uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES
ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND
POSDOCTORAL STUDIES

Abdelkrim El Basraoui
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.Sc. (Mathematics)
GRADE / DEGREE

Department of Mathematics and Statistics
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Modular Functions and Replicable Functions

TITRE DE LA THÈSE / TITLE OF THESIS

Abdellah Sebbar
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Daniel Daigle

Damien Roy

Kenneth Williams

Gary W. Slater
LE DOYEN DE LA FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES /
DEAN OF THE FACULTY OF GRADUATE AND POSTDOCORAL STUDIES

MODULAR FUNCTIONS AND REPLICABLE FUNCTIONS

By
Abdelkrim EL BASRAOUI
August 2005

A Thesis
submitted to the School of Graduate Studies and Research
in partial fulfillment of the requirements
for the degree of
Master of Science in Mathematics[1]

[1]The M.Sc. Program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics.

Your file Votre référence
ISBN: 978-0-494-16975-9
Our file Notre référence
ISBN: 978-0-494-16975-9

Contents

ACKNOWLEDGMENTS

I would like to thank warmly my supervisor Prof. Abdellah Sebbar for the many precious things he did for me, for introducing me to this subject, for the valuable suggestions he provided while reviewing this thesis, and for supporting me financially. I also thank the Department of Mathematics and Statistics for the financial support. A special thank go to my parents and family for their moral and financial support. My thanks also go to my colleagues and friends.

To my Parents

INTRODUCTION

The theory of modular functions plays a central role in mathematics and particulary in number theory. These functions are defined on the complex upper half-plane $\mathbb{H} := \{z \in \mathbb{C} |\ \Im m(z) > 0\}$ and are invariant under some subgroups of the group $\mathrm{SL}_2(\mathbb{R})$ consisting of the two by two matrices with real entries and determinant 1. The most interesting subgroups of $\mathrm{PSL}_2(\mathbb{R})$ are those commensurable with the modular group $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$. They give rise to various modular functions that are connected with several fields of mathematics. One particular modular function, the elliptic modular j-function, which was discovered by Dedekind in 1877, has a Fourier expansion

$$j(z) = \frac{1}{q} + 196884q + 21493760q^2 + \cdots, \qquad q = \exp(2\pi i z),\ z \in \mathbb{H}.$$

It generates the field of modular functions for $\mathrm{PSL}_2(\mathbb{Z})$; in other words it is a Hauptmodul for the modular group $\mathrm{PSL}_2(\mathbb{Z})$, and it also characterizes isomorphism classes of elliptic curves over $\mathbb{C}$ and has other important aspects. However, one of the most intriguing aspect is the connection with the so-called Moonshine theory. Indeed, when the Monster simple group $\mathbb{M}$ was discovered over three decades ago, it has been noted that its first non-trivial irreducible representation has dimension 196883, and this lead John McKay to formulate his famous equation

$$196884 = 196883 + 1$$

suggesting that there is a certain connection between the Monster group $\mathbb{M}$ and the j-function. Later, John Thompson provided similar equations linking coefficients of

j with dimensions of representations of $\mathbb{M}$ from the character table of the Monster, which were then used by Conway and Norton to formulate the theory of Moonshine in their remarkable paper "Monstrous Moonshine" [6]. In particular the Moonshine conjecture states that there is a relationship between finite simple groups and modular functions.

The Moonshine Conjecture:

To each conjugacy class of cyclic subgroups $< g >$ of the Monster $\mathbb{M}$, there corresponds a series

$$f_g(q) = \frac{1}{q} + \sum_{n=1}^{\infty} a_n(g) q^n$$

such that:

1. *For all $n \geq 1$, $g \mapsto a_n(g)$ is a character of the Monster group.*
2. *As a function of z, $z \in \mathbb{H}$, where $q = \exp(2\pi i z)$, $f_g(z)$ is modular function for some genus zero subgroup G of $PSL_2(\mathbb{R})$ containing a $\Gamma_0(N)$, for some N, with finite index, and the transformations $z \mapsto z + k$ if and only if $k \in \mathbb{Z}$.*

This conjecture has now been proved by Borcherds [3]. In their paper, Conway and Norton also conjectured that, for an element $g \in \mathbb{M}$, the functions f_{g^n} associated to powers of g are connected in the following way:

$$\sum_{\substack{ad=n \\ 0 \leq b < d}} f_{g^a}\left(\frac{az+b}{d}\right) = F_n\left(f_g(z)\right) \quad (*)$$

where F_n is a specific polynomial defined from f_g. In fact, F_n is the unique polynomial such that $F_n\left(f_g(z)\right) - 1/q^n$ has no fractional terms in q. In particular, if $g = e$, $f_g = j$ then

$$\sum_{\substack{ad=n \\ 0 \leq b < d}} j\left(\frac{az+b}{d}\right) = F_n\left(j(z)\right)$$

characterizes the action of the Hecke operator on the j-function. One can extend the formula $(*)$ to a more formal setting, namely, let

$$f(z) = \frac{1}{q} + \sum_{k=1}^{\infty} a_k q^k \ , \quad q = \exp(2\pi i z), \ a_k \in \mathbb{C}. \qquad (**)$$

We say that f is replicable if for each $a \geq 1$, there are functions $f^{(a)}$ also of the form $(**)$, such that, for each $n \geq 1$

$$\sum_{\substack{ad=n \\ 0 \leq b < d}} f^{(a)}\left(\frac{az+b}{d}\right) = F_n\left(f(z)\right).$$

In particular, using $(*)$ we see that the Moonshine functions f_g, $g \in \mathbb{M}$, are replicable. In [20], Norton made the following conjecture:

Conjecture:

A function of the form $(**)$, with $a_k \in \mathbb{Q}$ is replicable if and only if either $f(z) = 1/q + cq$, or it is the Hauptmodul for a certain congruence group .

In [10], Cummins and Norton proved a part of this conjecture, namely that rational Haupmoduls are replicable. The converse is not proved yet. The work by Martin [14] establishing the Modularity of a subclass of replicable functions was widely known since 1994 as the only verified case of the converse. However, my advisor and I have discovered a flaw in the proof that renders his argument invalid.

The thesis is organized as follows:

In chapter 1, we introduce the Möbius group $\mathrm{PSL}_2(\mathbb{Z})$ and its discrete subgroups. We characterize in more details the congruence subgroups in algebraic and geometric terms.

In chapter 2 we introduce the notion of modular functions and provide several examples. We end the chapter with an emphasis on the field of modular functions for certain congruence subgroups.

In chapter 3, we introduce the notion of replicable functions and its origin from finite group theory and Moonshine theory. We then provide the replication of certain classical modular functions using direct methods

In the last chapter, we review in details the proof by Cummins and Norton of the replicability of the rational Haupmoduls.

Chapter 1

DISCRETE SUBGROUPS OF $\mathbf{PSL}_2(\mathbb{R})$

In this chapter, we introduce the discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$ acting on the complex upper half-plane $\mathbb{H} := \{z \in \mathbb{C} |\ \Im m(z) > 0\}$, and study some properties of the quotient spaces obtained by identifying equivalent points in $\mathbb{H}$ under the action of these groups. We will also study a particular class of discrete subgroups, namely the class of congruence groups.

1.1 MOBIUS TRANSFORMATIONS

The group $\mathrm{SL}_2(\mathbb{R})$, consisting of 2×2 matrices of determinant 1 with real entries, acts on the complex upper half plane $\mathbb{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

In fact this is an action of $\mathrm{PSL}_2(\mathbb{R}) := \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ which extends to $\mathbb{H} \cup \mathbb{R} \cup \{\infty\}$. By the point at infinity in the above union, we mean the point $i\infty$.

The elements of $\mathrm{SL}_2(\mathbb{R})$ are classified according to their traces. Let $\alpha \in \mathrm{SL}_2(\mathbb{R}) \setminus \{\pm I\}$, we have the following cases

- $Tr(\alpha) = \pm 2 \Leftrightarrow \alpha$ fixes one point on $\mathbb{R} \cup \{\infty\}$, and α is called parabolic and the fixed point is called a cusp.
- $|Tr(\alpha)| > 2 \Leftrightarrow \alpha$ fixes two points on $\mathbb{R} \cup \{\infty\}$, and α is called hyberbolic.
- $|Tr(\alpha)| < 2 \Leftrightarrow \alpha$ fixes one point on $\mathbb{H}$, and α is called elliptic while the fixed point is called an elliptic point.

The action of $\mathrm{SL}_2(\mathbb{R})$ is transitive on $\mathbb{H}$, since, for $a > 0,\ b \in \mathbb{R}$

$$\begin{pmatrix} a^{1/2} & a^{-1/2}b \\ 0 & a^{-1/2} \end{pmatrix} .i = ai + b.$$

Furthermore, we have

Theorem 1.1.1 ([19]). *The automorphism group of* $\mathbb{H}$ *is* $Aut(\mathbb{H}) = PSL_2(\mathbb{R})$.

We are interested in the quotients $G \setminus \mathbb{H}^*$, where G is a subgroup of $\mathrm{PSL}_2(\mathbb{R})$ and $\mathbb{H}^*$ is the union of $\mathbb{H}$ and the set of cusps of G, obtained by identifying G-equivalent points in $\mathbb{H}^*$ with the induced topology.

1.2 DISCRETE SUBGROUPS OF $\mathrm{PSL}_2(\mathbb{R})$

Definition 1.2.1. Let G be a subgroup of $\mathrm{PSL}_2(\mathbb{R})$. Then G is called a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ if the induced topology on G is discrete.

Example 1.2.1. One of the most important and intensively studied discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is the modular group

$$\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$$

where $\mathrm{SL}_2(\mathbb{Z})$ is the group of 2×2 matrices of determinant 1 with entries in $\mathbb{Z}$. The set of cusps of $\mathrm{PSL}_2(\mathbb{Z})$ is $\mathbb{Q} \cup \{\infty\}$. To see this, first note that ∞ is fixed by the parabolic transformation $T : z \mapsto z + 1$ of $\mathrm{PSL}_2(\mathbb{Z})$, so ∞ is a cusp. Now,

let s be a cusp of $\mathrm{PSL}_2(\mathbb{Z})$, $s \neq \infty$, and let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ be the parabolic element that fixes s so that $(as+b)/(cs+d) = s \in \mathbb{Q}$, and so $s = (a-d)/2c$. Conversely, if $s \in \mathbb{Q}$, write $s = p/q$, with $(p,q) = 1$, so that there exists $r, t \in \mathbb{Z}$ such that $\gamma = \begin{pmatrix} p & r \\ q & t \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma \cdot \infty = p/q$ which is also a cusp, since ∞ is. Therefore, the set of cusps of $\mathrm{PSL}_2(\mathbb{Z})$ is $\mathbb{Q} \cup \{\infty\}$, and all the cusps are equivalent under $\mathrm{PSL}_2(\mathbb{Z})$. Similarly, one can prove that the elliptic elements of $\mathrm{PSL}_2(\mathbb{Z})$ are either of order 2 or 3 and the set of elliptic points is represented by the two points i and $\rho = \exp(2\pi i/3)$, i.e. any elliptic point is $\mathrm{PSL}_2(\mathbb{Z})$-equivalent to one of these two points. The elliptic point i is fixed by the transformation $S : z \mapsto -1/z$ while ρ is fixed by ST. It is known that $\mathrm{PSL}_2(\mathbb{Z}) = \langle S, T \rangle$ and $\mathrm{PSL}_2(\mathbb{Z})$ is the free product $\langle S \rangle * \langle ST \rangle$.

We shall now give some properties that characterize discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$ and that generalize the case of $\mathrm{PSL}_2(\mathbb{Z})$.

Proposition 1.2.1 ([19], Proposition 2.5). *Let G be a discrete subgroup of a locally compact group F acting on a topological space S such that for any $s \in S$ the stabilizer $\{g \in G |\ g.s = s\}$ is compact. Then*

1. *For any $s \in S$, $\{g \in G |\ g.s = s\}$ is finite.*
2. *For any $s \in S$, there is a neighborhood U of s such that, if $g \in G$ and $U \cap gU \neq \emptyset$, then $g.s = s$.*
3. *For any two G-nonequivalent points $s, s' \in S$, there exist neighborhoods U of s and V of s' such that $gU \cap V = \emptyset$ for all $g \in G$.*

Corollary 1.2.2. *Let G be a discrete subgroup of $PSL_2(\mathbb{R})$. If $z \in \mathbb{H}$ is an elliptic point then $G_z = \{\gamma \in G |\ \gamma z = z\}$ is finite.*

Keeping the same notations and conditions as in the above corollary, we have

Proposition 1.2.3 ([28], Proposition 1.16). *G_z is a finite, cyclic group.*

Let us now fix a discrete subgroup G of $\mathrm{PSL}_2(\mathbb{R})$, and let us denote, as above, the union of $\mathbb{H}$ and the cusps of G by $\mathbb{H}^*$. Notice that $\mathbb{H}^*$ depends on G, and $\mathbb{H}^* = \mathbb{H}$ if G has no cusps.

