{-1} \circ \pi(P))^f$. So $(\pi^{-1} \circ \pi(P))^f = M_n(\mathcal{O}_k; f)$ and $H^1(f, \pi^{-1} \circ \pi(P); \Gamma) = \tilde{M}_n^+(\mathcal{O}_k; f)$. Hence the exact sequence (22) becomes (13), and the bijection (24) implies (14).

# 5 Cyclic Action

## 5.1 Cyclic Action

Equipped with the generalization of Gauss Correspondence and an even more general polynomial cohomology, let us now turn back to the question proposed in section 3.3.

In that question, a cyclic group $\mathcal{G} =< \theta >$ of order two acts on $M_2(\mathbb{Z})$ as:

$$^{\theta}x = x^{*t} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}, \text{ if } x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}).$$

From Lemma 4.3.1, we know that this action is actually given by conjugation of a special matrix $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, whose action on $M_2(\mathbb{Z})$ is cyclic of order two. Hence, considering the cyclic action of a matrix on a matrix algebra by conjugation is one way to generalize it. This action is actually an action of $\mathbb{Z}$, so first let us look at a triple system $(\mathcal{G}, (G, M))$ with $\mathcal{G} = \mathbb{Z}$ in general.

**Lemma 5.1.1.** If the action of $1 \in \mathbb{Z}$ on $G$ is written as $s(g) = {}^1g$, $\forall g \in G$, then for any $c \in Z^1(\mathbb{Z}, G)$, we have

$$c_n = \begin{cases} As(A)s^2(A)\cdots s^{n-1}(A) & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{n}(A^{-1}) & \text{if } n < 0 \end{cases}$$

for some $A \in G$. Conversely, for any $A \in G$, that expression gives a cocycle in $Z^1(\mathbb{Z}, G)$. Moreover, for any two $c, c' \in Z^1(\mathbb{Z}, G)$,

$$c \sim c' \iff \exists u \in G, \text{ such that } c'_1 = u^{-1}c_1 s(u)$$

**Pf.** First let us show the expression of $c_n$ by induction. Take $A = c_1 \in G$, then we know that $c_0 = 1$, and $c_1 = A$. Thus $c_0 = c_{1+(-1)} = c_1 s(c_{-1}) = 1$, $c_{-1} = s^{-1}(A^{-1})$.

Suppose the expression of $c_n$ is true for $n = m, -m$, where $m \in \mathbb{Z}$, and $m > 0$, then

$$\begin{aligned} c_{m+1} &= c_1 s(c_m) = As(As(A)s^2(A)\cdots s^{m-1}(A)) \\ &= As(A)s^2(A)\cdots s^m(A) \\ c_{-m-1} &= c_{-1}s^{-1}(c_{-m}) \\ &= s^{-1}(A^{-1})s^{-1}(s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-m}(A^{-1})) \\ &= s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-m-1}(A^{-1}) \end{aligned}$$

Hence the expression for $c_n$ holds for $\forall n \in \mathbb{Z}$. Conversely, for any $A \in G$, that expression gives a cocycle in $Z^1(\mathbb{Z}, G)$, because ${c_0}^0 c_n = c_n = c_{0+n}$, ${c_n}^n c_0 = c_n = c_{n+0}$, $\forall n \in \mathbb{Z}$, and for

$\forall m, t \in \mathbb{Z}$, $m, t > 0$, we have

$$\begin{aligned}
{c_t}^t c_m &= As(A)s^2(A)\cdots s^{t-1}(A)s^t(As(A)s^2(A)\cdots s^{m-1}(A)) \\
&= As(A)s^2(A)\cdots s^{t+m-1}(A) = c_{t+m} \\
{c_t}^t c_{-m} &= As(A)s^2(A)\cdots s^{t-1}(A)s^t(s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-m}(A^{-1})) \\
&= As(A)s^2(A)\cdots s^{t-1}(A)s^{t-1}(A^{-1})s^{t-2}(A^{-1})\cdots s^{t-m}(A^{-1}) \\
&= \begin{cases} As(A)s^2(A)\cdots s^{t-m-1}(A) & \text{if } t > m \\ 1 & \text{if } t = m \\ s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{t-m}(A^{-1}) & \text{if } t < m \end{cases} \\
&= c_{t-m} \\
{c_{-t}}^{-t} c_m &= s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-t}(A^{-1})s^{-t}(As(A)s^2(A)\cdots s^{m-1}(A)) \\
&= s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-t}(A^{-1})s^{-t}(A)s^{-t+1}(A)s^{-t+2}(A)\cdots s^{m-t-1}(A) \\
&= \begin{cases} As(A)s^2(A)\cdots s^{m-t-1}(A) & \text{if } m > t \\ 1 & \text{if } m = t \\ s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{m-t}(A^{-1}) & \text{if } m < t \end{cases} \\
&= c_{m-t} \\
{c_{-t}}^{-t} c_{-m} &= s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-t}(A^{-1})s^{-t}(s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-m}(A^{-1})) \\
&= s^{-1}(A^{-1})s^{-2}(A^{-1})\cdots s^{-t}(A^{-1})s^{-t-1}(A^{-1})s^{-t-2}(A^{-1})\cdots s^{-t-m}(A^{-1}) \\
&= c_{-t-m}
\end{aligned}$$

Moreover, for any two $c, c' \in Z^1(\mathbb{Z}, G)$, $c \sim c' \iff \exists u \in G$, such that $c'_n = u^{-1}c_n s^n(u)$, $\forall n \in \mathbb{Z}$. Thus if $c \sim c'$, we have $c'_1 = u^{-1}c_1 s(u)$.

But if $c'_1 = u^{-1}c_1 s(u)$, for some $u \in G$, we have ${c'_1}^{-1} = s(u^{-1})c_1^{-1}u$, and thus

$$s^{m-1}(c'_1) = s^{m-1}(u)^{-1}s^{m-1}(c_1)s^m(u), \text{ for } m > 0 \tag{27}$$

$$s^m({c'_1}^{-1}) = s^{m+1}(u^{-1})s^m(c_1^{-1})s^m(u), \text{ for } m < 0 \tag{28}$$

When $n > 0$, multiply the equations for $m = 1, 2, \ldots, n$ in (27) together, we get

$$c'_1 s(c'_1)s^2(c'_1)\cdots s^{n-1}(c'_1) = u^{-1}c_1 s(c_1)s^2(c_1)\cdots s^{n-1}(c_1)s^n(u)$$

i.e., $c'_n = u^{-1}c_n s^n(u)$. Similarly, when $n < 0$, multiply the equations for $m = -1, -2, \ldots, n$ in (28) together, we get

$$s^{-1}({c'_1}^{-1})s^{-2}({c'_1}^{-1})\cdots s^n({c'_1}^{-1}) = u^{-1}s^{-1}(c_1^{-1})s^{-2}(c_1^{-1})\cdots s^n(c_1^{-1})s^n(u)$$

i.e., $c'_n = u^{-1}c_n s^n(u)$. Obviously, $c'_0 = u^{-1}c_0 s^0(u) = 1$, hence we get $c'_n = u^{-1}c_n s^n(u)$ for $\forall n \in \mathbb{Z}$, and then $c \sim c'$. $\square$

Now let us consider the case that $G, M$ are both contained in an algebra $\mathcal{A}$, and the actions of $G$ on $M$ and $\mathbb{Z}$ on $\mathcal{A}$ are both given by conjugation. Assume the action of $\mathbb{Z}$ on $\mathcal{A}$ is given by a fixed element $P \in G$, i.e., ${}^1g = PgP^{-1}$, $\forall g \in G$. To signify this action is given by $P$, we denote the corresponding $Z^1(\mathbb{Z}, G)$, $H^1(\mathbb{Z}, G)$, $M_c$, $P_c$ and the equivalence relation $\sim$ by $Z^1(\mathbb{Z}, G)_P$, $H^1(\mathbb{Z}, G)_P$, $M_{c,P}$, $P_{c,P}$ and $\overset{P}{\sim}$ respectively. In those notations, we have the following:

**Corollary 5.1.1.** $\forall c \in Z^1(\mathbb{Z}, G)_P$, $c_n = (c_1 P)^n P^{-n}$, $n \in \mathbb{Z}$. And if $c, c' \in Z^1(\mathbb{Z}, G)_P$, $c \overset{P}{\sim} c' \iff \exists u \in G$, such that $c'_1 P = u^{-1}c_1 P u$. Moreover, there is a bijection $i_P$ between $H^1(\mathbb{Z}, G)_P$ and $G/\sim$, where the equivalence relation is given by conjugation in $G$, and for every $[c] \in H^1(\mathbb{Z}, G)_P$, $M_c = C_{(c_1 P)}(M)$, the centralizer of $c_1 P$ in $M$. Thus for any two fixed $P, Q \in G$, $i_{PQ} = i_Q^{-1} \circ i_P$ gives a bijection between $H^1(\mathbb{Z}, G)_P$ and $H^1(\mathbb{Z}, G)_Q$. In addition, if $i_{PQ}([c]) = [d]$, then $M_{c,P} \simeq M_{d,Q}$.

**Pf.** For $\forall c \in Z^1(\mathbb{Z}, G)$, let $A = c_1 \in G$, we have

$$\begin{aligned} c_n &= \begin{cases} A(PAP^{-1})(P^2AP^{-2})\cdots(P^{n-1}AP^{-(n-1)}) & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ (P^{-1}A^{-1}P)(P^{-2}A^{-1}P^2)\cdots(P^nA^{-1}P^{-n}) & \text{if } n < 0 \end{cases} \\ &= (AP)^n P^{-n} \end{aligned}$$

Moreover, for any two $c, c' \in Z^1(\mathbb{Z}, G)$, $c \sim c' \iff \exists u \in G$, such that $c'_1 = u^{-1}c_1 P u P^{-1}$, i.e. $c'_1 P = u^{-1}c_1 P u$, $c'_1 P$ and $c_1 P$ are conjugate to each other in $G$.

Define a map $i_P : H^1(\mathbb{Z}, G)_P \to G/\sim$ as $i_P([c]) = [c_1 P]$. It is easy to know that it is well-defined and bijective. And for every $[c] \in H^1(\mathcal{G}, G)_P$, we have $M_c = \{x \in M : (c_1 P)x(c_1 P)^{-1} = x\} = C_{(c_1 P)}(M)$, which is obvious.

If $i_{PQ}([c]) = i_Q^{-1} \circ i_P([c]) = [d]$, then $d \sim d'$ for the cocycle $d' \in Z^1(\mathcal{G}, G)_Q$ with $d'_1 = c_1 P Q^{-1}$. One can verify directly that $M_{c,P} = M_{d',Q}$, thus $M_{c,P} = M_{d',Q} \simeq M_{d,Q}$. $\square$

The maps $i_P$ and $i_{PQ}$ in this corollary are just the $\tau_c$'s in Proposition 2.1.2, if taking $[c] \in H^1(\mathbb{Z}, G)_{1_G}$ with $c_1 = P$ and $[c] \in H^1(\mathbb{Z}, G)_Q$ with $c_1 = PQ^{-1}$ respectively, where $H^1(\mathbb{Z}, G)_{1_G}$ is identified with $G/\sim$. One can choose to prove those parts of the corollary by this method.