For the purpose of characterizing the quotient $G \setminus \mathbb{H}^*$ we first define a topology on $\mathbb{H}^*$. For $z \in \mathbb{H}$, as a fundamental system of neighborhoods of z we take the usual one. If $c \neq \infty$ is a cusp, a fundamental system is given by

$$\{c\} \cup \{\text{the interior of the circle tangent to the real axis at c}\}.$$

For ∞ we take $\{\infty\} \cup \{z \in \mathbb{H} |\ \Im m(z) > k\}$ for all positive integers k.

Theorem 1.2.4 ([28], Theorem 1.28). *The quotient space $G\backslash\mathbb{H}^*$, with the quotient topology induced by $\mathbb{H}^*$, is Hausdorff.*

Proposition 1.2.5 ([28], Proposition 1.32). *If the quotient space $G \setminus \mathbb{H}^*$ is compact, then the number of inequivalent cusps (respectively elliptic points) is finite.*

It may happen that $G \setminus \mathbb{H}$ is compact, in this case G has no parabolic elements.

Example 1.2.2. If $G = \mathrm{PSL}_2(\mathbb{Z})$ then the quotient space $\mathrm{PSL}_2(\mathbb{Z}) \setminus \mathbb{H}^*$ is the sphere, so it is compact (see Example 1.2.3 below).

Now, with the above properties, we can define a structure of Riemann surface, i.e. a one dimensional connected complex analytic manifold, on the quotient $G \setminus \mathbb{H}^*$ as follows.
If z_0 is neither elliptic nor a cusp, then we can choose a neighborhood U of z_0 such that the projection map $p : \mathbb{H}^* \longrightarrow G \setminus \mathbb{H}^*$ induces a homeomorphism from U to $G \setminus U$. We take as a local coordinate $(p(U), p^{-1})$.

If z_0 is an elliptic, let $\overline{G}_{z_0} := G_{z_0}.\{\pm I\}/\{\pm I\}$ where $G_{z_0} = \{\gamma \in G |\ \gamma z_0 = z_0\}$. Let ψ be an isomorphism of $\mathbb{H}$ onto the unit disc such that $\psi(z_0) = 0$, for example $\psi : z \mapsto (z - z_0)/(z + z_0)$. If $\overline{G}_{z_0}$ has order n, then $\psi\overline{G}_{z_0}\psi^{-1}$ consists of transformations $x \mapsto \xi_n^k x$, $0 \leq k < n$, $\xi_n = \exp(2\pi i/n)$. Let U be a neighborhood z_0 such that $G_{z_0} = \{\gamma \in G |\ \gamma U \cap U \neq \emptyset\}$, define a map $\varphi : G_{z_0} \setminus U \longrightarrow \mathbb{C}$ by $\varphi(p(z)) = \psi(z)$, then φ is a homeomorphism onto an open subset of $\mathbb{C}$. As a local coordinate for z_0 we take $(G_{z_0} \setminus U, \varphi)$.

Finally, when z_0 is a cusp, let $\alpha \in \mathrm{SL}_2(\mathbb{R})$ such that $\alpha z_0 = \infty$. Then

$$\alpha G_{z_0} \alpha^{-1}.\{\pm I\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \mid m \in \mathbb{Z} \right\},$$

for some positive h. Then, we can define a homeomorphism φ of $G_{z_0} \setminus U$, where U is as in the elliptic case, into an open subset of $\mathbb{C}$ by $\varphi(p(z)) = \exp(2\pi i \alpha z/h)$. The local coordinate for z_0 is then given by $(G_{z_0} \setminus U, \varphi)$.

Thus, we have been able to define a structure of a Riemann surface on $G \setminus \mathbb{H}^*$.

Definition 1.2.2. If the Riemann surface $G \setminus \mathbb{H}^*$ is compact, then G is called a Fucshian group of the first kind. In this case, we define the genus of G to be the genus of the *compact* Riemann surface $G \setminus \mathbb{H}^*$.

Let $\Re, \Re'$ be two compact Riemann surfaces, and $f : \Re' \longrightarrow \Re$ a holomorphic mapping. Then f is either surjective or constant. Suppose that f is non-constant. Then $(\Re', f)$ is called a covering of $\Re$ and f is a covering map. Moreover, there exists an integer n called the degree of the covering $(\Re', f)$ of $\Re$, known to be $n = e_1 + \cdots + e_h$ for some h, where e_i is the ramification index of the covering $(\Re', f)$ at some point $z_0 \in \Re'$, i.e. the multiplicity of $f(z_0)$ in the fiber of f. It is known that the degree of the covering is independent of the choice of z_0, and that the number of points z_0 such that $e_{z_0} > 1$ is finite. Now, if g and g' are the genera of $\Re$ and $\Re'$ respectively, then they are connected by the following formula

$$2g' - 2 = n(2g - 2) + \sum_{z \in \Re'} (e_z - 1)$$

where e_z is the ramification index at z. This formula is known as the Riemann-Hurwitz formula.

For some subgroups F of $\mathrm{PSL}_2(\mathbb{R})$ it is sometimes easy to recognize the structure of $F \setminus \mathbb{H}^*$ by constructing what we call the fundamental region for F.

Definition 1.2.3. Let G be a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. A fundamental region for G is a connected subspace, say D_G, of $\mathbb{H}$ such that no two points in the interior of the closure of D_G are equivalent under a transformation of G and every point of $\mathbb{H}$ is equivalent to some point of D_G under G.

Example 1.2.3. When $G = \mathrm{PSL}_2(\mathbb{Z})$, the fundamental region D_1 for $\mathrm{PSL}_2(\mathbb{Z})$ is given be $D_1 = \{z \in \mathbb{H} |\ -1/2 \leq \Re e(z) \leq 0,\ |z| \geq 1\} \cup \{z \in \mathbb{H} |\ 0 < \Re e(z) < 1/2,\ |z| > 1\}$, see figure 1. If we identify the equivalent points in the closure $\overline{D}_1$ of D_1, we get a punctured sphere. Hence, as stated above, we recognize the structure of the quotient $\mathrm{PSL}_2(\mathbb{Z}) \setminus \mathbb{H}^*$ from the fundamental region D_1 of $\mathrm{PSL}_2(\mathbb{Z})$.

It can be shown that any discrete subgroup G of $\mathrm{PSL}_2(\mathbb{R})$ has a fundamental region, however, an explicit construction of a fundamental domain is not easy.

1.3 CONGRUENCE SUBGROUPS

Definition 1.3.1. Let H_1, H_2 be subgroups of a group F. Then H_1 and H_2 are said to be commensurable if $H_1 \cap H_2$ is of finite index in both H_1 and H_2.

Note that the notion of commensurability is an equivalence relation. This notion allows us to deduce some common properties between the concerned groups.

Proposition 1.3.1 ([28], Proposition 1.11,(2)). *Let H_1, H_2 be commensurable subgroups of a topological group F. If H_1 is discrete, then H_2 is discrete.*

Proposition 1.3.2 ([28], Proposition 1.30). *Let G_1, G_2 be commensurable subgroups of $PSL_2(\mathbb{R})$. Then G_1 and G_2 have the same set of cusps.*

Proposition 1.3.3 ([28], Proposition 1.31, 1.32). *Let G_1, G_2 be as in the above proposition. Then $G_1 \setminus \mathbb{H}^*$ is compact if and only if $G_2 \setminus \mathbb{H}^*$ is compact. If $G_1 \setminus \mathbb{H}^*$ is compact then the set of G_1-inequivalent cusps (resp. elliptics) is finite.*

We will be mainly interested in groups G that are commensurable with $\mathrm{PSL}_2(\mathbb{Z})$. It follows in this case that G is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ and the set of cusps of G is $\mathbb{Q} \cup \{\infty\}$. Examples of such groups are defined as follows.

Let N be a positive integer, the principal congruence subgroup $\Gamma(N)$ of $\mathrm{PSL}_2(\mathbb{Z})$ is defined by

$$\Gamma(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a \equiv d \equiv 1(\mod N),\ b \equiv c \equiv 0(\mod N) \right\}.$$

It is of finite index in $\mathrm{PSL}_2(\mathbb{Z})$, for $N \geq 3$

$$\mu(N) = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma(N)] = \frac{N^3}{2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

$$\text{while} \quad [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma(2)] = 6.$$

In fact, we have the following exact sequence

$$0 \longrightarrow \Gamma(N) \longrightarrow \mathrm{PSL}_2(\mathbb{Z}) \longrightarrow PSL_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 0,$$

where $PSL_2(\mathbb{Z}/N\mathbb{Z}) = SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ and $SL_2(\mathbb{Z}/N\mathbb{Z})$ is the group of matrices of determinant 1 and with entries in $\mathbb{Z}/N\mathbb{Z}$. Clearly, $\Gamma(N)$ is the kernel of the map $\mathrm{PSL}_2(\mathbb{Z}) \longrightarrow PSL_2(\mathbb{Z}/N\mathbb{Z})$, so it is normal in $\mathrm{PSL}_2(\mathbb{Z})$.

It is easy to see that, for $N \geq 2$, $\Gamma(N)$ has no elliptic points.

Definition 1.3.2. Let N be a positive integer. A subgroup G of $\mathrm{PSL}_2(\mathbb{Z})$ is called a congruence subgroup if it contains a $\Gamma(N)$, and it is called of level N if N is the smallest integer such that $\Gamma(N)$ is in G.

Example 1.3.1. The groups

$$\Gamma_1(N) = \left\{ \alpha \in \mathrm{PSL}_2(\mathbb{Z}) |\ \alpha \equiv \begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix} (\mod N) \right\} / \{\pm I\},$$

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) |\ b \equiv 0(\mod N) \right\} / \{\pm I\}$$

which clearly are congruence subgroups of level N. Notice that $\Gamma_1(N) = \langle \Gamma(N),\ T \rangle$.

An other important example of congruence subgroups, is the subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) |\ c \equiv 0(\mod N) \right\} / \{\pm I\}.$$

Clearly, $\Gamma_0(N)$ is a congruence subgroup of level N and is conjugate to the subgroup $\Gamma^0(N)$ by the transformation $z \mapsto Nz$.

The index $\mu_0(N)$, the numbers ν_2 and ν_3 of elliptic points of order two and three respectively, and the number ν_∞ of cusp points are given by (see for example [28], Proposition 1.43)

$$\mu_0(N) = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_0(N)] = N.\prod_{p|N}\left(1+\frac{1}{p}\right)$$

$$\nu_2 = \begin{cases} 0, & \text{if } 4 \mid N; \\ \prod_{p|N}\left(1+\left(\frac{-1}{p}\right)\right), & \text{otherwise.} \end{cases}$$

$$\nu_3 = \begin{cases} 0, & \text{if } 9 \mid N; \\ \prod_{p|N}\left(1+\left(\frac{-3}{p}\right)\right), & \text{otherwise.} \end{cases}$$

$$\nu_\infty = \sum_{d|N} \varphi((d, N/d))$$

where φ is the Euler's function and $(\frac{-}{p})$ the quadratic residue symbol given by

$$\left(\frac{-1}{p}\right) = \begin{cases} 0, & \text{if } p = 2; \\ 1, & \text{if } p \equiv 1(\mod 4); \\ -1, & \text{if } p \equiv 3(\mod 4). \end{cases}$$

$$\left(\frac{-3}{p}\right) = \begin{cases} 0, & \text{if,} p = 3; \\ 1, & \text{if,} p \equiv 1(\mod 3); \\ -1, & \text{if,} p \equiv 2(\mod 3). \end{cases}$$

To illustrate some of the properties mentioned at the end of the previous section we draw the fundamental region for the groups $\Gamma(2)$, $\Gamma_0(2)$, and $\Gamma_0(4)$, and give the generators of these groups (see figures 2, 3 and 4 respectively).

$$\Gamma(2) = \langle S_2, T^2 \rangle$$

$$\Gamma_0(2) = \langle S_2, T \rangle$$

$$\Gamma_0(4) = \langle S_4, T \rangle$$

where T is as before, $S_2 : z \mapsto z/(2z+1)$, and $S_4 : z \mapsto z/(4z+1)$.

In particular, $\Gamma(N)$ and $\Gamma_0(N)$ are commensurable with $\mathrm{PSL}_2(\mathbb{Z})$, so they have $\mathbb{Q} \cup \{\infty\}$ as their set of cusps.

Let G be a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ of genus g, let ν_∞ be the number of inequivalent cusps, and let r be the number of inequivalent elliptic points. Let $m_1, ..., m_r$ be the orders of the stabilizer of all conjugacy classes of elliptic points. Then we say that G has signature $(g;\ m_1, ..., m_r;\ \nu_\infty)$. The algebraic structure of the group can be determined by its signature. In fact, the group has a presentation:
generators :

$$A_1,\ B_2, ...,\ A_g,\ B_g;\ E_1, ...,\ E_r;\ P_1, ...,\ P_{\nu_\infty}$$

relations :

$$E_1^{m_1} = ... = E_r^{m_r} = \prod_{i=1}^{\nu_\infty} P_i \prod_{i=1}^{r} E_i \prod_{i=1}^{g} A_i B_i A_i^{-1} B_i^{-1}.$$

The generators P_i are parabolic, the E_i are elliptic, and the A_i and B_i are hyperbolic.

Now, denote by ν_2, ν_3 the numbers of G-inequivalent elliptic points of order 2 and 3 respectively, and μ the index of G in $\mathrm{PSL}_2(\mathbb{Z})$. The Riemann-Hurwitz formula yields

Proposition 1.3.4. *If G is a subgroup of $PSL_2(\mathbb{Z})$, then*

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2} \tag{1}$$

Remark 1.3.1. • We can use the above proposition, noting that

$$\nu_\infty(\Gamma(N)) = \frac{\mu(N)}{N},$$

to prove that $\Gamma(N)$ has genus zero if and only if $1 \leq N \leq 5$.

- In [22] Ogg noticed that the number of the integers N such that $\Gamma_0(N)$ is of genus zeros is finite, namely for the following values of $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18$, and 25.

- It has been shown [16] that $\Gamma_0(N)$ has no elliptics of order 2 if -1 is not a square mod N, and has no elliptics of order 3 if -3 is not a square mod N. Therefore, the values of N for which $\Gamma_0(N)$ is genus 0 and torsion free are $N = 4,\ 6,\ 8,\ 9,\ 12,\ 16,\ 18,\ 25$. Also, we note that $\Gamma_0(N^2)$ and $\Gamma(N)$ are conjugate for $N = 2,\ 3,\ 4,\ 6$, however $\Gamma_0(36)$ is no longer of genus 0.

Table 1 illustrates the index, and the signature for $\Gamma_0(N)$ for these values of N stated in the previous remark.

Table 1.1.

N	Index	Signature
1	1	(0;2,2;1)
2	3	(0;2,0;2)
3	4	(0;0,3;2)
4	6	(0;0,0;3)
5	6	(0;2,2,3,3;2)
6	12	(0;0,0;4)
7	8	(0;0,3,3;6)
8	12	(0;0,0;4)
9	12	(0;0,0;4)
10	18	(0;2,2,0;4)
12	24	(0;0,0;6)
13	14	(0;2,2,3,3;2)
16	24	(0;0,0;6)
18	36	(0;0,0;8)
25	30	(0;2,2,0;6)

Chapter 2

MODULAR FUNCTIONS

In this chapter, we introduce the notion of modular functions and Hauptmoduln for discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$. We study their properties and the function field of related Riemann surfaces.

2.1 MODULAR FUNCTIONS

Let G be a group commensurable with $\mathrm{PSL}_2(\mathbb{Z})$. Recall that the quotient space $G \setminus \mathbb{H}^*$ has a structure of Riemann surface inherited from $\mathbb{H}$.

Definition 2.1.1. A modular function for G is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ invariant under the action of G, i.e. for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and $z \in \mathbb{H}$

$$f\left(\frac{az+b}{cz+d}\right) = f(z),$$

and such that f is meromorphic at the cusps. To say that f is meromorphic at the cusps means that for any $\alpha \in \mathrm{PSL}_2(\mathbb{Z})$ the function $f(\alpha z)$ has a Fourier expansion, also called q-expansion, of the form

$$f(\alpha z) = \sum_{k=-\infty}^{\infty} b_k^{\alpha} q^{k/N_\alpha}$$

for some b_k^α and N_α depending also on α with $b_k^\alpha = 0$ for all but finitely many negative k, where $q = \exp(2\pi iz)$ and $z \in \mathbb{H}$.

Remark 2.1.1. For convenience, when the meaning is clear, we refer to the transformation $z \mapsto (az+b)/(cz+d)$ by the corresponding matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$, as we did in the above definition.

A modular function, in fact, defines a meromorphic function on the Riemann surface $G \setminus \mathbb{H}^*$.

Modular functions have interesting properties, we state some of them in the following theorem

Theorem 2.1.1 ([2], Theorem 2.4, 2.6).

1. *If f is modular and not identically 0, then the number of zeros of f is equal to the number of poles of f in the closure of the fundamental region.*

2. *If f is a modular function and bounded on $\mathbb{H}$ then f is constant.*

2.2 SOME CLASSICAL MODULAR FUNCTIONS

The functions in this section can all be expressed in terms of the classical Jacobi Theta functions defined by

$$\theta_2(z) = \sum_{-\infty}^{\infty} p^{(n+\frac{1}{2})^2}, \quad \theta_3(z) = \sum_{-\infty}^{\infty} p^{n^2}, \quad \theta_4(z) = \sum_{-\infty}^{\infty} (-1)^n p^{n^2},$$

where $p = \exp(\pi iz)$ and $z \in \mathbb{H}$, which behave under the generators $T : z \mapsto z+1$ and $S : z \mapsto -1/z$ and of $\mathrm{PSL}_2(\mathbb{Z})$ as follows

$$\theta_2(Tz) = \exp(\frac{\pi i}{4})\theta_2(z),\ \theta_3(Tz) = \theta_4(z),\ \theta_4(Tz) = \theta_3(z)$$

$$\theta_2(Sz) = (-iz)^{\frac{1}{2}}\theta_4(z),\ \theta_3(Sz) = (-iz)^{\frac{1}{2}}\theta_3(z),\ \theta_4(Sz) = (-iz)^{\frac{1}{2}}\theta_2(z)$$

and which satisfy the fundamental relation (see for example [25], for more other relations)

$$\theta_2^4 + \theta_4^4 = \theta_3^4.$$

2.2.1 The j-function

When $G = \mathrm{PSL}_2(\mathbb{Z})$, the classical elliptic function

$$j(z) = 1728\frac{g_2^3(z)}{\Delta(z)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots,$$

where g_2 is the Eisenstein series and Δ is the discriminant function defined by

$$g_2(z) = 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m+nz)^4}, \quad \text{and} \quad g_3(z) = 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m+nz)^6}$$

$$\Delta(z) = g_2^3(z) - 27g_3^2(z) = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24},$$

is invariant under $\mathrm{PSL}_2(\mathbb{Z})$. It takes the values 0, 1, and ∞ on the points ρ, i, and ∞ respectively. It is known that ([16])

$$j(z) + 744 = 2^8 \frac{(\theta_2^8(z) + \theta_3^8(z) + \theta_4^8(z))^3}{\theta_2^8(z)\theta_3^8(z)\theta_4^8(z)}.$$

2.2.2 The β-function

The β-function is defined by

$$\beta(z) = (16\frac{\theta_3(z)^4}{\theta_2(z)^4} - 8)^2 - 40 = \frac{1}{q} + 276q - 2048q^2 \cdots .$$

The facts that β is invariant under $\Gamma_0(2)$ and has a q-expansion as in the definition follow from the properties of Jacobi Theta functions. Recall that $\theta_2(\infty) = 0$, so the β-function has a simple zero at infinity. Some special values of β are

$$\beta(\frac{-1+i}{2}) = -40, \qquad \beta(0) = 24, \qquad \beta(\infty) = \infty$$

2.2.3 The λ-function

We define a modular function for $\Gamma_0(4)$, which we call the
λ-function, by

$$\lambda(z) = 16\frac{(\theta_3^2(z) + \theta_4^2(z))^4}{\theta_2^8(z)} - 8 = \frac{1}{q} + 20q - 62q^3 + 216q^5 - \cdots .$$

It takes the values $-8, 8$, and ∞ at the three inequivalent cusps $-1, 0$, and ∞ respectively.

2.3 THE DEFINITION OF A HAUPTMODUL

Considerable interest has been shown in genus zero subgroups of $\mathrm{PSL}_2(\mathbb{R})$, since the advent of "Moonshine", especially to those subgroups commensurable with $\mathrm{PSL}_2(\mathbb{Z})$, mainly, because of the following property.
When the genus of G is 0, any nonconstant function giving an isomorphism from the compact Riemann surface $G \setminus \mathbb{H}^*$ onto $\mathbb{C} \cup \{\infty\}$ generates the field of modular functions for G.

Definition 2.3.1. Let G be commensurable with $\mathrm{PSL}_2(\mathbb{Z})$ of genus zero. Let f be an isomorphism from $G \setminus \mathbb{H}^*$ onto $\mathbb{C} \cup \{\infty\}$. Then f is called a *Hauptmodul* for the genus zero group G if f maps ∞ to ∞; it is unique up to multiplication by a nonzero constant and addition of a constant.
If, in addition, the q-expansion of f has the form

$$f(z) = \frac{1}{q^{1/N}} + \sum_{k=1}^{\infty} a_k q^{k/N} \tag{2}$$

for some positive integer N, where $q = \exp(2\pi i z)$ and $z \in \mathbb{H}$, then we say that f is the normalized Hauptmodul at infinity for G. The normalized Hauptmodul is unique.

Throughout this work, by Hauptmodul we mean the unique normalized Hauptmodul for G.

Example 2.3.1. 1. The j-function induces an isomorphism from $G \setminus \mathbb{H}^*$ onto $\mathbb{C} \cup \{\infty\}$, and has q-expansion of the form (3) ($N = 1$). Therefore it is a Hauptmodul for the modular group $\mathrm{PSL}_2(\mathbb{Z})$.

2. The β-function is a Hauptmodul for the genus zero group $\Gamma_0(2)$. One can, using only properties of Jacobi Theta functions to prove that

$$j = \frac{(\beta - 232)^3}{(\beta - 24)^2}.$$

3. For $\Gamma_0(4)$, the Hauptmodul is given by the λ-function. Similarly, as in the previous example, the λ-function is connected to the j-function and to the β-function by the following

$$j = \frac{(\lambda^2 + 240\lambda + 2112)^3}{(\lambda + 8)(\lambda - 8)^4}, \quad \beta = \lambda + \frac{256}{\lambda + 8}.$$

Remark 2.3.1. $\Gamma_0(4)$ is conjugate to $\Gamma(2)$ by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, therefore, one can easily check that $\lambda(z/2)$ is a Hauptmodul for $\Gamma(2)$. More generally, recall the result of [16], the values of N for which $\Gamma(N)$ is conjugate to $\Gamma_0(N^2)$ and $\Gamma_0(N^2)$ is genus zero are exactly $N = 1, 2, 3, 4$ and they are the only ones, the matrix of conjugation being $\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}$. In these cases, if $f_N(z)$ is a Hauptmodul for $\Gamma_0(N^2)$ then $f_N(z/N)$ is a Hauptmodul for $\Gamma(N)$.

Also, one can express all the Hauptmoduls in terms of the Dedekind Eta function, defined as follows

$$\eta(z) = q^{1/24} \prod_{k=1}^{\infty} (1 - q^k),$$

where q is as usual, and satisfies

$$\eta(Tz) = \exp(2\pi i/24)\eta(z),$$

$$\eta(Sz) = \sqrt{-iz}\, \eta(z).$$

In table 2.1, we give the expression of the Haupmoduls for $\Gamma_0(N)$ in terms of the Dedekind Eta function, for those values of N such that $\Gamma_0(N)$ is genus zero (see [6]).

Table 2.1.

N	Hauptmodul for $\Gamma_0(N)$
2	$\frac{\eta^{24}(z)}{\eta^{24}(2z)}$
3	$\frac{\eta^{12}(z)}{\eta^{12}(3z)}$
4	$\frac{\eta^{8}(z)}{\eta^{8}(4z)}$
5	$\frac{\eta^{6}(z)}{\eta^{6}(5z)}$
6	$\frac{\eta^{5}(z)\eta(3z)}{\eta(2z)\eta^{5}(6z)}$
7	$\frac{\eta^{4}(z)}{\eta^{4}(7z)}$
8	$\frac{\eta^{12}(4z)}{\eta^{4}(2z)\eta^{8}(8z)}$
9	$\frac{\eta^{3}(z)}{\eta^{3}(9z)}$
10	$\frac{\eta^{4}(2z)\eta^{2}(5z)}{\eta^{2}(z)\eta^{4}(10z)}$
12	$\frac{\eta^{4}(4z)\eta^{2}(6z)}{\eta^{2}(2z)\eta^{4}(12z)}$
13	$\frac{\eta^{2}(z)}{\eta^{2}(13z)}$
16	$\frac{\eta^{2}(z)\eta(8z)}{\eta(2z)\eta^{2}(16z)}$
18	$\frac{\eta(6z)\eta^{3}(9z)}{\eta(3z)\eta^{3}(18z)}$
25	$\frac{\eta(z)}{\eta(25z)}$

2.4 FIELDS OF MODULAR FUNCTIONS

Let N be a positive integer, and denote by $\mathfrak{F}_{N,\mathbb{C}}$ the field of modular functions of level N over $\mathbb{C}$, i.e. the field of modular functions invariant under $\Gamma(N)$ whose q-expansions have coefficients in $\mathbb{C}$. The group $\mathrm{PSL}_2(\mathbb{Z})$ operates as a group of automorphisms of $\mathfrak{F}_{N,\mathbb{C}}$ by $f \mapsto f \circ \alpha$, $\alpha \in \mathrm{PSL}_2(\mathbb{Z})$. Indeed, let $\alpha \in \mathrm{PSL}_2(\mathbb{Z})$, $\gamma \in \Gamma(N)$, and $f \in \mathfrak{F}_{N,\mathbb{C}}$. Then $f(\alpha\gamma z) = f(\gamma'\alpha z) = f(\alpha z)$, since $\Gamma(N)$ is normal in $\mathrm{PSL}_2(\mathbb{Z})$. Therefore, $f \circ \alpha$ is invariant under $\Gamma(N)$, and clearly meromorphic on $\mathbb{H}$.