## 5.2 Special Linear Group

Now I think I am ready to consider the cyclic action of a matrix on a matrix algebra by conjugation. Let $m \in \mathbb{Z}$ be a positive integer, the matrix be some $P \in \mathrm{SL}_m(\mathbb{Z})$ and the matrix algebra be $M_m(\mathbb{Z})$. Suppose the order of this action of $P$ on $\mathrm{SL}_m(\mathbb{Z})$ is $h$, and this action is irreducible, i.e., $P$ satisfies $f(P) = 0$ for some irreducible polynomial $f(t) \in \mathbb{Z}[t]$. Let $\mathcal{G} = \mathbb{Z}/h\mathbb{Z}$, $G = \mathrm{SL}_m(\mathbb{Z})$, $M = \mathrm{sl}_m(\mathbb{Z})$, $\mathcal{A} = M_m(\mathbb{Z})$ and consider the triple system $(\mathcal{G}, (G, M))$.

If $h = 0$, i.e. the action of $P$ on $G$ is infinite cyclic, then by Corollary 5.1.1, we have already known the $H^1(\mathcal{G}, G)_P$ and $M_{c,P}$, and they are independent of the choice of $P$ which gives an infinite cyclic action.

Now we turn to the situation that the action of $P$ on $G$ is finite cyclic, thus $h > 0$, and the following is evident:

**Corollary 5.2.1.** $Z^1(\mathcal{G}, G)_P = \{c \in Z^1(\mathbb{Z}, G)_P | (c_1 P)^h = P^h\}$, and for any two $c, c' \in Z^1(\mathcal{G}, G)_P$, $c \overset{P}{\sim} c' \iff \exists u \in G$, such that $c'_1 P = u^{-1} c_1 P u$. Moreover, there is a bijection $i_P$ between $H^1(\mathcal{G}, G)_P$ and $\{A \in G | A^h = P^h\}/\sim$, where the equivalence relation is given by conjugation in $G$.

**Pf.** Similar to that of Corollary 5.1.1, define the map $i_P : H^1(\mathcal{G}, G)_P \to \{A \in G | A^h = P^h\}/\sim$ as $i_P([c]) = [c_1 P]$, and it is again well-defined and bijective. □

**Corollary 5.2.2.** If the actions of two fixed $P, Q \in G$ have the same order $h$, then there is a bijection $i'_{PQ}$ between $H^1(\mathcal{G}, G)_P$ and $H^1(\mathcal{G}, G)_Q$. In addition, if $i'_{PQ}([c]) = [d]$, then $M_{c,P}/P_{c,P} \simeq M_{d,Q}/P_{d,Q}$.

**Pf.** First, we claim that there is no irreducible finite cyclic action in the case that $m$ odd and $h$ even, and for the other cases, if there is such an action, we must have

$$P^h = \begin{cases} I, & \text{if } m \text{ odd, and } h \text{ odd} \\ \pm I, & \text{if } m \text{ even, and } h \text{ odd} \\ -I, & \text{if } m \text{ even, and } h \text{ even} \end{cases}$$

Now we show the claim. Because the order of the action of $P$ on $G$ is $h$, we have $P^h A P^{-h} = A$, $\forall A \in G$. Thus $P^h = aI$, for some $a \in \mathbb{Z}$. Notice that $\det(P^h) = a^m = 1$, $a = \pm 1$ when $m$ even, and 1 when $m$ odd.

When $h$ is even, $P^h$ must be $-I$. Otherwise we have $P^h - I = 0$, then either $P^{h/2} + I = 0$

or $P^{h/2} - I = 0$, i.e., $P^{h/2} = \pm I$. The reason is that the action of $P$ is irreducible, and satisfies $f(P) = 0$ for some irreducible polynomial $f(t) \in \mathbb{Z}[t]$. By Lemma 4.2.1, we know $f$ is the minimal polynomial for $P$, and hence $f(t)|t^h - 1$. Thus either $f(t)|t^{h/2} + 1$ or $f(t)|t^{h/2} - 1$, and then either $P^{h/2} + I = 0$ or $P^{h/2} - I = 0$, and $P^{h/2} = \pm I$. But this contradicts the assumption that the order of the action of $P$ on $G$ is $h$. So $P^h$ must be $-I$.

Summing up, we get the above claim.

Now we define the map

$$\begin{array}{rccc} r_{PQ}: & \{A \in G | A^h = P^h\}/\sim & \longrightarrow & \{A \in G | A^h = Q^h\}/\sim \\ & [A] & \longmapsto & [r_{PQ}(A)] \end{array}$$

where $r_{PQ}(A) = A$ if $P^h = Q^h$ and $r_{PQ}(A) = -A$ if $P^h = -Q^h$. This map is well-defined and bijective. Then the $i'_{PQ}$ is taken to be $i_Q^{-1} \circ r_{PQ} \circ i_P$, a bijection. Under this $i'_{PQ}$, if $i'_{PQ}([c]) = [d]$, then $d \sim d'$ for the cocycle $d' \in Z^1(\mathcal{G}, G)_Q$ with $d'_1 = c_1 P Q^{-1}$ when $P^h = Q^h$ and $d'_1 = -c_1 P Q^{-1}$ when $P^h = -Q^h$. It can still be verified that $M_{c,P} = M_{d',Q}$, $P_{c,P} = P_{d',Q}$. Thus we still have $M_{c,P}/P_{c,P} = M_{d',Q}/P_{d',Q} \simeq M_{d,Q}/P_{d,Q}$. $\square$

The map $i'_{PQ}$ in the above corollary is just the $\tau_c$ in Proposition 2.1.2, if taking $[c] \in H^1(\mathcal{G}, G)_Q$ with $c_1 = \pm P Q^{-1}$, where the sign for the $\pm P Q^{-1}$ is chosen according to whether $P^h = Q^h$ or not. However, the map $i_P$ in the corollary 5.2.1 may not be viewed this way.

From Corollary 5.2.2, we know that, for a given positive integer $h$, the $H^1(\mathcal{G}, G)$ and $M_c/P_c$ can be determined, independent of the choice of $P$ which gives the cyclic action of order $h$. Now we are going to determine completely $H^1(\mathcal{G}, G)$ and $M_c/P_c$ in $m = 2$ case without assuming irreducible action in the beginning.

**Lemma 5.2.1.** When $m = 2$, either $P = \pm I$ or $\Phi_e(P) = 0$, for one $e \in \{3, 4, 6\}$, where $\Phi_3(t) = t^2 + t + 1$, $\Phi_4(t) = t^2 + 1$, and $\Phi_6(t) = t^2 - t + 1$ are cyclotomic functions. Thus $P$ always acts irreducibly, and $h$ is $1, 2$ or $3$.

**Pf.** Although we do not assume irreducible action in the beginning, the argument in Corollary 5.2.2 to show $P^h = \pm I$ still works. Suppose the Jordan canonical form of $P$ is $J \in \mathrm{SL}_2(\mathbb{C})$, then $J$ is either of the form $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ or of the form $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, and $J^h = \pm I$.

If $J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, then $J^h = \begin{pmatrix} \lambda^h & h\lambda^{h-1} \\ 0 & \lambda^h \end{pmatrix} = \pm I$, $\lambda = 0$, impossible. Thus $J =$

$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. Again, by $J^h = \pm I$, we get $\lambda_1 = \exp(k\pi i/h), \lambda_2 = \exp(-k\pi i/h)$ with some $k \in \mathbb{Z}$.

Notice that $\mathrm{tr}(J) = \mathrm{tr}(P) \in \mathbb{Z}$, so $\lambda_1 + \lambda_2 = 2\cos(k\pi/h) \in \mathbb{Z}$. But $\cos(k\pi/h) \in [-1, 1]$, so $\cos(k\pi/h) = -1, -1/2, 0, 1/2, 1$. For $\cos(k\pi/h) = \pm 1$, $(\lambda_1, \lambda_2) = (\pm 1, \pm 1)$, thus $P = \pm I$. For the other values, $\mathrm{tr}(P) = \mathrm{tr}(J) = \lambda_1 + \lambda_2 = 2\cos(k\pi/h) = -1, 0, 1$, thus the characteristic polynomial for $P$ is $\Phi_e$ for some $e \in \{3, 4, 6\}$, and $\Phi_e(P) = 0$.

As $t-1, t+1, \Phi_3(t), \Phi_4(t), \Phi_6(t)$ are all irreducible, $P$ always acts irreducibly. For the cases of $t-1, t+1$, it is obvious that $h = 1$. For the case of $\Phi_4(t)$, $P^2 = -I$, thus $h|2$. But if $h = 1$, we will have $P = \pm I$, and it doesn't satisfy $\Phi_4(P) = 0$, contradiction. So $h = 2$. For the cases of $\Phi_3(t), \Phi_6(t)$, $P^3 = \pm I$, thus $h|3$. And for the same reason, if $h = 1$ for either of them, we will have $P = \pm I$, and it doesn't satisfy the corresponding $\Phi_e(P) = 0$, $e \in \{3, 6\}$, contradiction. So $h = 3$. $\square$

If $h = 1$, it is a trivial case, $H^1(\mathcal{G}, G) = 1$ and $M_1/P_1 = 1$. If $h = 2$, then $P^2 = -I$. Such a $P$ can be chosen to be $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, the matrix in (9), then we get back the simple example in section 3.3.