We shall now find generators for $\mathfrak{F}_{N,\mathbb{C}}$, which behave nicely under the transformations of $\mathrm{PSL}_2(\mathbb{Z})$.

Definition 2.4.1. Let N be an integer > 1, for $r, s \in \mathbb{Z}$ not both divisible by N, we define functions $f_{(r,s)}$ by $f_{(r,s)}(z) = f((rz+s)/N; z)$, where

$$f(w;z) = \frac{g_2(z)g_3(z)}{\Delta(z)}\wp(w;z,1), \qquad z \in \mathbb{H},\ w \in \mathbb{C},$$

where the $g_i (i = 2,3)$ the classical Eisenstein series, Δ the discriminant modular function, and $\wp$ the Weierstrass $\wp$-function associated to the lattice $L = \mathbb{Z} + z\mathbb{Z}$ defined as

$$\wp(w;z,1) = \frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right),$$

is the so called *first Weber* function.
If $(r,s,N) = 1$, $f_{(r,s)}$ is called *primitive* of level N.

Now, since the $\wp$-function is periodic, it follows that $f_{(r,s)}$ depends only on the residue classes of r and $s \mod N$, that means that
$f_{(r,s)} = f_{(r',s')}$ whenever $r \equiv r' \mod N$ and $s \equiv s' (\mod N)$. Thus, we make the following notation which may exhibit more this property. Let $(a_1, a_2) = a \in \mathbb{Q}^2$ but not in $\mathbb{Z}^2$, and we write $f_a(z) = f(a_1 z + a_2; z)$. Such functions are called the *Fricke* functions.

If $\alpha \in \mathrm{PSL}_2(\mathbb{Z})$, since $\mathbb{Z} + z\mathbb{Z} = \mathbb{Z} + \alpha z\mathbb{Z}$, we have

$$f_a \circ \alpha(z) = f_{a\alpha}(z) = f_a(\alpha z).$$

Note that $-I$ acts trivially, since the $\wp$-function is an even function. Hence, the action of $\mathrm{PSL}_2(\mathbb{Z})$ is well defined. Here also, we denote a transformation $z \mapsto (az+b)/(cz+d)$ by its corresponding matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$. We also notice that, by definition, the f_a are holomorphic on $\mathbb{H}$.

Remark 2.4.1. The Fricke functions are modular of level N, because if $\alpha \in \Gamma(N)$, then $a\alpha \equiv a(\mod N)$ and hence, from the comments above, $f_{a\alpha} = f_a$ and so $f_{a\alpha}(z) = f_a(\alpha z) = f_a(z)$, for every $\alpha \in \Gamma(N)$.

If f_a is primitive of level N, then so is $f_{a\alpha}$ for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.
Indeed, let $a = (r/N, s/N)$ such that $f_a = f_{(r,s)}$ is primitive,
$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$ and $e, g, h \in \mathbb{Z}$ such that
$re + sf + Ng = 1$ $((r, s, N) = 1)$. Set $e' = ed - gb$, $g' = -ec + ga$, $h' = h$, then $e'(ar + bs) + g'(cr + ds) + h'N = 1$, i.e. $(ar + cs, br + ds, N) = 1$, so $f_{a\alpha}$ is primitive.

Hence $\mathrm{PSL}_2(\mathbb{Z})$ permutes the primitive Fricke functions of level N among themselves.

Theorem 2.4.1 ([13], Theorem 2, p. 65). *For every positive integer $N \geq 1$, we have*

$$\mathfrak{F}_{N,\mathbb{C}} = \mathbb{C}(j, f_a |\ Na \in (\mathbb{Z}/N\mathbb{Z})^2, a \neq 0).$$

Furthermore, the Galois group of $\mathfrak{F}_{N,\mathbb{C}}$ over $\mathbb{C}(j)$,

$$Gal(\mathfrak{F}_{N,\mathbb{C}}/\mathbb{C}(j)) = PSL_2(\mathbb{Z}/N\mathbb{Z})$$

acts as $f_a \mapsto f_{a\alpha}$, $\alpha \in PSL_2(\mathbb{Z}/N\mathbb{Z})$.

Next, let G be a congruence subgroup of the modular group $\mathrm{PSL}_2(\mathbb{Z})$ of level N, so that $\Gamma(N) \subset G \subset \mathrm{PSL}_2(\mathbb{Z})$. If f is invariant under G, then f is also modular for $\Gamma(N)$. Therefore, the field of modular functions for G is a subfield of the field $\mathfrak{F}_{N,\mathbb{C}}$ of modular functions of level N.

The following result characterizes the field of modular functions for the special case when $G = \Gamma_0(N)$.

Theorem 2.4.2 ([19], Theorem 6.1). *The field, say $\mathbb{C}(\Gamma_0(N))$, of modular functions for $\Gamma_0(N)$ is generated over $\mathbb{C}$ by $j(z)$ and $j(Nz)$.*

Remark 2.4.2. When the genus of $\Gamma_0(N)$ is zero, namely for the following values of $N = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 12,\ 13,\ 16,\ 18,\ 25$, $\mathbb{C}(\Gamma_0(N)) = \mathbb{C}(f_N)$ where f_N is the unique Hauptmodul for $\Gamma_0(N)$. Therefore, f_N can be expressed as a rational fraction of $j(z)$ and $j(Nz)$, and also $j(z)$ and $j(Nz)$ can be expressed as a rational fractions of f_N.

Our next goal is to compute the field of modular functions over $\mathbb{Q}$. Let $f_{(r,s)}$ be as in the previous section. For a fixed integer $N > 1$, we form a polynomial in X by the product

$$P(X) = \prod_{(r,s)\in(\mathbb{Z}/N\mathbb{Z})^2} (X - f_{(r,s)}).$$

Notice that the functions in the product may all be primitive of level N.
The coefficients of this polynomial are invariant under $SL_2(\mathbb{Z})$, since $SL_2(\mathbb{Z})$ permutes the $f_{(r,s)}$. Hence, these coefficients are modular functions for $SL_2(\mathbb{Z})$, holomorphic on $\mathbb{H}$, therefore they are polynomials in j. The q-expansion of $f_{(r,s)}$ is given by

$$f_{(r,s)}(z) = -2^{-7}3^{-5}(1 + \frac{12q^{r/N}\xi_N^s}{1 - q^{r/N}\xi_N^s} + 12\sum_{m,n\geq 1} nq^{mn}(q^{nr/N}\xi_N^s + q^{-nr/N}\xi_N^{-s} - 2)), \tag{3}$$

where $\xi_N = \exp(2\pi i/N)$. Therefore, these polynomials have their coefficients in the field $\mathbb{Q}(\xi_N)$.

Denote by $F = \mathbb{Q}(j, f_a |\ Na \in (\mathbb{Z}/N\mathbb{Z})^2,\ a \neq (0,0))$, $\mathbb{Q}_N = \mathbb{Q}(\xi_N)$, and $\mathfrak{F}_N$ the field of modular functions of level N over $\mathbb{Q}_N$. We have the following

Theorem 2.4.3 ([13], [28]). *We have*

1. $\mathfrak{F}_N = F$.

2. *The Galois group of $\mathfrak{F}_N$ over $\mathbb{Q}(j)$ is*

$$PGL_2(\mathbb{Z}/N\mathbb{Z}) = GL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

If $\alpha \in GL_2(\mathbb{Z}/N\mathbb{Z})$, then the automorphism induced by α on $\mathbb{Q}_N$ is given by the determinant, i.e. if we denote by $\sigma(\alpha)$ the induced automorphism by α on $\mathbb{Q}_N$ then

$$\sigma(\alpha)(\xi_N) = \xi_N^{\det \alpha}.$$

3. *The Galois group of $\mathfrak{F}_N$ over $\mathbb{Q}_N(j)$ is $PSL_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. 1. Obviously $F \subseteq \mathfrak{F}_N \subset \mathfrak{F}_{N,\mathbb{C}}$. Next, we have to show that F and $\mathbb{C}$ are linearly disjoint over $\mathbb{Q}_N$. (Recall that two subfields E and F of a field L, both containing a field K, are said to be linearly disjoint over K if every subset of E (respectively F) linearly independent over K is also linearly independent over F (respectively over E)). It will follow, since $\mathbb{C}(F) = \mathfrak{F}_{N,\mathbb{C}}$, that $F = \mathfrak{F}_N$.

Let $\mu_1, .., \mu_k \in \mathbb{C}$ be linearly independent over $\mathbb{Q}_N$. Suppose $\sum_{i=1}^k \mu_i g_i = 0$, $g_i \in F$. Let $g_i = \sum_n c_{i,n} q^{n/N}$ with $c_{i,n} \in \mathbb{Q}_N$. Then we get $\sum_{i=1}^k \mu_i c_{i,n} = 0$ for every $n \geq 1$, so, since the μ_i are linearly independent over $\mathbb{Q}_N$, $c_{i,n} = 0$ for every i and n. Therefore $g_i = 0$ for every i. Hence F and $\mathbb{C}$ are linearly independent over $\mathbb{Q}_N$.

2. First, by Theorem 3.1, we see that the Galois group of $\mathfrak{F}_N$ over $\mathbb{Q}(j)$ contains $PSL_2(\mathbb{Z}/N\mathbb{Z})$.

Set $G_N = \{\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$. Then every element of $GL_2(\mathbb{Z}/N\mathbb{Z})$ decomposes uniquely into the product of an element in G_N by an element of $SL_2(\mathbb{Z}/N\mathbb{Z})$. Indeed, let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z})$. If $\det \alpha = k \in (\mathbb{Z}/N\mathbb{Z})^\times$, then $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \begin{pmatrix} a & b \\ c/k & d/k \end{pmatrix}$, with $\begin{pmatrix} a & b \\ c/k & d/k \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$.

Next, we shall prove $G_N \subset Gal(\mathfrak{F}_N/\mathbb{Q}(j))$. We see, from expression (3), that $f_a = f_{(r,s)}$ is in the field of power series $\mathbb{Q}_N((q^{1/N}))$. For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, let σ_d be the automorphism of $\mathbb{Q}_N((q^{1/N}))$ obtained by extending the automorphism $\psi : \xi_N \longmapsto \xi_N^d$ of $\mathbb{Q}_N$ to $\mathbb{Q}_N((q^{1/N}))$ as follows $\sum c_n X^n \longmapsto \sum \psi(c_n) X^n$. Then j, g_2, and g_3 are fixed by this automorphism, since their q-expansion is in $\mathbb{Q}((q))$. On the other hand, we see, by (3) that $\sigma_d : f_{(r,s)}(z) \longmapsto f_{(r,sd)}(z)$, i.e. σ_d defines

an element of $Gal(\mathfrak{F}_N/\mathbb{Q}(j))$, σ_d is represented by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, and hence $G_N \subset Gal(\mathfrak{F}_N/\mathbb{Q}(j))$. However, from the comments at the beginning of the proof of (2), and noting that $\pm I$ acts trivially, we get $PGL_2(\mathbb{Z}/N\mathbb{Z}) = Gal(\mathfrak{F}_N/\mathbb{Q}(j))$.

Moreover, if $\alpha \in GL_2(\mathbb{Z}/N\mathbb{Z})$, then the automorphism induced by α on $\mathbb{Q}_N$ is given by the determinant, since the decomposition of elements of $GL_2(\mathbb{Z}/N\mathbb{Z})$.

3. Follows from above.

□

If $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \in G_N$, the automorphism in the Galois group $PGL_2(\mathbb{Z}/N\mathbb{Z})$ induced by α will be denoted by $*k$, and write $f * k$ for the image of f under that automorphism. This action is, in fact, an action of the corresponding automorphism $\sigma(\alpha) \in Gal(\mathbb{Q}_N/\mathbb{Q})$ on the coefficients in the q-expansion of f. As an immediate consequence, we have

Corollary 2.4.4. *Let G be a genus zero congruence subgroup, of level N, and a Hauptmodul f. Denote by $G * k$ the fixing group of the image $f * k$. Then $G * k$ also contains $\Gamma(N)$.*

Remark 2.4.3. One is now able to prove, using theorem 3.3, that $\mathbb{Q}(j(z), j(Nz))$ is the subfield of the function field $\mathfrak{F}_N$ fixed by $\Gamma_0(N)$.

2.5 THE AUTOMORPHISMS OF THE MODULAR FUNCTION FIELD $\mathfrak{F}_N$

In this section we discuss briefly some results concerning the automorphisms of the function field $\mathfrak{F}_N$ of modular functions of level N over $\mathbb{Q}$.