In that case, we used the Gauss Correspondence to get $H^1(\mathcal{G}, G)$, but we can also use the generalization of Gauss Correspondence to do it. In Theorem 4.4.1, if we take $k = \mathbb{Q}$, $f(t) = \Phi_4(t)$, $P = J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $\theta = i$, then $n = 2$, $\mathcal{O}_k = \mathbb{Z}$, $\mathcal{O}_k^\times = \{\pm 1\}$, $K = \mathbb{Q}(i)$, and $H_K = 1$. $N_{K|k}\mathcal{O}_K^\times = 1$, because the only non-trivial automorphism in $\mathrm{Gal}(K/k)$ is the complex conjugation. $\tilde{M}_2^+(\mathbb{Z}; \Phi_4) = \{A \in M_2(\mathbb{Z}) | \Phi_4(A) = 0\}/\sim$, where the equivalence relation is given by conjugation in $\mathrm{SL}_2(\mathbb{Z})$. From Lemma 4.2.1, we know that any matrix $A \in M_2(\mathbb{Z})$ with $\Phi_4(A) = 0$ must have $\Phi_4$ as its characteristic polynomial, thus $\det(A) = 1$, $A \in \mathrm{SL}_2(\mathbb{Z})$. Also noticing that $P^2 = -I$, we have

$$\begin{aligned} \tilde{M}_2^+(\mathbb{Z}; \Phi_4) &= \{A \in M_2(\mathbb{Z}) | \Phi_4(A) = 0\}/\sim \\ &= \{A \in \mathrm{SL}_2(\mathbb{Z}) | \Phi_4(A) = 0\}/\sim \\ &= \{A \in \mathrm{SL}_2(\mathbb{Z}) | A^2 = -I\}/\sim \\ &= \{A \in \mathrm{SL}_2(\mathbb{Z}) | A^2 = P^2\}/\sim \\ &\xrightarrow{\sim} H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P \end{aligned}$$

By (15), we have

$$i_{\Phi_4} : \tilde{M}_2^+(\mathbb{Z}; \Phi_4) \xrightarrow{\sim} \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times H_K = \{\pm 1\}$$

and then

$$i_P^{-1} \circ i_{\Phi_4}^{-1} : \{\pm 1\} \xrightarrow{\sim} \tilde{M}_2^+(\mathbb{Z}; \Phi_4) \xrightarrow{\sim} H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$$

By the definition of $i_P$ and $i_{\Phi_4}$, we can find the elements of $H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$ easily. Take $I, Q \in \mathrm{GL}_2(\mathbb{Z})$, where $Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. We have $\det(I) = 1$, $\det(Q) = -1$, and the elements in $H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$ are given by $I^{-1}PIP^{-1} = I$ and $Q^{-1}PQP^{-1} = -I$, i.e., $H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P = \{[c], [d]\}$ with $c_1 = I$ and $d_1 = -I$.

Although it seems that the solution does not get simpler than before, the generalization of Gauss Correspondence can be applied to other cases where getting a solution by the original Gauss Correspondence is not so easy. We can see that when we look at $h = 3$ case instead of $h = 2$ case above.

Similar as before, take $k = \mathbb{Q}$, $f(t) = \Phi_3(t)$, $P = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$, and $\theta = \omega$ in Theorem 4.4.1, where $\omega$ is a primitive cubic root of unity in $\mathbb{C}$. Then $n = 2$, $\mathcal{O}_k = \mathbb{Z}$, $\mathcal{O}_k^\times = \{\pm 1\}$, $K = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$, and $H_K = 1$ again. $N_{K|k}\mathcal{O}_K^\times = 1$ again, for the same reason that the only non-trivial automorphism in $\mathrm{Gal}(K/k)$ is the complex conjugation. $\tilde{M}_2^+(\mathbb{Z}; \Phi_3) = \{A \in M_2(\mathbb{Z}) | \Phi_3(A) = 0\}/\sim$, where the equivalence relation is given by conjugation in $\mathrm{SL}_2(\mathbb{Z})$. Again from Lemma 4.2.1, any matrix $A \in M_2(\mathbb{Z})$ with $\Phi_3(A) = 0$ have $\Phi_3$ as its characteristic polynomial, thus $\det(A) = 1$, $A \in \mathrm{SL}_2(\mathbb{Z})$, and $\tilde{M}_2^+(\mathbb{Z}; \Phi_3) = \{A \in M_2(\mathbb{Z}) | \Phi_3(A) = 0\}/\sim = \{A \in \mathrm{SL}_2(\mathbb{Z}) | \Phi_3(A) = 0\}/\sim$.

However, $\{A \in \mathrm{SL}_2(\mathbb{Z}) | \Phi_3(A) = 0\}/\sim$ is different from $\{A \in \mathrm{SL}_2(\mathbb{Z}) | A^3 = P^3 = I\}/\sim$ in this case. So in order to get $H^1(\mathbb{Z}/3\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$, we need to find out the extra elements outside $\{A \in \mathrm{SL}_2(\mathbb{Z}) | \Phi_3(A) = 0\}/\sim$.

It is obvious that $I$ is such an element. $\Phi_3(I) = 3I \neq 0$, but $I^3 = I = P^3$. By direct computation, we can know that it is the only matrix in $\mathrm{SL}_2(\mathbb{Z})$ satisfying this property, and any other matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ with $A^3 = I$ satisfies $\Phi_3(A) = 0$. So $\{A \in \mathrm{SL}_2(\mathbb{Z}) | A^3 = P^3\}/\sim = \{[I]\} \cup \tilde{M}_2^+(\mathbb{Z}; \Phi_3)$, a disjoint union.

For $\tilde{M}_2^+(\mathbb{Z}; \Phi_3)$, we follow the similar procedure as before. By (15), we have

$$i_{\Phi_3}^{-1} : \{\pm 1\} = \mathcal{O}_k^\times / N_{K|k}\mathcal{O}_K^\times \times H_K \xrightarrow{\sim} \tilde{M}_2^+(\mathbb{Z}; \Phi_3)$$

Take the same $I, Q \in \mathrm{GL}_2(\mathbb{Z})$ as before. $\det(I) = 1$, $\det(Q) = -1$, and the elements in $\tilde{M}_2^+(\mathbb{Z}; \Phi_3)$ are given by $I^{-1}PI = P$ and $Q^{-1}PQ = P^2$, so $\{A \in \mathrm{SL}_2(\mathbb{Z}) | A^3 = P^3\}/\sim = \{[I], [P], [P^2]\}$.

Now from $i_P^{-1} : \{A \in \mathrm{SL}_2(\mathbb{Z}) | A^3 = P^3\}/\sim \xrightarrow{\sim} H^1(\mathbb{Z}/3\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$, we get $H^1(\mathbb{Z}/3\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P = \{[c], [c'], [c'']\}$, with

$$\begin{aligned} c_1 &= IP^{-1} = P^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \\ c_1' &= PP^{-1} = I \\ c_1'' &= P^2P^{-1} = P = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \end{aligned}$$

Next, we are going to compute the corresponding $M_c/P_c$ for them. For any element $[c] \in H^1(\mathbb{Z}/3\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$, let $A = c_1 \in \mathrm{SL}_2(\mathbb{Z})$, then we can get the following by direct computation:

$$M_c = \{x \in \mathrm{sl}_2(\mathbb{Z}) : (AP)x = x(AP)\}$$

$$P_c = \{p_c(x) = x + (AP)x(AP)^{-1} + (AP)^2x(AP)^{-2}, x \in \mathrm{sl}_2(\mathbb{Z})\}$$

For the $[c] \in H^1(\mathbb{Z}/3\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$ with $c_1 = P^{-1}$, it is easy to get $M_c = \mathrm{sl}_2(\mathbb{Z})$ and $P_c = 3\mathrm{sl}_2(\mathbb{Z})$, thus $M_c/P_c = (\mathbb{Z}/3\mathbb{Z})^3$.

For the $[c'], [c''] \in H^1(\mathbb{Z}/3\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z}))_P$, $c_1' = I$, $c_1'' = P$, then $c_1'P = P$, $(c_1'P)^2 = P^2$, $c_1''P = P^2 = P^{-1}$, $(c_1''P)^2 = P^4 = P$. Thus $M_{c'} = M_{c''}$ and $P_{c'} = P_{c''}$. Then by direct computation, we get $M_{c'} = P_{c'} = \begin{pmatrix} 1 & -2 \\ 2 & -1 \end{pmatrix} \mathbb{Z}$, so $M_{c'}/P_{c'} = M_{c''}/P_{c''} = 1$.

In general, for $m \geq 3$, we can still use the methods developed here to try to find $H^1(\mathcal{G}, G)$ and $M_c/P_c$.

### 5.3 Congruence Subgroup

After $\mathrm{SL}_m(\mathbb{Z})$, one may want to explore the case of the cyclic action of a matrix on a congruence subgroup $\Gamma(N)$. To deal with this question, I will use the polynomial cohomology.

When $N$ is prime, it has already been studied by Prof. Kühnlein ([10]). However, in the view point of polynomial cohomology, his proof can be made more organized and clearer. In this section, I will explain that first, and then I will study the case when $N$ is not prime.

For positive integers $N$ and $m$, the congruence subgroup $\Gamma(N)$ in the special linear group $\mathrm{SL}_m(\mathbb{Z})$ is defined to be

$$\Gamma(N) = \{A \in \mathrm{SL}_m(\mathbb{Z}) : A \equiv I \pmod{N}\}$$

Now take $m = \phi(e)$ for a positive integer $e \geq 3$, and let $K = \mathbb{Q}(\zeta)$, for a primitive $e$-th root of unity $\zeta$, then we know $[K : \mathbb{Q}] = m$. Take an element $\theta \in \mathrm{GL}_m(\mathbb{Z})$, and let it act cyclically on $M_m(\mathbb{Z})$ by conjugation. Suppose this action is irreducible and finite, and $\theta$ satisfies $\Phi_e(\theta) = 0$. Consider the triple system $(\mathcal{G}, (\Delta, M))$ with $\mathcal{G} =< \theta >= \mathbb{Z}/e\mathbb{Z}$, $\Delta = \Gamma(N)$.

$\theta$ is actually an element in $\mathrm{SL}_m(\mathbb{Z})$. Because $\Phi_e(\theta) = 0$, by Lemma 4.2.1, we know $\Phi_e$ is the characteristic polynomial of $\theta$, thus the eigenvalues of $\theta$ are just all the primitive $e$-th roots of unity in $\mathbb{C}$. For $e \geq 3$, they come in pairs of complex conjugation and their product is 1. So $\det(\theta) = 1$.

Assume $N$ is prime at first. In this case we denote it by $p$. We also denote $\Gamma = \mathrm{GL}_m(\mathbb{Z})$, and further assume that $p$ does not divide $e$ and $p \geq 3$.

**Lemma 5.3.1.** There is a bijection between $H^1(\mathcal{G}, \Delta)$ and $H^1(\Phi_e, \Delta\theta; \Delta)$.

**Pf.** The proof in Corollary 5.2.1 still works here, and we can get that the map $i_\theta : H^1(\mathcal{G}, \Delta) \to H^1(t^e - 1, \Delta\theta; \Delta)$ with $i_\theta([c]) = [c_1\theta]$ is well-defined and bijective.

According to [10], any element of order dividing $e$ in $\Delta\theta$ is conjugate to a zero of $\Phi_e$ in $\Gamma$. Thus it is itself a zero of $\Phi_e$, and then $H^1(t^e - 1, \Delta\theta; \Delta) = H^1(\Phi_e, \Delta\theta; \Delta)$. We need the conditions that $p$ is prime and does not divide $e$ in this step. However, we can find the extra elements as what I did in the last section. □

Note that the map $i_\theta$ in the above lemma cannot be viewed as a map $\tau_c$ in Proposition 2.1.2.

From this lemma, the problem of determining $H^1(\mathcal{G}, \Delta)$ reduces to that of $H^1(\Phi_e, \Delta\theta; \Delta)$. Now look at the following exact sequence:

$$1 \longrightarrow \Delta \longrightarrow \Gamma \overset{\mathrm{mod}_p}{\longrightarrow} \Gamma/\Delta \longrightarrow 1 \tag{29}$$

where $\mathrm{mod}_p$ is given by modulo $p$ for each entry. By Theorem 4.5.1, where we take

- the commutative ring $R$ to be $\mathbb{Z}$;
- the polynomial $f$ to be $\Phi_e \in \mathbb{Z}[t]$;

- the $R$-algebra $\mathcal{A}$ to be $M_m(\mathbb{Z})$;
- the multiplicative subset $M$ to be $\Gamma = \mathrm{GL}_m(\mathbb{Z})$;
- the multiplicative set $S$ to be $\Gamma/\Delta$, which is $\{\tau \in \mathrm{GL}_m(\mathbb{F}_p) : \det(\tau) = \pm 1\} \subset \mathrm{GL}_m(\mathbb{F}_p)$;
- the $R$-algebra $\mathcal{B}$ to be $M_m(\mathbb{F}_p)$;
- the map $\pi : \mathcal{A} \to \mathcal{B}$ to be the map given by mod $p$ for each entry;
- $P$ to be $\theta \in \Gamma^{\Phi_e}$;

we can get the following long exact sequence of pointed sets:

$$C_{\overline{\theta}}(\Gamma/\Delta) \xrightarrow{\delta_\theta} H^1(\Phi_e, \Delta\theta; \Delta) \xrightarrow{i} H^1(\Phi_e, \Gamma) \xrightarrow{\mathrm{mod}_p} H^1(\Phi_e, \Gamma/\Delta) \tag{30}$$

where $\overline{\theta} = \mathrm{mod}_p(\theta) = \Delta\theta \in (\Gamma/\Delta)^{\Phi_e}$. And if $\{\delta_i\theta \in (\Delta\theta)^{\Phi_e} : i \in \mathcal{I}\}$ is a set of representatives of $i(H^1(\Phi_e, \Delta\theta; \Delta))$, we can have a bijection $i_{\Phi_e}$:

$$H^1(\Phi_e, \Delta\theta; \Delta) \xrightarrow{\sim} \coprod_{i \in \mathcal{I}} (C_{\delta_i\theta}(\Gamma)\Delta/\Delta) \backslash C_{\overline{\theta}}(\Gamma/\Delta)$$

Then we need to determine $\mathcal{I}$ and those $(C_{\delta_i\theta}(\Gamma)\Delta/\Delta)\backslash C_{\overline{\theta}}(\Gamma/\Delta)$. For the latter, we have $C_{\delta_i\theta}(\Gamma)\Delta/\Delta \simeq \mathcal{O}_K^\times/((1+p\mathcal{O}_K) \cap \mathcal{O}_K^\times)$ ([10]). And because $C_{\overline{\theta}}(\Gamma/\Delta)$ is finite, all those $(C_{\delta_i\theta}(\Gamma)\Delta/\Delta)\backslash C_{\overline{\theta}}(\Gamma/\Delta)$ have the same cardinality, thus we can get a bijection:

$$H^1(\Phi_e, \Delta\theta; \Delta) \xrightarrow{\sim} \mathcal{I} \times (C_\theta(\Gamma)\Delta/\Delta) \backslash C_{\overline{\theta}}(\Gamma/\Delta) \tag{31}$$

If $p$ is not prime, we can also get a similar result like this. But for $p$ prime, we can get $\mathcal{I}$ in addition. The method is to use the polynomial cohomology again.

Notice that $\Gamma/\Delta = \{\tau \in \mathrm{GL}_m(\mathbb{F}_p) : \det(\tau) = \pm 1\} \subset \mathrm{GL}_m(\mathbb{F}_p)$, we have another exact sequence:

$$1 \longrightarrow \Gamma/\Delta \longrightarrow \mathrm{GL}_m(\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^\times/\{\pm 1\} \longrightarrow 1 \tag{32}$$

Now use Theorem 4.5.1, where we take

- The commutative ring $R$ to be $\mathbb{F}_p$;
- The polynomial $f$ to be the $\Phi_e \in \mathbb{F}_p[t]$;

- The $R$-algebra $\mathcal{A}$ to be $M_m(\mathbb{F}_p)$;
- The multiplicative subset $M$ to be $\mathrm{GL}_m(\mathbb{F}_p)$;
- The multiplicative set $S$ to be $\mathbb{F}_p^\times/\{\pm 1\}$;
- The map $\pi : M \to S$ to be the determinant map;
- $P$ to be $\overline{\gamma} = \mathrm{mod}_p(\gamma) \in (\Gamma/\Delta)^{\Phi_e} \subset \mathrm{GL}_m(\mathbb{F}_p)^{\Phi_e}$, where $\gamma$ is an arbitrary element in $\Gamma^{\Phi_e}$;

we have the following long exact sequence of pointed sets:

$$C_{\overline{\gamma}}(\mathrm{GL}_m(\mathbb{F}_p)) \stackrel{\det}{\to} \mathbb{F}_p^\times/\{\pm 1\} \stackrel{\delta_{\overline{\gamma}}}{\to} H^1(\Phi_e, \Gamma/\Delta) \stackrel{i}{\to} H^1(\Phi_e, \mathrm{GL}_m(\mathbb{F}_p)) \tag{33}$$

For $p$ prime, we can show that the determinant map in the above exact sequence is surjective ([10]). Thus by exactness, $\ker(i) = i^{-1}([\overline{\gamma}]) = [\overline{\gamma}]$. For any other $\overline{\gamma}' \in \Gamma^{\Phi_e}$, by [10] again, we can get that $[\overline{\gamma}] = [\overline{\gamma}']$ in $H^1(\Phi_e, \mathrm{GL}_m(\mathbb{F}_p))$, then $[\overline{\gamma}] = [\overline{\gamma}']$ in $H^1(\Phi_e, \Gamma/\Delta)$, which in turn shows that the map $\mathrm{mod}_p$ in (30) satisfies $\ker(\mathrm{mod}_p) = H^1(\Phi_e, \Gamma)$. Hence the map $i$ in (30) is surjective, and $\mathcal{I}$ can be taken as $H^1(\Phi_e, \Gamma)$.

For $\forall A \in M_m(\mathbb{Z})$, if $\Phi_e(A) = 0$, then by the same argument as that for $\theta$ before, $\det(A) = 1$, and $A \in \Gamma$. So we have

$$\begin{aligned} \tilde{M}_m(\mathbb{Z}; \Phi_e) &= \{A \in M_m(\mathbb{Z}) | \Phi_e(A) = 0\}/\sim \\ &= \{A \in \Gamma | \Phi_e(A) = 0\}/\sim \\ &= H^1(\Phi_e, \Gamma) \end{aligned}$$

where the equivalence relation $\sim$ is given by conjugation in $\Gamma$. Moreover, by LMT, $H^1(\Phi_e, \Gamma) = \tilde{M}_m(\mathbb{Z}; \Phi_e) \simeq H_K$. Hence from (31), we have a bijection:

$$H^1(\Phi_e, \Delta\theta; \Delta) \stackrel{\sim}{\longrightarrow} H_K \times (C_\theta(\Gamma)\Delta/\Delta) \backslash C_{\overline{\theta}}(\Gamma/\Delta) \tag{34}$$

In view of Lemma 5.3.1, it becomes

$$H^1(\mathcal{G}, \Delta) \stackrel{\sim}{\longrightarrow} H_K \times (C_\theta(\Gamma)\Delta/\Delta) \backslash C_{\overline{\theta}}(\Gamma/\Delta) \tag{35}$$

Now we are going to explore the case when $N$ is not prime. Denote more naturally $\Gamma$ for $\mathrm{SL}_m(\mathbb{Z})$ instead of $\mathrm{GL}_m(\mathbb{Z})$. Look at the following exact sequence:

$$1 \longrightarrow \Delta \longrightarrow \Gamma \stackrel{\mathrm{mod}_N}{\longrightarrow} \Gamma/\Delta \longrightarrow 1 \tag{36}$$

where $\mathrm{mod}_N$ is given by modulo $N$ for each entry.

Similar as before, in Theorem 4.5.1 we take

- the commutative ring $R$ to be $\mathbb{Z}$;
- the polynomial $f$ to be $\Phi_e \in \mathbb{Z}[t]$;
- the $R$-algebra $\mathcal{A}$ to be $M_m(\mathbb{Z})$;
- the multiplicative subset $M$ to be $\Gamma = \mathrm{SL}_m(\mathbb{Z})$;
- the multiplicative set $S$ to be $\Gamma/\Delta = \mathrm{SL}_m(\mathbb{Z}/N\mathbb{Z})$;
- the $R$-algebra $\mathcal{B}$ to be $M_m(\mathbb{Z}/N\mathbb{Z})$;
- the map $\pi : \mathcal{A} \to \mathcal{B}$ to be the map given by mod $N$ for each entry;
- $P$ to be $\theta \in \Gamma^{\Phi_e}$;

and we have $\ker(\mathrm{mod}_N) = \Delta$, $\mathrm{mod}_N^{-1} \circ \mathrm{mod}_N(\theta) = \Delta\theta$. Also, for $\mathbb{Z}/N\mathbb{Z}$ is a commutative ring with unity, we know $\Gamma/\Delta = \mathrm{SL}_m(\mathbb{Z}/N\mathbb{Z}) = \{A \in M_m(\mathbb{Z}/N\mathbb{Z}) : \det(A) = 1\}$ is a group, and the inverse of an element is given by its companion matrix.

Then we have the following long exact sequence of pointed sets:

$$C_{\overline{\theta}}(\Gamma/\Delta) \xrightarrow{\delta_\theta} H^1(\Phi_e, \Delta\theta; \Delta) \xrightarrow{i} H^1(\Phi_e, \Gamma) \xrightarrow{\mathrm{mod}_N} H^1(\Phi_e, \Gamma/\Delta) \tag{37}$$

where $\overline{\theta} = \mathrm{mod}_N(\theta) = \Delta\theta \in (\Gamma/\Delta)^{\Phi_e}$. And if $\{\delta_i\theta \in (\Delta\theta)^{\Phi_e} : i \in \mathcal{I}\}$ is a set of representatives of $i(H^1(\Phi_e, \Delta\theta; \Delta))$, we have a bijection $i_{\Phi_e}$:

$$H^1(\Phi_e, \Delta\theta; \Delta) \xrightarrow{\sim} \coprod_{i \in \mathcal{I}} (C_{\delta_i\theta}(\Gamma)\Delta/\Delta) \backslash C_{\overline{\theta}}(\Gamma/\Delta) \tag{38}$$

**Lemma 5.3.2.** For any $\tilde{\theta} \in M_m(\mathbb{Z})^{\Phi_e}$, we have $C_{\tilde{\theta}}(M_m(\mathbb{Z})) = \mathbb{Z}[\tilde{\theta}]$ and $\Gamma(N) \cap \mathbb{Z}[\tilde{\theta}] = (1 + N\mathbb{Z}[\tilde{\theta}]) \cap \mathrm{SL}_m(\mathbb{Z})$. Moreover, there is a $\mathbb{Z}$-algebra isomorphism $\tau : C_{\tilde{\theta}}(M_m(\mathbb{Z})) = \mathbb{Z}[\tilde{\theta}] \to \mathcal{O}_K$, such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Z}[\tilde{\theta}] & \xrightarrow{\det} & \mathbb{Z} \\ \downarrow \tau & & \| \\ \mathcal{O}_K & \xrightarrow{N_{K|\mathbb{Q}}} & \mathbb{Z} \end{array}$$

Thus under this $\tau$, we can get that $C_{\tilde{\theta}}(\mathrm{SL}_m(\mathbb{Z}))$ is isomorphic to ${}_N\mathcal{O}_K = \{a \in \mathcal{O}_K | N_{K|\mathbb{Q}}(a) = 1\}$.