Now, consider the group

$$U = \prod_p GL_2(\mathbb{Z}_p) \times GL_2^+(\mathbb{R}),$$

where $GL_2(\mathbb{Z}_p)$ is the group of invertible matrices with entries in the ring of p-adic integers, and $\mathrm{GL}_2^+(\mathbb{R})$ is the group of real invertible matrices with positive determinant.

The next result characterizes the action of U on $\mathfrak{F}_N$.

Proposition 2.5.1 ([28], Proposition 6.21). *For every $u \in U$ and every N, there exists $\alpha \in M_2(\mathbb{Z}) \cap GL_2^+(\mathbb{Q})$ such that $u_p \equiv \alpha \mod (N.M_2(\mathbb{Z}_p))$ for every prime p. Then $au = a\alpha$ for every $Na \in (\mathbb{Z}/N\mathbb{Z})^2$, $a \neq (0,0)$. Therefore, $f_a \mapsto f_{au} = f_{a\alpha}$ defines an element of $Gal(\mathfrak{F}_N/\mathbb{C}(j))$. Call it $\sigma(u)$, and write $h^{\sigma(u)}$ for the image of $h \in \mathfrak{F}_N$ under that automorphism. Moreover, $h^{\sigma(\gamma)} = h \circ \gamma$ for every $h \in \mathfrak{F}_N$ and $\gamma \in SL_2(\mathbb{Z})$.*

Theorem 2.5.2 ([28], Proposition 6.22).

1. *For every $\alpha \in GL_2^+(\mathbb{Q})$ and $h \in \mathfrak{F}_N$, $h \circ \alpha \in \mathfrak{F}_{N'}$ for some integer N'.*

2. *For all $\alpha, \beta \in GL_2^+(\mathbb{Q})$, $u, v \in U$ such that $\alpha u = v\beta$, we have*

$$(j \circ \alpha)^{\sigma(u)} = j \circ \beta, \quad \text{and} \quad (f_a \circ \alpha)^{\sigma(u)} = f_{av} \circ \beta$$

for all $Na \in (\mathbb{Z}/N\mathbb{Z})^2$, $a \neq (0,0)$.

For $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, we define similarly $\sigma(u)$ by $h^{\sigma(\alpha)} = h \circ \alpha$ for every $h \in \mathfrak{F}_N$.

We conclude this chapter by a corollary which is an immediate consequence of the above result and which we will use in chapter 4.

Corollary 2.5.3 ([10]). *Let $h \in \mathfrak{F}_N$, $\alpha \in GL_2^+(\mathbb{Q}) \cap M_2(\mathbb{Z})$. Set $k = det(\alpha)$. Then $h \circ \alpha \in \mathfrak{F}_{kN}$.*

Proof. First note that, by Theorem 2.5.2, 1., if $f_a \in \mathfrak{F}_N$, then $f_a \circ \alpha \in \mathfrak{F}_{N'}$ for some N'.

Now, let $\gamma \in \Gamma(kN)$, write $\gamma = I + kNB$. Define $\gamma' = \alpha\gamma\alpha^{-1} = I + kN\alpha B\alpha^{-1}$. Note that $\alpha B\alpha^{-1}$ has the form $1/k \begin{pmatrix} x & y \\ t & z \end{pmatrix}$. Therefore $\gamma' \in \Gamma(N)$. Hence $f_a(\alpha\gamma z) = f_a(\gamma'\alpha z) = f_a(\alpha z)$, so that $f_a \circ \alpha$ is invariant under $\Gamma(kN)$. Now, by Proposition 3.4.1

of chapter 3, α is equivalent to a triangular matrix $\alpha' = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad = k, 0 \leq b < d$, i.e. there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\alpha = \gamma\alpha'$. However, since $f_a \circ \alpha = f_a \circ \gamma\alpha' = f_{a\gamma} \circ \alpha'$ and $f_{a\gamma} \in \mathfrak{F}_N$, $f_a \circ \alpha$ has an expansion with respect to $q^{1/kN}$ with coefficients in $\mathbb{Q}(\exp(2\pi iz/kN))$, therefore $f_a \circ \alpha \in \mathfrak{F}_{kN}$.

Similarly, keeping the same notions as above, for j, we have $j \circ \alpha = j \circ \gamma\alpha' = j \circ \gamma'$, which is clearly an element of $\mathfrak{F}_{kN}$. Finally, since $\mathfrak{F}_N$ is generated by the f_a and j, the result follows.

□

Chapter 3

REPLICABLE FUNCTIONS

In this chapter, we introduce the notion of replicable functions, and provide some of their basic properties.

3.1 FINITE SIMPLE GROUPS

In studying finite group theory, interest is focussed on simple groups, i.e. those groups whose only normal subgroups are the trivial ones or the groups themselves. The importance of finite simple groups lies in the fact that any finite group can be constructed from a sequence of finite simple groups.

The classification of all finite simple groups has now been completed. It is one of the important accomplishments of the end of the twentieth century. The list of finite simple groups is composed of the following four families.

1. The cyclic groups $C_p = \mathbb{Z}/p\mathbb{Z}$, p prime.

2. The alternating groups A_n, $n \geq 5$.

3. The 16 infinite families of lie type groups, for example the projective special linear group $PSL_n(F_p) := SL_n(F_p)/\{aI\}$, $a \in F_p$ such that $a^n = 1$ where

$SL_n(F_p)$ is the group of $n \times n$ matrices with entries from the finite field F_p and determinant 1, except for $PSL_2(\mathbb{Z}/2\mathbb{Z}) = S_3$ and $PSL_2(\mathbb{Z}/3\mathbb{Z}) = A_4$.

4. The family of the 26 sporadic simple groups given by Table 1 .

The Monster, or Friendly-Giant, was discovered independently in 1973 by Fischer and Griess and is by definition the largest of these 26 sporadic groups. It has order

$$|\mathbb{M}| = 2^{45}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71 \approx 8.10^{53}.$$

The name "Monster" was invented by Conway, referring to its gigantic order.
It has been noticed that even with that gigantic order, the largest order of an element of $\mathbb{M}$ is 119, the number of conjugacy classes is 193, and the number of conjugacy classes of cyclic groups is 172.

In the following table, we give the explicit list of all sporadic groups (see [5]).

Table 3.1. The sporadic groups

Group	Order	Investigators
M_{11}	$2^4.3^2.5.11$	Mathieu
M_{12}	$2^6.3^3.5.11$	Mathieu
M_{22}	$2^7.3^2.5.7.11$	Mathieu
M_{23}	$2^7.3^2.5.7.11.23$	Mathieu
M_{24}	$2^{10}.3^3.5.7.11.23$	Mathieu
J_2	$2^7.3^3.5^2.7$	Hall,Janko
Suz	$2^{13}.3^7.5^2.7.11.13$	Suzuki
HS	$2^9.3^2.5^3.7.11$	Higman, Sims
McL	$2^7.3^6.5^3.7.11$	McLaughlin
Co_3	$2^{10}.3^7.5^3.7.11.23$	Conway
Co_2	$2^{18}.3^6.5^3.7.11.23$	Conway
Co_1	$2^{21}.3^9.5^4.7^2.11.13.23$	Conway, Leech
He	$2^{10}.3^37.5^2.7^3.17$	Held/Higman, McKay
Fi_{22}	$2^{17}.3^9.5^2.7.11.13$	Fischer
Fi_{23}	$2^{18}.3^{13}.5^2.7.11.13.17.23$	Fischer
Fi'_{24}	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$	Fischer
HN	$2^{14}.3^6.5^6.7.11.19$	Harada, Norton/Smith
Th	$2^{15}.3^{10}.5^3.7^2.13.19.31$	Thompson/Smith
B	$2^{41}.3^{13}.5^6.7^2.11.13.17.19.23$ .31.47	Fischer/Sims, Leon
$\mathbb{M}$	$2^{45}.3^{20}.5^9.7^6.11^2.13^3.17.19$ .23.29.31.41.47.59.71	Fischer, Griess
J_1	$2^3.3.5.7.11.19$	Janko
$O'N$	$2^9.3^4.5.7^3.11.19.31$	O'Nan/Sims
J_3	$2^7.3^5.5.17.19$	Janko/Higman, McKay
Ly	$2^8.3^7.5^6.7.11.31.37.67$	Lyons/Sims
Ru	$2^{14}.3^3.5^3.7.13.29$	Rudvalis/Conway, Wales
J_4	$2^{21}.3^3.5.7.11^3.23.29.31.37.43$	Janko/Norton, Parker, Benson, Conway, Thackray

It has often happened that the existance of a sporadic group was predicted some time before its construction. In such cases, to illustrate this phenomenon, the slash in table 3.1 separates names of people who were mainly concerned with the prediction, before it, and those mainly concerned with the construction, after it, while the comma means that independent investigators were involved. For more details see [5].

Many properties of the monster have been established even before Griess proved, in 1981, its existence, such as the entire character table which was computed by Fischer, Livingstone, and Thorne.

It turned out that the first non-trivial irreducible representation has dimension 196883.

Recall that a group representation of a finite group G is a group action on a K-vector space V, K a field, by invertible linear maps. So a representation group is a group homomorphism $\phi : G \to GL(V)$. A representation is said to be irreducible if it has no nontrivial invariant space. If ϕ is a group representation of G, we define the character χ of ϕ by

$$\chi : G \longrightarrow K$$

$$g \mapsto \chi(g) = Tr(\phi(g))$$

where $Tr(\phi(g))$ is the trace of the matrix $\phi(g)$, when the dimension of the vector space V is finite.

3.2 MONSTROUS MOONSHINE

Since the discovery of the Monster $\mathbb{M}$, many surprising and important connections to several fields have been reached, for instance to the theory of modular functions.

In 1978 John McKay, observed that

$$196884 = 1 + 196883,$$

where 196884 is the coefficient of q in the q-expansion of the j-function, and 196883 is the dimension of the first non-trivial irreducible representation of the Monster $\mathbb{M}$,

and thus suggesting a connection between number theory and the representations of the Monster $\mathbb{M}$. Another mathematician, John Thompson, decided to take McKay's observation further, and pointed out that the next few coefficients of the elliptic modular j-function were also simple linear combinations of dimensions of irreducible representations of the Monster $\mathbb{M}$; for example $2149376 = 21296876 + 196883 + 1$. He suggested to replace the coefficients of the j-function by the traces of the corresponding representations ϕ_n on different elements g of $\mathbb{M}$. Conway and Norton followed up Thompson's suggestion, and they found by calculating the first few terms that the resulting series, known as the Thompson-McKay series,

$$f_g(z) = \frac{1}{q} + \sum_{k=1}^{\infty} Tr(\phi_k(g))q^k$$

are all Hauptmoduls for some genus zero subgroup of $\mathrm{PSL}_2(\mathbb{Z})$.

In their remarkable paper [6] they proposed ideas to explain this unexpectedly relationship between finite group theory and number theory, resulting in a new, beautiful, and sophisticated theory, known as *Moonshine theory*. In 1979, they conjectured what is known as the Moonshine conjecture.

The Moonshine conjecture:

To each conjugacy class of cyclic subgroups $< g >$ of the Monster $\mathbb{M}$, there corresponds a series

$$f_g(q) = \frac{1}{q} + \sum_{n=1}^{\infty} a_n(g)q^n$$

such that:

1. *For all $n \geq 1$, $g \mapsto a_n(g)$ is a character of the Monster group.*
2. *As a function of z, $z \in \mathbb{H}$, where $q = \exp(2\pi iz)$, $f_g(z)$ is modular function for some genus zero subgroup G of $PSL_2(\mathbb{R})$ containing a $\Gamma_0(N)$, for some N, with finite index, and the transformations $z \mapsto z + k$ if and only if $k \in \mathbb{Z}$.*

This conjecture has been proved by Borcherds [3] in 1992.

Furthermore, Conway and Norton observed that, for a given $g \in \mathbb{M}$, the McKay-Thompson series f_{g^k} attached to powers of g are connected in a special way. Indeed, these series satisfy the relation

$$\sum_{\substack{ad=n \\ 0\leq b<d}} f_{g^a}\left(\frac{az+b}{d}\right) = F_n\left(f_g(z)\right), \tag{4}$$

where F_n is a specific polynomial depending only on n and f_g, this will be subject of later section. For example if $f = j$ the j-function, then the n-th action of the classical Hecke operator, given by

$$n.T_n(j(z)) = \sum_{\substack{ad=n \\ 0\leq b<d}} j\left(\frac{az+b}{d}\right), \tag{5}$$

is in fact a polynomial in j, and that polynomial satisfies certain properties, for instance it is such that

$$n.T_n(j(z)) = \frac{1}{q^n} + \sum_{k=1}^{\infty} c_k^{(n)} q^k \tag{6}$$

by the notation $c_k^{(n)}$, we mean just that the coefficients in the above expansion depends on the coefficients of the j-function.

3.3 FABER POLYNOMIALS

Let f be a function with a formal q-expansion given by

$$f(z) = \frac{1}{q} + \sum_{k=1}^{\infty} a_k q^k, \tag{7}$$

where $a_k \in \mathbb{C}$, $q = exp(2\pi iz)$, and $z \in \mathbb{H}$. Then, for each $n \in \mathbb{N}$, there exists a unique monic polynomial of degree n, denoted by F_n^f or just by F_n if there is no confusion, such that

$$F_n(f(z)) = \frac{1}{q^n} + \sum_{k=1}^{\infty} a_k^{(n)} q^k \tag{8}$$

i.e. the only term of negative power is $1/q^n$.

This polynomial F_n is called the Faber polynomial of f. They were introduced by Faber in 1903 in the study of approximation theory of analytic functions.

Example 3.3.1. 1. If f is the j-function, then the n-th associated Faber polynomial is nothing else but the n-th Hecke operator. (Proof, see Proposition 3.5.2, 1.).

2. If $f(z) = 1/q$, then for each $n \in \mathbb{N}$, $F_n(X) = X^n$.

Now, let f be a function given by (7) which we thought of as a function in q. We now write $f(q)$ instead of $f(z)$, and consider the derived function

$$g_x(q) = \frac{q.f'(q)}{x - f(q)} \tag{9}$$

from f. The derivative is derived with respect to q.

Using expression (7) of f, we have

$$g_x(q) = \frac{1 - \sum_{k=1}^{\infty} k a_k q^{k+1}}{1 - q\left(x - \sum_{k=1}^{\infty} a_k q^{k+1}\right)},$$

so in a neighborhood of $q = 0$, the Taylor expansion of $g_x(q)$ is a power series in q. Write its q-expansion as

$$g_x(q) = \sum_{k=0}^{\infty} Q_k(x) q^k. \tag{10}$$

Then, by substituting (7) and (10) in (9), we obtain

$$\left(\sum_{k=0}^{\infty} Q_k(x) q^k\right)\left(x - \frac{1}{q} - \sum_{k\geq 1}^{\infty} a_k q^k\right) = \frac{-1}{q} + \sum_{k\geq 1}^{\infty} a_k q^{k-1}.$$

Identifying the coefficients of powers of q, we get
$Q_0(x) = 1$, $Q_1(x) = x$ and for $n \geq 2$

$$Q_{n+1}(x) = xQ_n(x) - \sum_{k=1}^{n-1} a_{n-k} Q_k(x) - (n+1)a_n. \tag{11}$$

Example 3.3.2. $Q_0(x) = 1$; $Q_1(x) = x$; $Q_2(x) = x^2 - 2a_1$;
$Q_3(x) = x^3 - 3a_1 x - 3a_2$.

Proposition 3.3.1. *For each $n \in \mathbb{N}$, Q_n is the n-th Faber polynomial associated to f.*

Proof. We have

$$g_x(q) = \frac{q.f'(q)}{x - f(q)} = \sum_{k=0}^{\infty} Q_k(x) q^k.$$

Write the last equality as

$$\frac{f'(q)}{x - f(q)} = \frac{1}{q} + \sum_{k=1}^{\infty} Q_k(x) q^{k-1}.$$

Integrating with respect to q, we get

$$-\log(f(q) - x) = \log(q) + \sum_{k=1}^{\infty} \frac{Q_k(x)}{k} q^k$$

so that

$$-\log(f(q) - f(p)) - \log(q) = \sum_{k=1}^{\infty} \frac{Q_k(f(p))}{k} q^k. \quad (\star)$$

However, we can write $\log(f(q) - f(p))$ as follows

$$\begin{aligned}
\log(f(q) - f(p)) &= \log\left(\frac{1}{q} - \frac{1}{p} + \sum_{k=1}^{\infty} a_k \left(q^k - p^k\right)\right) \\
&= \log(\left(\frac{1}{q} - \frac{1}{p}\right) + \log\left(1 + pq \sum_{k=1}^{\infty} a_k \frac{q^k - p^k}{p - q}\right) \\
&= \log(\left(\frac{1}{q} - \frac{1}{p}\right) + \sum_{k,m \geq 1}^{\infty} h_{k,m} q^k p^m.
\end{aligned}$$

Therefore,

$$\begin{aligned}
-\log(f(q) - f(p)) - \log(q) &= \log\left(1 - \frac{q}{p}\right) + \sum_{k,m \geq 1}^{\infty} h_{k,m} q^k p^m \\
&= \sum_{m=1}^{\infty} \frac{q^m}{m p^m} + \sum_{k,m \geq 1}^{\infty} h_{k,m} q^k p^m.
\end{aligned}$$

So, the coefficient of q^k in the above equation is

$$\frac{1}{kp^k} + \sum_{m=1}^{\infty} h_{k,m} p^m.$$

The corresponding coefficient from $(\star)$ is $1/kQ_k(f(p))$, and therefore the result follows. □

Example 3.3.3. From (11), if $f(z) = 1/q + cq$, with $c \in \mathbb{C} - \{0\}$, then for $n \geq 1$

$$F_n(x) = \frac{1}{2^{n+1}}[(x - (x^2 - 4c)^{1/2})^n + (x + (x^2 - 4c)^{1/2})^n].$$

This follows from the recurrence relation and the fact that all the coefficients of f are zero except $a_{-1} = 1$ and $a_1 = c$.
In particular, if $c = 1$, then $F_n(x) = T_n(2x)$, where T_n is the Chebyshev polynomial of degree n.

3.4 TRANSFORMATIONS OF ORDER n

The result of this section will be useful in order to establish the replication of some important examples and also to derive some partial results in the next chapter.

Let n be a fixed positive integer, and let

$$\Delta(n) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) |\ det(A) = ad - bc = n \right\}.$$

Obviously $\Delta(1) = \mathrm{SL}_2(\mathbb{Z})$.

Then one defines a relation on $\Delta(n)$ as follows:
We say that two elements A_1 and A_2 of $\Delta(n)$ are equivalent if and only if there exists an element $B \in \mathrm{SL}_2(\mathbb{Z})$ such that $A_1 = BA_2$. Clearly this is an equivalence relation.

Proposition 3.4.1. *A complete system of nonequivalent representatives of the equivalence classes in $\Delta(n)$ is given by the set*

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = n, 0 \leq b < d \right\}.$$

Moreover, if $A_1 \in S$ and $B_1 \in SL_2(\mathbb{Z})$, then there exist $A_2 \in S$ and $B_2 \in SL_2(\mathbb{Z})$ such that $A_1 B_1 = B_2 A_2$.

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta(n)$. If $c = 0$, multiplying if necessary by $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, for some $k \in \mathbb{Z}$, we may assume $0 \leq b < d$, i.e $A \in S$. Therefore we may suppose $c \neq 0$. Next, reduce the fraction a/c in lowest terms, i.e. $a/c = -r/s$ with $(r, s) = 1$, so that $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with p, q are integers such that $ps - qr = 1$. Clearly $B \in \mathrm{SL}_2(\mathbb{Z})$ is such that $BA = \begin{pmatrix} pa + qc & pb + qd \\ 0 & rb + sd \end{pmatrix}$. Hence A is equivalent to an upper-triangular matrix. Multiplying if necessary by $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, for some integer k, we may suppose that A is equivalent to an element $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ of S. To complete the proof of the first statement we need only to verify that if two elements $A_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$ and $A_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ of S are equivalent then $A_1 = A_2$. Suppose that A_1 and A_2 are equivalent, so there is $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such $A_2 = BA_1$. Equating entries, we find $r = 0$, and $ps = 1$ since $B \in \mathrm{SL}_2(\mathbb{Z})$, therefore $p = s = \pm 1$. Replacing B by $-B$ if necessary, we may assume $p = s = 1$. Therefore, we get $a_1 = a_2, d_1 = d_2$ and $b_1 = b_2$ (since $b_2 = b_1 + qd_1, 0 \leq b_2 < d_2 = d_1$, so $q = 0$). This completes the proof of the first statement.

The second statement is now straightforward since $det(A_1 B_1) = n$. □

For the remaining of this section, we investigate $\Delta(n)$ in connection with $\Gamma_0(2)$ and $\Gamma_0(4)$.

Corollary 3.4.2. *Let* $A_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \in S$, $B_1 = \begin{pmatrix} p_1 & q_1 \\ r_1 & s_1 \end{pmatrix} \in \Gamma_0(2)$ *and let* A_2, B_2 *as in Proposition* 3.4.1, *write* $A_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$, *then, independently of the choice of* n*:*

1. *If* a_1 *is odd, then so is* a_2, *and in this case* $B_2 \in \Gamma_0(2)$.

2. *If* a_1 *is even,* a_2 *is also even.*

Proof. Equating entries in $A_1B_1 = B_2A_2$, we get

$$\begin{cases} a_1p_1 + r_1b_1 = a_2p_2 & (\star) \\ d_1r_1 = a_2r_2 & (\star\star) \end{cases}$$

1. If a_1 is odd, we get from $(\star)$ that a_2p_2 is odd, since $A_1 \in \Gamma_0(2)$ so p_1 is odd. Therefore a_2 and p_2 are odd. However, from $(\star\star)$ we have $2|a_2r_2$, and so $2|r_2$, i.e. $B_2 \in \Gamma_0(2)$.

2. If a_1 is even, $(\star)$ implies that $2|a_2p_2$, hence $2|a_2$ or $2|p_2$. If $2|a_2$, we are done. If not, then $2|p_2$. Since $det(B_2) = 1$, we find that r_2 is odd, then from $(\star\star)$, we get $2|a_2r_2$, and therefore a_2 is even.

□

Corollary 3.4.3. *Let* $A_1 \in S$, $B_1 \in \Gamma_0(4)$, *and let* A_2, B_2 *be as in Proposition* 3.4.1, *then we have:*

1. *If* a_1 *is odd, so is* a_2, *and in this case* $B_2 \in \Gamma_0(4)$.

2. *If* $a_1 \equiv 2(\mod 4)$, *then so is* a_2, *and we have* $B_2 \in \Gamma_0(2)$.

3. *If* $a_2 \equiv 0(\mod 4)$, *then* $a_2 \equiv 0(\mod 4)$.

Proof. We proceed similarly as in Corollary 3.4.2, so we get

$$\begin{cases} a_1p_1 + b_2r_2 = a_2p_2 & (\star) \\ d_1r_1 = a_2r_2 & (\star\star) \end{cases}$$

1. If a_1 is odd, similarly as above we get that a_2 and p_2 are odd, and from $(\star\star)$ we get $4|a_2r_2$, and so $4|r_2$, i.e. $B_2 \in \Gamma_0(4)$.

2. If $a_1 \equiv 2(\mod 4)$. From $(\star)$ we have $2|a_2p_2$, so $2|a_2$ or $2|p_2$. If $2|p_2$, $det(B_2) = 1$ implies that r_2 is odd. Hence from $(\star\star)$ we get $4|a_1$, a contradiction. Therefore $2|a_2$. Note that $a_2 \equiv 2(\mod 4)$ because if not, by $(\star)$ we will have that $4|a_1$ since p_1 is odd. Thus, by $(\star\star)$ we have $4|a_2r_2$, and hence $2|r_2$, i.e. $B_2 \in \Gamma_0(2)$ as needed.

3. For the last case, $a_1 \equiv 0(\mod 4)$, we have by $(\star)$ $a_2p_2 \equiv 0(\mod 4)$, so if p_2 is odd then we are done. If p_2 is even, by $(\star\star)$ we get $4|a_2r_2$, but $det(B_2) = 1$ therefore r_2 is odd, and hence $4|a_2$.

□

3.5 REPLICABLE FUNCTIONS

We define replicable functions formally, as follows:

Definition 3.5.1. A function f of the form (4) is said to be a replicable function, if for each positive integer a, $a \geq 1$, there are functions $f^{(a)}$ also of the form (7), called replicates of f, such that, for each positive integer n, $n \geq 1$,

$$\sum_{\substack{ad=n \\ 0\leq b<d}} f^{(a)}\left(\frac{az+b}{d}\right) = F_n(f(z)). \tag{12}$$

where F_n is the n-th Faber polynomial associated with f.

Lemma 3.5.1. *Let $\{f^{(a)}\}_{a\geq 1}$ be a sequence of functions with q-expansion given by*

$$f^{(a)}(z) = \frac{1}{q} + \sum_{k=1}^{\infty} a_k^{(a)} q^k.$$

Then for every $n \geq 1$, the sum

$$\sum_{\substack{ad=n \\ 0\leq b<d}} f^{(a)}\left(\frac{az+b}{d}\right) - \frac{1}{q^n}$$

has no fractional term in q. Furthermore, this sum is equal

$$\sum_{\substack{ad=n \\ 0\le b<d}} f^{(a)}\left(\frac{az+b}{d}\right) = \frac{1}{q^n} + \sum_{k=1}^{\infty} \gamma_k(n) q^k,$$

where

$$\gamma_k(n) = n \sum_{d|(k,n)} \frac{1}{d} a^{(d)}_{\frac{kn}{d^2}}.$$

Proof. First, note that

$$\sum_{\substack{ad=n \\ 0\le b<d}} f^{(a)}(\frac{az+b}{d})$$

has a term $1/q^n$, exactly when $a = n$.