**Pf.** For any $\tilde{\theta} \in M_m(\mathbb{Z})^{\Phi_e}$, $\Phi_e(\tilde{\theta}) = 0$. So by Lemma 4.2.1, the characteristic polynomial of $\tilde{\theta}$ is equal to $\Phi_e$. $\Phi_e$ has no multiple roots, thus by Lemma 4.2.2, $C_{\tilde{\theta}}(M_m(\mathbb{Z})) = M_m(\mathbb{Z}) \cap \mathbb{Q}[\tilde{\theta}]$.

But $M_m(\mathbb{Z}) \cap \mathbb{Q}[\tilde{\theta}] = \mathbb{Z}[\tilde{\theta}]$. The reason is as the following. The characteristic polynomial of $\tilde{\theta}$ is $\Phi_e$, thus $\zeta$ is an eigenvalue of $\tilde{\theta}$. So we have

$$\exists\, x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \mathcal{O}_K^m, x \neq 0, s.t. \quad \tilde{\theta}x = \zeta x. \tag{39}$$

Here we know there exists such an eigenvector $x$ in $K^m$. But after multiplying an appropriate number in $\mathbb{Z}$, it can be taken from $\mathcal{O}_K^m$.

Thus for $\forall A \in M_m(\mathbb{Z}) \cap \mathbb{Q}[\tilde{\theta}]$, $A = p(\tilde{\theta})$ for some $p[t] \in \mathbb{Q}[t]$, and then $Ax = p(\tilde{\theta})x = p(\zeta)x$. Hence $p(\zeta)$ is an eigenvalue of $A$, i.e., a root of the polynomial $\det(tI - A)$. Thus $p(\zeta) \in \mathbb{Q}(\zeta) = K$ is integral over $\mathbb{Z}$, and then $p(\zeta) \in \mathcal{O}_K = \mathbb{Z}[\zeta]$.

Suppose $p(\zeta) = q(\zeta)$ for some $q(t) \in \mathbb{Z}[t]$. Then there exists $a(t) \in \mathbb{Q}[t]$, such that $p(t) = q(t) + a(t)\Phi_e(t)$. Hence $A = p(\tilde{\theta}) = q(\tilde{\theta}) + a(\tilde{\theta})\Phi_e(\tilde{\theta}) = q(\tilde{\theta}) \in \mathbb{Z}[\tilde{\theta}]$. Thus we get $M_m(\mathbb{Z}) \cap \mathbb{Q}[\tilde{\theta}] = \mathbb{Z}[\tilde{\theta}]$, and then $C_{\tilde{\theta}}(M_m(\mathbb{Z})) = \mathbb{Z}[\tilde{\theta}]$.

For $\forall A \in \Gamma(N) \cap \mathbb{Z}[\tilde{\theta}]$, there exists $B \in M_m(\mathbb{Z})$, such that $A = 1 + NB \in \mathbb{Z}[\tilde{\theta}]$. So $B \in \mathbb{Q}[\tilde{\theta}] \cap M_m(\mathbb{Z}) = \mathbb{Z}[\tilde{\theta}]$, thus $A \in (1 + N\mathbb{Z}[\tilde{\theta}]) \cap \mathrm{SL}_m(\mathbb{Z})$. The inclusion for the other side is obvious. Hence $\Gamma(N) \cap \mathbb{Z}[\tilde{\theta}] = (1 + N\mathbb{Z}[\tilde{\theta}]) \cap \mathrm{SL}_m(\mathbb{Z})$.

Now let us define

$$\begin{array}{rccc} \tau: & C_{\tilde{\theta}}(M_m(\mathbb{Z})) = \mathbb{Z}[\tilde{\theta}] & \longrightarrow & \mathcal{O}_K = \mathbb{Z}[\zeta] \\ & g(\tilde{\theta}) & \longmapsto & g(\zeta) \end{array}$$

It is obviously a $\mathbb{Z}$-algebra isomorphism. In view of (39), if we take $\mathbf{a} = [x_1, \ldots, x_m]_{\mathbb{Z}} \subseteq \mathcal{O}_K$, then it is an integral ideal in $\mathcal{O}_K$. Thus $\{x_1, \ldots, x_m\}$ forms an integral basis for $\mathbf{a}$, and it is linearly independent over $\mathbb{Q}$. So for any $g(t) \in \mathbb{Z}[t]$, from $\tilde{\theta}x = \zeta x$, we get $g(\tilde{\theta})x = g(\zeta)x$. Hence $\det(g(\tilde{\theta})) = N_{K|\mathbb{Q}}(g(\zeta)) = N_{K|\mathbb{Q}}(\tau(g(\tilde{\theta})))$. The diagram commutes. $\square$

By this lemma, $\forall i \in \mathcal{I}$, we have

$$\begin{aligned} C_{\delta_i\theta}(\Gamma)\Delta/\Delta &\simeq C_{\delta_i\theta}(\Gamma)/(C_{\delta_i\theta}(\Gamma)\cap\Delta) \\ &= C_{\delta_i\theta}(\Gamma)/(C_{\delta_i\theta}(\Gamma)\cap(\Delta\cap\mathbb{Z}[\delta_i\theta])) \\ &= C_{\delta_i\theta}(\Gamma)/(C_{\delta_i\theta}(\Gamma)\cap((1+N\mathbb{Z}[\delta_i\theta])\cap\Gamma)) \\ &= C_{\delta_i\theta}(\Gamma)/(C_{\delta_i\theta}(\Gamma)\cap(1+N\mathbb{Z}[\delta_i\theta])) \\ &\simeq {}_N\mathcal{O}_K/({}_N\mathcal{O}_K\cap(1+N\mathcal{O}_K)) \end{aligned}$$

Again, because $C_{\overline{\theta}}(\Gamma/\Delta)$ is finite, all those $(C_{\delta_i\theta}(\Gamma)\Delta/\Delta)\backslash C_{\overline{\theta}}(\Gamma/\Delta)$ have the same cardinality, thus from (38), we get the following bijection:

$$H^1(\Phi_e,\Delta\theta;\Delta)\xrightarrow{\sim}\mathcal{I}\times(C_\theta(\Gamma)\Delta/\Delta)\backslash C_{\overline{\theta}}(\Gamma/\Delta) \tag{40}$$

Because $H^1(\Phi_e,\Gamma)\simeq H_K\times\{\pm1\}$, we can get an injection

$$H^1(\Phi_e,\Delta\theta;\Delta)\hookrightarrow H_K\times\{\pm1\}\times(C_\theta(\Gamma)\Delta/\Delta)\backslash C_{\overline{\theta}}(\Gamma/\Delta) \tag{41}$$

That is what we can get up to now. Note that $H^1(\Phi_e,\Delta\theta;\Delta)$ is contained in $H^1(t^e-1,\Delta\theta;\Delta)$, which can be identified with $H^1(\mathcal{G},\Delta)$, and there might be some elements outside $H^1(\Phi_e,\Delta\theta;\Delta)$. Thus in order to get $H^1(\mathcal{G},\Delta)$, we need to figure out those outsiders in some way. If $m$ is small, one can accomplish it by direct computation, as what I did in the last section.

# 6 Poincaré Sums for Elliptic Curves over $\mathbb{C}$

## 6.1 Triple System $(L_\tau,(\mathcal{O}^\times,\mathcal{O}))$

The story before are all about triple systems $(\mathcal{G},(G,M))$ with $\mathcal{G}$ finite. But what should the definition be for $\mathcal{G}$ infinite? Especially how should the Poincaré sums be defined? We already have an example in the modular forms, from which our motivation starts. But I want to look at one more example.

Let $\tau$ be a point in the upper half plane. Let $p:\mathbb{C}\to E_\tau$ be the universal covering of the elliptic curve $E_\tau=\mathbb{C}/L_\tau$, where $L_\tau=\mathbb{Z}+\mathbb{Z}\tau$. We know that the Galois group of $p$ is simply $L_\tau$, and the action of $L_\tau$ on $\mathbb{C}$ is given by:

$${}^\omega z=z+\omega,\forall z\in\mathbb{C},\omega\in L_\tau.$$

Let $\mathcal{O}$ denote the set of holomorphic functions over $\mathbb{C}$. Then $L_\tau$ has a natural left action on it:

$$^{\omega}f(z) = f(^{\omega^{-1}}z) = f(z-\omega), \forall f \in \mathcal{O}, z \in \mathbb{C}, \omega \in L_\tau.$$

As in Section 3.1, the groups $H^1(L_\tau, \mathcal{O}^\times)$ and $M_c$ are defined as follows.

A 1-cocycle is a map $c : L_\tau \to \mathcal{O}^\times$ such that

$$c_{\omega+\omega'} = c_\omega {}^{\omega} c_{\omega'}, \forall \omega, \omega' \in L_\tau.$$

We denote by $Z^1(L_\tau, \mathcal{O}^\times)$ the set of all 1-cocycles. Two cocycles $c, c'$ are called equivalent: $c \sim c'$ if there is an element $u \in \mathcal{O}^\times$ such that

$$c'_\omega = u^{-1 \omega} u c_\omega, \forall \omega \in L_\tau.$$

The cohomology set is, by definition,

$$H^1(L_\tau, \mathcal{O}^\times) = Z^1(L_\tau, \mathcal{O}^\times)/\sim .$$

We shall denote by $[c]$ the cohomology class containing a cocycle $c$. It is easy to see that $H^1(L_\tau, \mathcal{O}^\times)$ forms a group.

To each cocycle $c \in Z^1(L_\tau, \mathcal{O}^\times)$, we set

$$M_c = \{f \in \mathcal{O} : c_\omega {}^{\omega} f = f, \forall \omega \in L_\tau\}.$$

It is a $\mathbb{C}$-subspace in the $\mathbb{C}$-algebra of holomorphic functions $\mathcal{O}$.

## 6.2 Elements of $H^1(L_\tau, \mathcal{O}^\times)$

Now I am going to determine the structure of $H^1(L_\tau, \mathcal{O}^\times)$. I use a common result from [9] and [5] to reduce the problem to the normalizable cocycle case, and then use Fourier theory to deal with it. It turns out that every element in $H^1(L_\tau, \mathcal{O}^\times)$ can be written out explicitly.

Because of habit, I use $c$ to denote both cocycles and constants, but it is easy to distinguish them from the context, and there will be no confusion about it. And for simplicity, I use $\mathbf{e}(z)$ instead of $\exp(2\pi i z)$.