Now, we can write this sum as

$$\begin{aligned}
\sum_{d|n} \sum_{0\le b<d} f^{(n/d)}\left(\frac{nz+bd}{d^2}\right) &= \sum_{d|n} \sum_{0\le b<d} \left(\exp\left(-2\pi i(nz+bd)/d^2\right)\right. \\
&\qquad \left. + \sum_{k=1}^{\infty} a_k^{(n/d)} \exp\left(2\pi i z k (nz+bd)/d^2\right)\right) \\
&= \sum_{d|n} \sum_{0\le b<d} \exp\left(-2\pi i(nz+bd)/d^2\right) \\
&\quad + \sum_{k=1}^{\infty} \sum_{d|n} a_k^{(n/d)} \exp(2\pi i k n z/d^2) \sum_{0\le b<d} \exp(2\pi i k b/d).
\end{aligned}$$

The first sum, in the last equality is equal to $1/q^n$ while the sum on b is equal to d if $d|k$ and is 0 otherwise. Hence

$$\sum_{d|n} \sum_{0\le b<d} f^{(n/d)}\left(\frac{nz+bd}{d^2}\right) = \frac{1}{q^n} + \sum_{k=1}^{\infty} \sum_{\substack{d|n \\ d|k}} d a_k^{(n/d)} \exp(2\pi i k n z/d^2).$$

Writing $k = ld$, and replacing d by n/d we get

$$\sum_{d|n} \sum_{0\le b<d} f^{(n/d)}\left(\frac{nz+bd}{d^2}\right) = \frac{1}{q^n} + \sum_{l=1}^{\infty} \sum_{d|n} \frac{n}{d} a^{(d)}_{nl/d} q^{ld}.$$

Finally, replacing again l by k/d, we get

$$\sum_{\substack{ad=n \\ 0\leq b<d}} f^{(a)}\left(\frac{az+b}{d}\right) = \frac{1}{q^n} + \sum_{k=1}^{\infty} \gamma_k(n) q^k,$$

where

$$\gamma_k(n) = n \sum_{d|(k,n)} \frac{1}{d} a^{(d)}_{\frac{kn}{d^2}}.$$

□

Example 3.5.1. If $f(z) = 1/q$, then f is replicable with $f^{(a)}(z) = 1/q$, for every $a \geq 1$. This is consequence of the property of the sum of the d-th roots of unity

$$\sum_{0\leq b<d} \exp(-2\pi i \frac{b}{d}) = 0.$$

Replication of the Moonshine functions follows from Borcherds' proof. Here we establish replication of a few of them in an elementary way.

Proposition 3.5.2.

1. *The j-function is replicable, and it replicates itself.*

2. *The β-function is replicable. The replicates of β are defined as follows*

$$\beta^{(a)} = \begin{cases} j \text{ , if } a \text{ is even,} \\ \beta, \text{ if } a \text{ is odd.} \end{cases}$$

3. *The λ-function. We define the replicates of λ as follows*

$$\lambda^{(a)} = \begin{cases} \lambda \text{ , if } a \text{ is odd,} \\ \beta \text{ , if } a \equiv 2(\mod 4), \\ j \text{ , if } a \equiv 0(\mod 4). \end{cases}$$

Proof. 1. Recall the n-th Hecke operator action given by (5), is in fact a modular function for $\mathrm{PSL}_2(\mathbb{Z})$, so it is a rational function of j, since j generates the field of modular functions for $\mathrm{PSL}_2(\mathbb{Z})$. Now, since the right hand side of (1) is holomorphic on $\mathbb{H}$, therefore it is a polynomial in j. It remains to prove that this polynomial has the form (8), but this is a consequence of Lemma 3.5.1.

2. Indeed, to prove that, for $n \geq 1$

$$\sum_{\substack{ad=n \\ 0 \leq b < d}} \beta^{(a)}(\frac{az+b}{d}) = F_n(\beta(z))$$

is equivalent to prove that the left hand side of the above sum is invariant under the action of $\Gamma_0(2)$ and has the form $1/q^n + \sum_{k=1}^{\infty} c_k q^k$. In case, since the β is an Hauptmodul for $\Gamma_0(2)$, it follows that this sum is a rational fraction of β, and since each one of its members is holomorphic on $\mathbb{H}$, this fraction is, in fact, a polynomial of β.

Now, to prove that this sum is invariant under the action of $\Gamma_0(2)$ is equivalent to prove $\Gamma_0(2)$ permutes the elements $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ of the set

$S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} | ad = n, 0 \leq b < d \right\}$, and preserves the parity of a, as following:

Let $A_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \in S$, $B_1 = \begin{pmatrix} p_1 & q_1 \\ r_1 & s_1 \end{pmatrix} \in \Gamma_0(2)$, so that according to Proposition 3.4.1, there are $A_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in S$, $B_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, such that $B_1 A_1 = A_2 B_2$. Equating entries in the previous equality, we get

$$\begin{cases} a_1 p_1 + r_1 b_1 = a_2 p_2 & (\star) \\ d_1 r_1 = a_2 r_2 & (\star\star) \end{cases}$$

Then, if a_1 is odd, since $B_1 \in \Gamma_0(2)$, we have $2|r_1$ and $2 \nmid p_1$ (since $\det B_1 = 1$). Therefore, from $(\star)$ and $(\star\star)$, we get

$$\begin{cases} a_1 \equiv a_1 p_1 \equiv a_2 p_2 (\mod 2) \\ a_2 r_2 \equiv 0 (\mod 2) \end{cases}$$

Hence, a_1 is odd and $2|r_2$, i.e. $B_2 \in \Gamma_0(2)$.

Now, if a_1 is even, $(\star)$ implies that $2|a_2 p_2$, so either $2|a_2$ or $2|p_2$. If $2|a_2$, we are done. If not, then $2|p_2$. However, $\det B_2 = 1$, therefore r_2 is odd, and then, from $(\star\star)$, we have $2|a_2 r_2$, so that $2|a_2$. Thus, we have proved that the

sum is invariant under $\Gamma_0(2)$. Also, we obtain from this that $\Gamma_0(2)$ preserve the replication power ($\beta^{(a_1)} = \beta^{(a_2)}$ whenever $a_1 \equiv a_2(\mod 2)$) of β. The fact that the sum has the form

$$\frac{1}{q^n} + \sum_{k=1}^{\infty} c_k q^k$$

follows from Lemma 3.5.1.

3. Similarly, as in the previous example, but this time using Corollary 3.4.3, we get that λ is a replicable function.

□

Norton gave an equivalent definition for replicable function as follows. This definition is more convenient for numerical calculation.
Now, define coefficients $h_{m,n}$ by

$$F_n(f(z)) = \frac{1}{q^n} + n \sum_{m=1}^{\infty} h_{m,n} q^m. \tag{13}$$

In fact, as we are going to see in the following remark, are the same as in the proof of Proposition 3.3.1.

Remark 3.5.1. The function $g_x(q)$ in (10) is connected to the $h_{m,n}$, since the Faber polynomials F_n are. If we differentiate

$$\frac{f'(q)}{f(p) - f(q)} - \frac{1}{q}, \qquad |p| < 1$$

but this time with respect to p, and from the proof of Proposition 3.3.1, we get

$$\frac{-f'(q)f'(p)}{(f(p) - f(q))^2} + \frac{1}{(p-q)^2} = \sum_{m,n \geq 1} mn h_{m,n} p^{m-1} q^{n-1}.$$

The left hand side is symmetric in p and q, therefore $h_{m,n} = h_{n,m}$, for every $m, n \geq 1$.

Proposition 3.5.3 ([1]).

Let f be a function of the form $f(q) = 1/q + \sum_{k=1}^{\infty} a_k q^k$. Then f is replicable if and only if $h_{m,n} = h_{r,s}$ whenever $lcm(m,n) = lcm(r,s)$, and $(m,n) = (r,s)$, where $h_{m,n}$ is as in (13).

Proof. The proof is based on the Möbius inversion formula. Suppose that f is such that $h_{m,n} = h_{r,s}$ whenever $mn = rs$, and $(m,n) = (r,s)$, then set

$$f^{(a)}(z) = \frac{1}{q} + \sum_{k=1}^{\infty} a_k^{(a)} q^k, \tag{14}$$

where

$$a_k^{(a)} = a \sum_{d|a} \mu(d) h_{a/d,dak}, \tag{15}$$

and μ is the Möbius function defined by

For a positive integer n

$$\mu = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } p^2 | n \text{ for some prime } p\ ; \\ (-1)^r, & \text{if } n = \prod_{i=1}^{r} p_i\ , \text{ where the } p_i \text{ are distinct primes.} \end{cases}$$

It follows that $f^{(1)} = f$, and therefore $h_{1,n} = h_{n,1} = a_n$. Now, by the Möbius inversion formula, we have

$$\sum_{d|a} \frac{1}{d} a^{(d)}_{a^2k/d^2} = h_{a,ak},$$

and by hypothesis, with $a = (m,n)$ and $k = mn/a^2$, we get

$$\sum_{d|(m,n)} \frac{1}{d} a^{(d)}_{mn/d^2} = h_{(m,n),mn/(m,n)} = h_{m,n}. \tag{16}$$

Therefore, by Lemma 3.5.1, we have

$$\sum_{\substack{ad=n \\ 0 \le b < d}} f^{(a)}\left(\frac{az+b}{d}\right) = F_n(f(z)).$$

Conversely, if f has replicates of the form (14), with coefficients as in (15), it follows from Lemma 3.5.1 that the $h_{m,n}$ in (13) satisfy (16). Therefore, $h_{m,n} = h_{r,s}$ whenever $lcm(m,n) = lcm(r,s)$, and $(m,n) = (r,s)$. □

Replicable functions have important properties. In fact, we have the following results.

Proposition 3.5.4 ([8]). *The only replicable functions with a finite number of terms in their q-expansion are the trivial functions* $1/q + cq$.

Proof. Set $f(z) = 1/q + a_1 q + ... + a_n q^n$. If $n = 0$ or 1, then we are done, so we may assume $n \geq 2$, and $a_n \neq 0$.
First, note that a_{n-1} must be zero. To see this, consider the second replication formula for f, so we have

$$F_2(f(z)) = f(z)^2 - 2a_1 = f^{(2)}(2z) + f(\frac{z}{2}) + f(\frac{z+1}{2}).$$

Substituting f in the above equation, we obtain

$$F_2(f(z)) = f^{(2)}(2z) + f\left(\frac{z}{2}\right) + f\left(\frac{z+1}{2}\right) = f^{(2)}(2z) + 2(a_2 q + \cdots + a_{k'} q^{k'/2}),$$

where

$$k' = \begin{cases} k, & \text{if } n \text{ is even,} \\ k-1, & \text{if } n \text{ is odd.} \end{cases}$$

But, the coefficient of q^{2n-1} on the left hand side of the above formula is $2a_{n-1}a_n$. However, $f^{(2)}(z) = 1/q +$ power series in q, therefore $a_{n-1}a_n = 0$, and hence $a_{n-1} = 0$ (since $a_n \neq 0$). Thus, we may consider

$$f(z) = \frac{1}{q} + a_1 q + ... + a_{n-k} q^{n-k} + a_n q^n$$

with $2 \leq k < n$, and $a_{n-k+1} = \cdots = a_{n-1} = 0$ and $a_{n-k} \neq 0$.

Next, we are going to prove, first that f has the form $f(z) = 1/q + a_n q^n$, and second that n must be 1.

Now, consider the $(k+1)$-st replication formula

$$F_{k+1}(f(z)) = f^{(k+1)}((k+1)z) + \sum_{\substack{ad=k+1 \\ 0\le b<d}}{}' f^{(a)}\left(\frac{az+b}{d}\right),$$

where the superscript in the sum, on the right hand side, means just that it is taken over $a \neq k+1$. We have $(k+1)a_{n-k}a_n^k q^{(k+1)n-k}$ is the term with second largest degree on the left hand side of the above formula, and the corresponding contribution to that power of q from $f^{(a)}$ on the right hand side, according to Lemma 3.5.1, is given by

$$\gamma_{(k+1)n-k}(k+1) = (k+1)\sum_{d|((k+1)n-k,k+1)} \frac{1}{d} a^{(d)}_{(k+1)((k+1)n-k)/d^2} = (k+1)a_{(k+1)((k+1)n-k)} = 0,$$

since, by hypothesis, $a_{(k+1)((k+1)n-k)} = 0$. Therefore, $(k+1)a_{n-k}a_n^k = 0$, a contradiction. Therefore, f must have the form

$$f(z) = \frac{1}{q} + cq^n.$$

Now, let k be such that $(k, n(n+1)) = 1$ and $k > n+1$.