First let me introduce the definition of normalizable cocycles.

**Definition 6.2.1.** Call a cocycle $c$ normalizable, if there is some cocycle $c'$ with $c \sim c'$ and $c'_1 = 1$.

At first glance, it may seem that this kind of cocycles are very special. But we have the following powerful theorem.

**Theorem 6.2.1.** ([9],p.693; [5],p.218) For any holomorphic function $f \in \mathcal{O}(\mathbb{C})$, there is a $g \in \mathcal{O}(\mathbb{C})$, such that $f(z) = g(z+1) - g(z)$, $\forall z \in \mathbb{C}$.

It is easy to see that this theorem is only an additive version of what I need.

**Corollary 6.2.1.** For any $[c] \in H^1(L_\tau, \mathcal{O}^\times)$, $c$ is normalizable.

**Pf.** Take any $[c] \in H^1(L_\tau, \mathcal{O}^\times)$, $c_1 \in \mathcal{O}^\times$, so $c_1 = \mathbf{e}(f(z))$, for some $f(z) \in \mathcal{O}$. Then by Theorem 6.2.1, we know there is some $g_1 \in \mathcal{O}$, with $f(z) = g_1(z+1) - g_1(z)$. Put $g(z) = g_1(z+1) \in \mathcal{O}$, $u(z) = \mathbf{e}(g(z)) \in \mathcal{O}^\times$, then $f(z) = g(z) - g(z-1)$, $c_1 = u(z)/u(z-1)$. Let $c'_\omega = u(z)^{-1}u(z-\omega) \cdot c_\omega$, $\omega \in L_\tau$. Then $c \sim c'$, and $c'_1 = u(z)^{-1}u(z-1) \cdot c_1 = 1$, i.e., $c$ is normalizable. $\square$

We can now describe the elements in $H^1(L_\tau, \mathcal{O}^\times)$.

**Theorem 6.2.2.** Any cocycle is equivalent to a cocycle $c$ having the following form:

$$c_\omega = \mathbf{e}(na(z - \frac{n}{2}\tau) + nb) \tag{42}$$

where $\omega = m + n\tau \in L_\tau, m, n \in \mathbb{Z}, a = a(\tau) \in \mathbb{Z}, b = b(\tau) \in \mathbb{C}$. Conversely, for any $a = a(\tau) \in \mathbb{Z}, b = b(\tau) \in \mathbb{C}$, (42) gives a cocycle in $H^1(L_\tau, \mathcal{O}^\times)$. Any two cocycles $c, c'$ having the form (42) are equivalent if and only if $a = a'$, and $b - b' \in \mathbb{Z} + \mathbb{Z}\tau = L_\tau$, where $a', b'$ are the corresponding parameters to $c'$ as that of $a, b$ to $c$.

From this theorem, we see that all the cocycles are essentially given by Jacobi's theta function. And one may view them as generalized Jacobi's theta functions.

**Pf.** *Part I.* By Theorem 6.2.1, any cocycle $c$ is normalizable. Without loss of generality, we can assume that $c_1 = 1$. Suppose $c_\tau = \mathbf{e}(f(z))$, $f(z) \in \mathcal{O}$, then from $c_{1+\tau} = c_{\tau+1}$, we have ${c_1}^1 c_\tau = {c_\tau}^\tau c_1$, i.e. $\mathbf{e}(f(z-1)) = \mathbf{e}(f(z))$. So $f(z) - f(z-1) \in \mathbb{Z}$, $f'(z) = f'(z-1)$. Then $f'(z)$ admits a Fourier series which converges absolutely on the whole complex plane and uniformly on any compact subset of $\mathbb{C}$:

$$f'(z) = \sum_{r \in \mathbb{Z}} c'_r \mathbf{e}(rz)$$

Integrating both sides, we get

$$f(z) = \sum_{r \in \mathbb{Z}, r \neq 0} c''_r \mathbf{e}(rz) + az + b'$$

where $a = a(\tau), b' = b'(\tau), c''_r = c''_r(\tau) \in \mathbb{C}$. This series converges absolutely on the whole complex plane and uniformly on any compact subset of $\mathbb{C}$ too. Further we can get $a = f(z) - f(z-1) \in \mathbb{Z}$.

Now we have $c_\tau = \mathbf{e}(f(z)) = \prod_{r\in\mathbb{Z},r\neq 0} \mathbf{e}(c''_r\mathbf{e}(rz)) \cdot \mathbf{e}(az + b')$. From this we can get

$$c_{n\tau} = \prod_{r\in\mathbb{Z},r\neq 0} \mathbf{e}(c_r(1 - \mathbf{e}(-nr\tau))\mathbf{e}(rz)) \cdot \mathbf{e}(na(z - \frac{n}{2}\tau) + nb) \tag{43}$$

for all $n \in \mathbb{Z}$ and some $c_r = c_r(\tau), b = b(\tau) \in \mathbb{C}$, with $r \in \mathbb{Z}, r \neq 0$.

We prove it by induction.

First, we know $c_0 = c_{0+0} = c_0c_0$, so $c_0 = 1$, satisfying (43). $c_\tau = \prod_{r\in\mathbb{Z},r\neq 0} \mathbf{e}(c''_r\mathbf{e}(rz)) \cdot \mathbf{e}(az + b')$, satisfying (43) too while putting $c_r = c''_r/(1 - \mathbf{e}(-r\tau))$, $b = b' + a\tau/2$. For $c_{-\tau}$, we have $c_0 = c_{-\tau+\tau} = {c_{-\tau}}^{-\tau}c_\tau$, so $c_{-\tau} = ({}^{-\tau}c_\tau)^{-1} = \prod_{r\neq 0} \mathbf{e}(-c_r(1 - \mathbf{e}(-r\tau))\mathbf{e}(rz + r\tau)) \cdot \mathbf{e}(-az - a\tau/2 - b) = \prod_{r\neq 0} \mathbf{e}(c_r(1 - \mathbf{e}(r\tau))\mathbf{e}(rz)) \cdot \mathbf{e}(-a(z + \tau/2) - b)$, satisfying (43) too.

Assume (43) holds for $n = k, k \in \mathbb{Z}, k > 0$, then for $n = k+1$, we have $c_{(k+1)\tau} = {c_\tau}^\tau c_{k\tau} = \prod_{r\neq 0} \mathbf{e}(c_r(1-\mathbf{e}(-r\tau))\mathbf{e}(rz)) \cdot \mathbf{e}(a(z-\tau/2)+b) \cdot \prod_{r\neq 0} \mathbf{e}(c_r(1-\mathbf{e}(-kr\tau))\mathbf{e}(rz-r\tau)) \cdot \mathbf{e}(ka(z-\tau-k\tau/2)+kb) = \prod_{r\neq 0} \mathbf{e}(c_r(1-\mathbf{e}(-(k+1)r\tau))\mathbf{e}(rz)) \cdot \mathbf{e}((k+1)a(z-(k+1)\tau/2)+(k+1)b)$, satisfying (43).

Assume (43) holds for $n = -k, k \in \mathbb{Z}, k > 0$, then for $n = -k - 1$, we have $c_{-(k+1)\tau} = {c_{-\tau}}^{-\tau}c_{-k\tau} = \prod_{r\neq 0} \mathbf{e}(c_r(1 - \mathbf{e}(r\tau))\mathbf{e}(rz)) \cdot \mathbf{e}(-a(z + \tau/2) - b) \cdot \prod_{r\neq 0} \mathbf{e}(c_r(1 - \mathbf{e}(kr\tau))\mathbf{e}(rz + r\tau)) \cdot \mathbf{e}(-ka(z + \tau + k\tau/2) - kb) = \prod_{r\neq 0} \mathbf{e}(c_r(1 - \mathbf{e}((k + 1)r\tau))\mathbf{e}(rz)) \cdot \mathbf{e}(-(k + 1)a(z + (k + 1)\tau/2) - (k + 1)b)$, satisfying (43).

So by induction, (43) holds for all $n \in \mathbb{Z}$ and some $c_r, b \in \mathbb{C}$, with $r \in \mathbb{Z}, r \neq 0$.

Next we show $c_m = 1, \forall m \in \mathbb{Z}$. We know $c_0 = 1, c_1 = 1$. For $c_{-1}$, we have $c_0 = c_{-1+1} = {c_{-1}}^{-1}c_1 = c_{-1} = 1$, so $c_m = 1$, for $m = -1, 0, 1$. Assume $c_m = 1$ for $m = k, k \in \mathbb{Z}$, then $c_{k+1} = {c_1}^1c_k = c_k = 1$, $c_{k-1} = {c_{-1}}^{-1}c_k = 1$. So $c_m = 1, \forall m \in \mathbb{Z}$.

Thus, from $c_{m+n\tau} = {c_{n\tau}}^{n\tau}c_m = c_{n\tau}$, we get

$$c_\omega = \prod_{r\in\mathbb{Z},r\neq 0} \mathbf{e}(c_r(1 - \mathbf{e}(-nr\tau))\mathbf{e}(rz)) \cdot \mathbf{e}(na(z - \frac{n}{2}\tau) + nb) \tag{44}$$

for all $\omega = m + n\tau \in L_\tau, m, n \in \mathbb{Z}$.

Let $u(z) = \prod_{r\in\mathbb{Z},r\neq 0} \mathbf{e}(c_r\mathbf{e}(rz))$. It converges absolutely because so does the infinite product in (44) for any $n \in \mathbb{Z}$. Now putting $c'_\omega = u^{-1\omega}uc_\omega$, we have $c \sim c'$, and $c'$ is of the form (42).

*Part II.* For any $a = a(\tau) \in \mathbb{Z}, b = b(\tau) \in \mathbb{C}$, we need show that (42) gives a cocycle in $H^1(L_\tau, \mathcal{O}^\times)$. Take any $\omega' = m' + n'\tau, \omega'' = m'' + n''\tau \in L_\tau$, let $\omega = \omega' + \omega'' = m + n\tau \in L_\tau$, then $m = m' + m'', n = n' + n''$. And we have $c_{\omega'}{}^{\omega'} c_{\omega''} = \mathbf{e}(n'a(z - n'\tau/2) + n'b)\mathbf{e}(n''a(z - m' - n'\tau - n''\tau/2) + n''b) = \mathbf{e}((n' + n'')a(z - (n' + n'')\tau/2) + (n' + n'')b) = \mathbf{e}(na(z - n\tau/2) + nb) = c_\omega = c_{\omega' + \omega''}$. So (42) gives a cocycle in $H^1(L_\tau, \mathcal{O}^\times)$.

For any two cocycles $c, c'$ of the form (42), we have

$$c_\omega = \mathbf{e}(na(z - \frac{n}{2}\tau) + nb)$$

$$c'_\omega = \mathbf{e}(na'(z - \frac{n}{2}\tau) + nb')$$

for some $a, a' \in \mathbb{Z}$, $b, b' \in \mathbb{C}$, where $\omega = m + n\tau \in L_\tau, m, n \in \mathbb{Z}$.

If $a = a', b - b' \in \mathbb{Z} + \mathbb{Z}\tau = L_\tau$, then let $b - b' = d' + d\tau$, with $d, d' \in \mathbb{Z}$, and let $u(z) = \mathbf{e}(-dz)$. Then we have $u^{-1\omega} u c'_\omega = \mathbf{e}(dz - d(z - m - n\tau) + na(z - n\tau/2) + nb') = \mathbf{e}(na(z - n\tau/2) + nb' + nd\tau) = \mathbf{e}(na(z - n\tau/2) + nb' + nd' + nd\tau) = \mathbf{e}(na(z - n\tau/2) + nb) = c_\omega$, thus $c \sim c'$.

If $c \sim c'$, then there exists a $v(z) \in \mathcal{O}^\times$, such that $c_\omega = c'_\omega v^{-1\omega} v$. Now for $v(z) \in \mathcal{O}^\times$, there is a holomorphic function $u(z) \in \mathcal{O}$, such that $v(z) = \mathbf{e}(u(z))$. So we have

$$\mathbf{e}(na(z - \frac{n}{2}\tau) + nb) = \mathbf{e}(na'(z - \frac{n}{2}\tau) + nb' - u(z) + u(z - \omega))$$

and then

$$na(z - \frac{n}{2}\tau) + nb - na'(z - \frac{n}{2}\tau) - nb' + u(z) - u(z - \omega) \in \mathbb{Z} \tag{45}$$

Differentiating this element, we get

$$n(a - a') + u'(z) - u'(z - \omega) = 0 \tag{46}$$

Differentiate it once again, we get

$$u''(z) = u''(z - \omega)$$

Thus $u''(z)$ is a holomorphic function on the elliptic curve $E_\tau = \mathbb{C}/L_\tau$, hence a constant function. After integration, we find that $u(z)$ is a polynomial in $z$ of degree at most 2. So assume $u(z) = c_1 z^2 + c_2 z + c_3$. Then $u'(z) = 2c_1 z + c_2$.

Plug it in (46), we get

$$u'(z) - u'(z - \omega) = 2c_1\omega = -n(a - a') \in \mathbb{Z}, \forall \omega \in L_\tau$$

Let $\omega = 1$, we can get $c_1 = 0$, and hence $a = a'$.

Use these results in (45), we get

$$n(b - b') + c_2\omega \in \mathbb{Z}, \forall \omega \in L_\tau$$

Let $\omega = 1$, we get $c_2 \in \mathbb{Z}$. Let $\omega = \tau$, then we get $b - b' \in \mathbb{Z} + \mathbb{Z}\tau = L_\tau$. $\square$

Define a mapping $\varphi : H^1(L_\tau, \mathcal{O}^\times) \longrightarrow \mathbb{Z} \times E_\tau$ as the following. For any $[c] \in H^1(L_\tau, \mathcal{O}^\times)$, we have $[c] = [c']$ for some $c'$ of the form (42). Suppose $c'_\omega = \mathbf{e}(na(z - n\tau/2) + nb)$, with $a \in \mathbb{Z}, b \in \mathbb{C}$. Let $\varphi([c])$ in $\mathbb{Z} \times E_\tau$ be $(a, \bar{b})$, where $\bar{b}$ is the image of $b$ under the quotient map $\mathbb{C} \to \mathbb{C}/L_\tau$. From Theorem 6.2.2, we know that $\varphi$ is well-defined and bijective. And it can also be shown that it is a group isomorphism. Thus we reobtain the well-known group structure of $H^1(L_\tau, \mathcal{O}^\times)$.

The reason that we want to get the description of all the elements of $H^1(L_\tau, \mathcal{O}^\times)$ in spite of that its structure is already known is to describe $M_c$ in this case.

## 6.3 Description of $M_c$

**Theorem 6.3.1.** For any cocycle $c$ of the form (42), with $a \in \mathbb{Z}, b \in \mathbb{C}$, we have the following:

1. If $a \neq 0$, then $\dim M_c = |a|$, and the basis can be given by $\sum_{k\in\mathbb{Z}} c_{k\tau}\mathbf{e}(r(z - k\tau)), r = 0, \ldots, |a| - 1$;
2. If $a = 0$ and $b \notin L_\tau$, then $M_c = 0$;
3. If $a = 0$ and $b \in L_\tau$, then $\dim M_c = 1$, and the basis can be given by $\mathbf{e}(rz)$, where $b = r' + r\tau \in L_\tau, r, r' \in \mathbb{Z}$.

**Pf.** For any cocycle $c$ of the form (42), with $a \in \mathbb{Z}, b \in \mathbb{C}$, let $f \in M_c$, then we have

$$c_\omega{}^\omega f = f, \forall \omega \in L_\tau \tag{47}$$

Let $\omega = 1$, we have $f(z - 1) = f(z)$, so $f(z)$ admits a Fourier expansion $f(z) = \sum_{r\in\mathbb{Z}} c_r\mathbf{e}(rz)$. Plug it in (47), and let $\omega = \tau$, we get

$$\mathbf{e}(a(z - \tau/2) + b)\sum_{r\in\mathbb{Z}} c_r\mathbf{e}(rz - r\tau) = \sum_{r\in\mathbb{Z}} c_r\mathbf{e}(rz)$$

Thus

$$\sum_{r\in\mathbb{Z}} c_r\mathbf{e}((r + a)z - a\tau/2 + b - r\tau) = \sum_{r\in\mathbb{Z}} c_r\mathbf{e}(rz)$$

$$\sum_{r\in\mathbb{Z}} c_{r-a}\mathbf{e}(rz - a\tau/2 + b - (r-a)\tau) = \sum_{r\in\mathbb{Z}} c_r\mathbf{e}(rz)$$

$$\sum_{r\in\mathbb{Z}} c_{r-a}\mathbf{e}(-(r-a/2)\tau + b)\mathbf{e}(rz) = \sum_{r\in\mathbb{Z}} c_r\mathbf{e}(rz)$$

So we get

$$c_r = c_{r-a}\mathbf{e}(-(r-a/2)\tau + b)$$

$$c_{r+a} = c_r\mathbf{e}(-(r+a/2)\tau + b) \tag{48}$$

$$c_{r-a} = c_r\mathbf{e}((r-a/2)\tau - b) \tag{49}$$

If $a = 0$, then (48) becomes

$$c_r = c_r\mathbf{e}(-r\tau + b)$$

then we have $c_r = 0$, or $\mathbf{e}(-r\tau + b) = 1$, $-r\tau + b \in \mathbb{Z}$, $b \in \mathbb{Z} + r\tau$. If $b \notin \mathbb{Z} + \mathbb{Z}\tau$, from here we know $M_c = 0$. If $b \in \mathbb{Z} + \mathbb{Z}\tau$, say, $b = d' + d\tau$, $d, d' \in \mathbb{Z}$, then $c_r = 0$ for $r \neq d$, $f(z) = c_d\mathbf{e}(dz)$. And it is easy to check $f(z) = c_d\mathbf{e}(dz) \in M_c$, so $\dim M_c = 1$, and the basis can be given by $\mathbf{e}(dz)$.

If $a \neq 0$, then we have

$$c_{r+ka} = c_r\mathbf{e}(-(kr + k^2a/2)\tau + kb), \forall k \in \mathbb{Z} \tag{50}$$

From (48) and (49), it is easy to see that (50) holds for $k = -1, 0, 1$. Assume (50) holds for $k = k_0$, then by (48), we have

$$\begin{aligned} c_{r+(k_0+1)a} &= c_{r+k_0a+a} = c_{r+k_0a}\mathbf{e}(-(r + k_0a + a/2)\tau + b) \\ &= c_r\mathbf{e}(-(k_0r + k_0^2a/2)\tau + k_0b - (r + k_0a + a/2)\tau + b) \\ &= c_r\mathbf{e}(-((k_0+1)r + (k_0+1)^2a/2)\tau + (k_0+1)b) \end{aligned}$$

And by (49), we have

$$\begin{aligned} c_{r+(k_0-1)a} &= c_{r+k_0a-a} = c_{r+k_0a}\mathbf{e}((r + k_0a - a/2)\tau - b) \\ &= c_r\mathbf{e}(-(k_0r + k_0^2a/2)\tau + k_0b + (r + k_0a - a/2)\tau - b) \\ &= c_r\mathbf{e}(-((k_0-1)r + (k_0-1)^2a/2)\tau + (k_0-1)b) \end{aligned}$$

So (50) holds for $k = k_0 + 1, k_0 - 1$. Hence (50) holds for any $k \in \mathbb{Z}$.

Thus, $f(z)$ can be expressed as

$$\begin{aligned} f(z) &= \sum_{r\in\mathbb{Z}} c_r \mathbf{e}(rz) = \sum_{r=0}^{|a|-1}\sum_{k\in\mathbb{Z}} c_{r+ka}\mathbf{e}((r+ka)z) \\ &= \sum_{r=0}^{|a|-1}\sum_{k\in\mathbb{Z}} c_r \mathbf{e}(-(kr+k^2a/2)\tau + kb)\mathbf{e}((r+ka)z) \\ &= \sum_{r=0}^{|a|-1} c_r \sum_{k\in\mathbb{Z}} \mathbf{e}(ka(z-k\tau/2)+kb)\mathbf{e}(r(z-k\tau)) \\ &= \sum_{r=0}^{|a|-1} c_r \sum_{k\in\mathbb{Z}} c_{k\tau}\mathbf{e}(r(z-k\tau)) \end{aligned} \tag{51}$$

Let $f_r(z) = \sum_{k\in\mathbb{Z}} c_{k\tau}\mathbf{e}(r(z-k\tau)), r = 0,\ldots,|a|-1$, which converge absolutely because so does $\sum_{r\in\mathbb{Z}} c_r\mathbf{e}(rz)$. They are linearly independent, because if $\sum_{r=0}^{|a|-1} c'_r f_r(z) = 0$, then from (51), we get that $\sum_{r\in\mathbb{Z}} c'_r\mathbf{e}(rz)$ is the Fourier expansion of the zero function after defining $c'_r$ for other $r\in\mathbb{Z}$ by (50), thus giving $c'_r = 0, \forall r = 0,\ldots,|a|-1$. And $f_r(z), r = 0,\ldots,|a|-1$ are in $M_c$, which can be verified easily. Then from the results above, we know that $\dim M_c = |a|$, and the basis can be given by $f_r, r = 0,\ldots,|a|-1$. $\square$

From Theorem 6.2.2 and Theorem 6.3.1, our space $M_c$ are determined completely for any cocycle $c$ up to isomorphism.

Notice that $L_\tau = \mathbb{Z}+\mathbb{Z}\tau$, and in the first case of the above theorem, any element in $M_c$ is of the form (51), which is built from $\sum_{r=0}^{|a|-1} c_r\mathbf{e}(rz)$ by Poincaré sum procedure for $\mathbb{Z}\tau$, where $\sum_{r=0}^{|a|-1} c_r\mathbf{e}(rz)$ is invariant under the action of $\mathbb{Z}$. Also notice that an element of the form (51) is not a Poincaré sum over $L_\tau$ for some element in $\mathcal{O}$. This kind of new phenomenon would not occur if $L_\tau$ were finite.

## 6.4 Countable Group Case

From the results above for the elliptic curve case and those for the modular form case in Section 3.2, we get some feeling on what is going on in the countable group $\mathcal{G}$ case for a triple system $(\mathcal{G},(G,M))$. Now let us try to formulate it.

Let $\mathcal{G}$ be a countable topological group endowed with discrete topology, $G$ a topological group and $M$ an abelian topological group. Let $\mathcal{G}$ and $G$ act continuously on the group $M$. As before, we also assume that $M$ is a left $G$-module and $\mathcal{G}$ acts naturally on $(G,M)$.

If $H$ is a subgroup of $\mathcal{G}$, denote the set of representatives of left cosets of $H$ in $\mathcal{G}$ as

$\mathcal{G}/H$, and the subgroup of $M$ of all those fixed by elements in $H$ as $M^H$.

Given a subset $S \subseteq \mathcal{G}$ and the elements $a_t \in M, t \in S$, if for any subset $SS \subseteq S$ and any increasing sequence of finite subsets of $SS$, $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq \cdots \subseteq SS \subseteq S$ with $\bigcup_{n=1}^{\infty} S_n = SS$, the limit $\lim_{n\to\infty} \sum_{t\in S_n} a_t$ exists and doesn't depend on the choice of the increasing sequence of finite subsets of $SS$, then we call the series $\sum_{t\in S} a_t$ converges absolutely in $M$, and the value of $\sum_{t\in S} a_t$ is defined to be the limit when $SS = S$. It is easy to check that the partial series of an absolutely convergent series is also absolutely convergent, and the sum of two absolutely convergent series $\sum_{t\in S} a_t$, $\sum_{t\in S} b_t$ is also absolutely convergent, and their sum is $\sum_{t\in S}(a_t + b_t)$.

Now we turn to define the cohomology group $H^1(\mathcal{G}, G)$.

Similarly as before, a 1-cocycle is a map $c : \mathcal{G} \to G$ such that

$$c_{st} = c_s{}^s c_t, \forall s, t \in \mathcal{G}.$$

We denote by $Z^1(\mathcal{G}, G)$ the set of all 1-cocycles. Two cocycles $c, c'$ are called equivalent: $c \sim c'$ if there is an element $u \in G$ such that

$$c'_s = u^{-1} c_s{}^s u, \forall s \in \mathcal{G}.$$

The cohomology set is defined as

$$H^1(\mathcal{G}, G) = Z^1(\mathcal{G}, G)/\sim .$$

We shall denote by $[c]$ the cohomology class containing the cocycle $c$.

To each cocycle $c \in Z^1(\mathcal{G}, G)$, we set

$$M_c = \{a \in M : c_s{}^s a = a, \forall s \in \mathcal{G}\}.$$

However, from our results in both elliptic curve case and modular form case, we don't define $P_c$ as $\{a \in M : a = \sum_{s\in\mathcal{G}} c_s{}^s x$, for some $x \in M$, and it converges absolutely$\}$, but as $P_c = \{a \in M : a = p_{c,H}(x) = \sum_{s\in\mathcal{G}/H} c_s{}^s x$, for some subgroup $H \subseteq \ker(c) \subseteq \mathcal{G}$, some $x \in M^H$, and it converges absolutely$\}$. Denote $p_{c,H}(x)$ by $p_c(x)$ if $H = \ker(c)$.

It is easy to see that $M_c$ is a subgroup of $M$ and $P_c \subseteq M_c$ for every cocycle $c$. Moreover, we have a better description of $P_c$, which implies that $P_c$ is also a subgroup of $M$.

**Proposition 6.4.1.** Let $K = \ker(c)$ for a cocycle $c \in Z^1(\mathcal{G}, G)$, then $K$ is a subgroup of $\mathcal{G}$, and $P_c = \{a \in M : a = p_c(x) = \sum_{s\in\mathcal{G}/K} c_s{}^s x$, for some $x \in M^K$, and it converges

absolutely}. So $P_c$ is a subgroup of $M_c$, and $M_c$, $P_c$, $M_c/P_c$ are uniquely determined by the cocycle class $[c] \in H^1(\mathcal{G}, G)$ up to isomorphism.

**Pf.** It is obvious that $K$ is a subgroup of $\mathcal{G}$. Let $Q_c = \{a \in M : a = p_c(x) = \sum_{s\in\mathcal{G}/K} {c_s}^s x$, for some $x \in M^K$, and it converges absolutely$\}$. We are going to show that $P_c = Q_c$.

First, $Q_c \subseteq P_c$, which is evident. Then we look at the other side. $\forall a \in P_c$, there is some subgroup $H$, such that $a = p_{c,H}(x)$ for some element $x \in M^H$. From group theory, we know there is a bijection $\mathcal{G}/K \times K/H \to \mathcal{G}/H$ given by $(t, g) \mapsto tg$ if we choose $\mathcal{G}/H$ properly. Hence $a$ can be written as $a = \sum_{tg\in\mathcal{G}/H} {c_{tg}}^{tg} x$, where $t \in \mathcal{G}/K$, $g \in K/H$. But because of $\ker(c) = K$, we have $c_{tg} = {c_t}^t c_g = c_t$. Also note that $a = \sum_{tg\in\mathcal{G}/H} {c_{tg}}^{tg} x$ converges absolutely, so its partial series $\sum_{g\in K/H} {c_g}^g x = \sum_{g\in K/H} {}^g x$ converges absolutely too. We denote its value by $y$, and it is easy to see that $y \in M^K$. Now we have

$$\begin{aligned} a &= \sum_{tg\in\mathcal{G}/H} {c_{tg}}^{tg} x = \sum_{t\in\mathcal{G}/K} \sum_{g\in K/H} {c_{tg}}^{tg} x \\ &= \sum_{t\in\mathcal{G}/K} \sum_{g\in K/H} {c_t}^t({}^g x) = \sum_{t\in\mathcal{G}/K} {c_t}^t\Big(\sum_{g\in K/H} {}^g x\Big) \\ &= \sum_{t\in\mathcal{G}/K} {c_t}^t y \in Q_c \end{aligned}$$

So the proposition is proved. □

Equipped with the new terminology, we can have the following corollary from Theorem 6.3.1:

**Corollary 6.4.1.** For any cocycle $[c] \in H^1(L_\tau, \mathcal{O}^\times)$, we have $M_c/P_c = 1$.

**Pf.** It is obvious for the first and the second cases in Theorem 6.3.1. For the third case, we can let $b = 0$, because its corresponding cocycle is equivalent to that when $b$ is any element in $L_\tau$, and $M_c/P_c$ is the same up to isomorphism. Now it is easy to get the result. □

# References


[1] M. Bhargava, *Higher composition laws and applications*, Proceedings of the International Congress of Mathematicians, Madrid, Spain, 2006.

[2] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer-Verlag, New York (1978).

[3] D. A. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley, New York (1989).

[4] P. G. L. Dirichlet, *Vorlesungen über zahlentheorie*, 2nd ed., Braunschweig, 1871.

[5] O. Forster, *Lectures on Riemann surfaces*. Springer-Verlag New York Inc. (1981).

[6] C. F. Gauss, *Disquisitiones arithmeticae*, 1801, Werke, Bd. I. (English translation: Yale University Press, 1966).

[7] R. C. Gunning, *Lectures on modular forms*, Princeton University Press, Princeton, New Jersey (1962).

[8] D. Hilbert, *The theory of algebraic number fields ("Zahlbericht")*, transl. by I. Adamson, with an introduction by F. Lemmermeyer and N. Schappacher. Springer-Verlag, Berlin etc. 1998.

[9] A. Hurwitz and R. Courant, *Funktionentheorie*, 4. Auflage, Springer-Verlag (1964).

[10] S. Kühnlein, *Cohomology sets inside arithmetic groups*, Acta Arith. 107.1 (2003), 27-33.

[11] S. Lang, *Algebra*, Third Edition, Addison-Wesley, Massachusetts etc. 1993.

[12] C. G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math., vol.34 (1933), 313-316.

[13] S. M. Lee, and T. Ono, *On a certain invariant for real quadratic fields*. Proc. Japan Acad., **79A**, 119-122 (2003).

[14] J. Neukirch, *Algebraic number theory*, transl. by N. Schappacher. Springer-Verlag, Berlin Heidelberg New York, 1999.

[15] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*. Springer-Verlag, Berlin Heidelberg New York, 2000.

[16] T. Ono, *Arithmetic of algebraic groups and its applications*, St. Paul's International Exchange Series, Occasional Papers VI, St. Paul's University, 1986.

[17] T. Ono, *On certain cohomology sets attached to Riemann surfaces*. Proc. Japan Acad., **76A**, 116-117 (2000).

[18] T. Ono, *On certain cohomology set for* $\Gamma_0(N)$. Proc. Japan Acad., **77A**, 39-41 (2001).

[19] T. Ono, *On certain cohomology set for* $\Gamma_0(N)$. *II*. Proc. Japan Acad., **77A**, 108-110 (2001).

[20] T. Ono, *On certain exact sequences for* $\Gamma_0(m)$. Proc. Japan Acad., **78A**, 83-86 (2002).

[21] T. Ono, *A note on Poincaré sums for finite groups*. Proc. Japan Acad., **79A**, 95-97 (2003).

[22] T. Ono, *On Poincaré sums for local fields*. Proc. Japan Acad., **79A**, 115-118 (2003).

[23] T. Ono, *On Poincaré sums for number fields*. Proc. Japan Acad., **81A**, 65-68 (2005).

[24] T. Ono, *Gauss sums and Poincaré sums (a sketch)*. KIAS International Conference, 2006.

[25] I. Reiner, *Maximal orders*, Academic Press, London New York, 1975.

[26] J. P. Serre, *Local fields*. Springer-Verlag, New York, 1979.

[27] J. P. Serre, *Galois cohomology*. Springer-Verlag, Berlin Heidelberg New York, 1997.

[28] I. R. Shafarevich, *Basic algebraic geometry*, Springer-Verlag, Berlin, New York (1974).

[29] O. Taussky, *On a theorem of Latimer and MacDuffee*, Canadian J. Math. **1** (1949), 300-302.

[30] J. H. M. Wedderburn, *Lectures on matrices*, Amer. Math. Soc. Colloquium Publications, vol.17 (1934), 27.

# VITA

SHUAI WANG

Shuai Wang was born in December, 1976 in Jiangxi Province in China. He received his Bachelor of Science degree in Mathematics from Beijing Normal University in Beijing, China in 1998, and Master of Science degree in Mathematics from Beijing Normal University in 2001.

He enrolled in the graduate program at the Johns Hopkins University in 2001. His dissertation was completed under the direction of Professor Takashi Ono.