Write

$$F_k(f(z)) = f(z)^k + b_2 f(z)^{k-2} + ... + b_{n-1}f(z) + b_n$$

$$= \frac{1}{q^k} + ... + C_k^j a^j q^{-k+j(n+1)} + ... + a^k q^{nk} + b_2 f(z)^{k-2} + ... + b_{n-1}f(z) + b_n$$

The terms in the above sum that may have a term of degree $-k+n+1$ are $f^n, b_2 f^{n-2}, ...,$ $b_{k-n}f^n$. However, the coefficient of q^{-k+n+1} in this sum is $b_{k-n-1} + kc$. Therefore, by definition of Faber polynomials, we have $b_{k-n-1} + kc = b_2 = ... = b_{k-n} = 0$.

Therefore, the coefficient of $q^{(k-n-1)n}$ is $c^{k-n}(C_k^{k-n} - k)$. However, the corresponding term in

$$\sum_{\substack{ad=k \\ 0\le b<d}}{}' f^{(a)}\left(\frac{az+b}{d}\right)$$

is once again by Lemma 3.5.1, is given by

$$\gamma_{(k-n-1)n}(k) = k\sum_{d|((k-n-1)n,k)} \frac{1}{d} a^{(d)}_{kn(k-n-1)/d^2} = ka_{kn(k-n-1)} = 0,$$

since, by hypothesis, $a_{kn(k-n-1)} = 0$. Therefore, $c^{k-n}(C_k^{k-n} - k) = 0$, and therefore $C_k^{k-n} - k = 0$. Hence, $n = 1$. This completes the proof. □

The next proposition characterizes replicable functions in terms of their first 23 coefficients. The proof of this proposition is based on the following lemma.

Lemma 3.5.5. *For $N \geq 1$, there exists $m, n, m', n' \geq 1$ such that $m + n = N$, $(m, n) = (m', n')$, $mn = m'n'$, and $m'+n' < m+n$ exactly when $N \neq 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 18, 20,$ and 24.*

Proof. First, note that if the lemma holds for N, by taking km, kn, km', kn' instead of m, n, m', n', for $k \geq 1$, it holds for kN. We consider the following cases:

1. $N = 2^a$, except for $N = 2, 4$ or 8. From the remark above, we then obtain all higher powers of 2 as multiple of 16. For $N = 16$, take $m = 1, n = 15, m' = 3$, and $n' = 5$.

2. $N = 2^a + 1$, $a \geq 4$. Take $m = 2^a - 2, n = 3, m' = 2^{a-1} - 1$, and $n' = 6$. We have $(m, n) = 3 or 1$. If $(m, n) = 3$, i.e. $3|m = 2m'$, then $(m', n') = 3$, since m' is odd. If $(m, n) = 1$, we must have $(m', n') = 1$, because if not, $3|m'$ so $3|m$, i.e. $(m, n) = 3$, a contradiction. Clearly, $mn = m'n'$ and $m' + n' < m + n$.

3. N odd, but $N - 1$ is not a power of 2. In this case, let 2^a be the exact power of 2 which divides $N - 1$, and take $m = N - 1, n = 1, m' = 2^{-a}(N - 1)$, and $n' = 2^a$. Note that $(m, n) = (m', n')$ and $2^a < N - 1$, so $N(2^a - 1) > 2^{2a} - 1$, and so $N > 2^{-a}(N - 1)$, i.e. m, n, m', n' satisfy the conditions of the lemma.

4. N even, not a power of 2. Then N must be a product of $2, 4$ or 8 with $3, 5$ or 9, since all other possibilities are multiples of the above cases, except for $N = 40, 36$ or 72, since $N \neq 6, 10, 12, 18, 20,$ and 24.

   - For $N = 40$, take $m = 1, n = 39, m' = 3$,and $n' = 13$.
   - For $N = 36$, $m = 1, n = 35, m' = 5$, and $n' = 7$ is a solution.
   - The case $N = 72$ follows from the case $N = 36$ and the first remark with $k = 2$.

Now, for $N \neq 1, 2, 3, 5, 4, 6, 8, 9, 10, 12, 18, 20,$ and 24, we can verify case by case that no solution m, n, m', n' exists, and the lemma follows. □

Proposition 3.5.6 ([8]). *A replicable function f, of the form (7), is determined by only 12 of its first 23 coefficients. Namely, with the following coefficients a_1, a_2, a_3, a_4, a_5, a_7, a_8, a_9, a_{11}, a_{17}, a_{19}, and a_{23}.*

Proof. Lemma 3.5.5 implies, if $k+1 \neq 2, 3, 4, 5, 6, 8, 9, 10, 12, 18, 20$, and 24, that there exist $m, n, m', n' > 0$ such that $m + n = k + 1$, $h_{m,n} = h_{m',n'}$ (since f is replicable), and $m' + n' < m + n$.
Now, from (13) the leading term of $h_{m,n}$, viewed as a polynomial in the a_i's, is $a_{m+n-1} = a_k$. Therefore solving $h_{m,n} = h_{m',n'}$ for a_k we can express a_k as a polynomial in $a_1, \ldots, a_{k-1}$. Iterating this process we can express all the coefficients of f as polynomials in a_1, a_2, a_3, a_4, a_5, a_7, a_8, a_9, a_{11}, a_{17}, a_{19}, and a_{23}. □

The functions j, β, and λ are all both Hauptmoduls and replicable. Therefore an immediate question is the following.
What is the relationship between Hauptmoduls and replicable functions?

A complete answer to this question is still not found, however we have the following conjecture on the concept of modularity of replicable functions made by Norton [20].

Conjecture:

A function of the form $f(q) = 1/q + \sum_{k=1}^{\infty} a_k q^k$, with $a_k \in \mathbb{Q}$, is replicable if and only if either f is trivial, i.e. $f(z) = 1/q + cq$, or it is the Hauptmodul for some genus zero congruence subgroup of $PSL_2(\mathbb{R})$ containing a $\Gamma_0(N)$, for some $N \in \mathbb{Z}$, with finite index, and $z \mapsto z + k$ if and only if $k \in \mathbb{Z}$.

This conjecture will be studied in a later chapter.

We end this chapter with the following Maple procedure, given in [11], to compute $a_k = h_{k,1}$, and the $h_{m,n}$ for a replicable function with integer coefficients in terms of the 12 of its first 23 coefficients mentioned in Proposition 4.3.

Procedure:

```
H := proc(r,s)
Local vr, vs, vrs, mr, ms, grs, lrs, k, q, m, n, t ;
option remember;
vr := max(r,s) ; vs := min(r,s) ; vrs := vr + vs;
if vs = 1 and remember(vr,[1,2,3,4,5,7,8,9,11,13,17,19,23]) then
```

```
RETURN(a[vr])
elsif vs = 1 then
mr := vr; vr := vr+1;
ms := vs; vs := vs-1;
while mr+ms ≥ vr+vs do
vr := vr-1;
vs := vs+1;
lrs := ilcm(vr,vs); mr := lrs;
grs := igcd(vr,vs); ms := grs;
for k from grs by grs to lrs do
if irem(lrs,k) = 0 then
q := iquo(vr*vs,k);
if igcd(k,q) = grs then
if k+q ¡ mr+ms then
mr := k;
ms := q;
fi
fi
fi
od
od;                    ###mr*ms = r*s, (mr,ms) = (r,s)###
t := vrs*H(mr,ms);                ###mr+ms¡r+s###
for m from 1 to vr-1 do
for n from 1 to vs-1 do
t := t - (m+n)*H(m,n)*H(vrs-m-n-1,1)
od
od ;
RETURN(t/vrs)
else
t := vrs*H(vrs-1,1);
for m from 1 to vr-1 do
```

```
for n from 1 to vs-1 do
t := t + (m+n)*H(m,n)*H(vrs-m-n-1,1)
od
od ;
fi
end :
```

Chapter 4

REPLICABILITY OF HAUPMODULS

The aim of this chapter is to discuss Norton's conjecture [20] relating replicable function with modular functions. We will explain the proof by Cummins and Norton on how modular functions are replicable.

4.1 CONGRUENCE SUBGROUPS OF $\mathrm{PSL}_2(\mathbb{R})$

In this subsection we further extend the notion of congruence subgroup, presented in chapter 2, to subgroups of $\mathrm{PGL}_2^+(\mathbb{R}) = \mathrm{GL}_2^+(\mathbb{R})/\{\mathbb{R}^* I\}$, where the subscript $+$ denotes positive determinant, and we characterize the elements of such groups.

Let $\Gamma(N)$ be the principal congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. Consider the following diagram

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SL}_2(\mathbb{R}) \\ \downarrow & & \downarrow \\ \mathrm{PSL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{PSL}_2(\mathbb{R}). \end{array}$$

Then we see we may consider $\mathrm{PSL}_2(\mathbb{Z})$ as a subgroup of $\mathrm{PSL}_2(\mathbb{R})$. The group $\mathrm{PGL}_2^+(\mathbb{Q}) = \mathrm{GL}_2^+(\mathbb{Q})/\{\mathbb{Q}^* I\}$ is a subgroup of $\mathrm{PGL}_2^+(\mathbb{R}) = \mathrm{GL}_2^+(\mathbb{R})/\{\mathbb{R}^* I\}$. However $\mathrm{PSL}_2(\mathbb{R}) \cong \mathrm{PGL}_2^+(\mathbb{R})$. Thus we may consider the subgroups of $\mathrm{PGL}_2^+(\mathbb{Q})$ as subgroups of $\mathrm{PSL}_2(\mathbb{R})$. We identify $\mathrm{PSL}_2(\mathbb{Z})$ and its subgroups with their images in $\mathrm{PSL}_2(\mathbb{R})$.

Definition 4.1.1. A subgroup G of $\mathrm{PSL}_2(\mathbb{R})$ is called a congruence group if G contains a $\Gamma(N)$ with finite index.

Remark 4.1.1. A congruence subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is commensurable with $\mathrm{PSL}_2(\mathbb{Z})$ therefore it is discrete and its set of cusps is $\mathbb{Q} \cup \{\infty\}$.

Example 4.1.1. The normalizer of $\Gamma_0(N)$ inside $\mathrm{PSL}_2(\mathbb{R})$ is described in [6] as follows. Let h be the largest divisor of 24 for which $h^2|N$, and set $N = hn$. The normalizer of $\Gamma_0(N)$ consists of the transformations $\begin{pmatrix} ae & b/N \\ cn & de \end{pmatrix}$ of determinant $e > 0$, where e is an exact divisor of n/h, i.e. $e|n/h$ and $(n/h, n/he) = 1$. (If e is an exact divisor of k we write $e||k$). The normalizer can also be described in terms of the Atkin-Lehner involutions that are defined as follows: Let h be as above, $N = hn$. The set of matrices $\begin{pmatrix} a & b/h \\ cn & d \end{pmatrix}$ of determinant 1 form a group, say $\Gamma_0(n|h)$, conjugate to $\Gamma_0(n/h)$ by the element $\begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix}$. The set W_e of all matrices of the form $\begin{pmatrix} ae & b \\ cN & de \end{pmatrix}$, where $e||N$, and determinant e is a single coset of $\Gamma_0(N)$. A representative w_e of this coset in quotient of the normalizer by $\Gamma_0(N)$ is called an Atkin-Lehner involution. For the special case $e = N$, a representative is given by $w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ which is known as the Fricke involution.
The full normalizer of $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ is obtained by adjoining to the group $\Gamma_0(n|h)$ its Atkin-Lehner involution (which are conjugate to those of $\Gamma_0(n/h)$ by $\begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix}$). Following Conway and Norton, we denote the normalizer of $\Gamma_0(N)$ by

$\Gamma_0(n|h)+e,f,g...$, where the subscript $+e,f,g...$ means that the Atkin-Lehner involutions $w_e,\ w_f,\ w_g,...$ are present. We shall actually abbreviate this notation and denote the normalizer by $\Gamma_0(n|h)+$ when all the Atkin-Lehner involutions are present. For example, if N is square free then $\Gamma_0(N)+ = \langle \Gamma_0(N),\ w_N \rangle$.

Obviously, $\Gamma_0(n|h)+$ contains $\Gamma_0(N)$ with finite index, and therefore is a congruence subgroup of $\mathrm{PSL}_2(\mathbb{R})$.

Remark 4.1.2. Another unexpected property of the Monster is the following. In [23], Ogg also noticed that the 15 primes dividing the order of the Monster, namely $p = 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 41,\ 47,\ 59,\ 71$, are exactly the values of p for which $\Gamma_0(p)+$ is of genus zero.

Lemma 4.1.1. *Let G be a congruence subgroup of $PSL_2(\mathbb{R})$. Then every element $\alpha \in G$ is represented by a matrix with rational entries.*

Proof. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Since, if $s \in \mathbb{Q} \cup \{\infty\}$ is a cusp for G, then so is $\gamma \cdot s$. Therefore $\gamma \cdot 0 = b/d \in \mathbb{Q} \cup \{\infty\}$ and $\gamma \cdot \infty \in \mathbb{Q} \cup \{\infty\}$.

If $\gamma \cdot 0 = \infty$, so $d = 0,\ b \neq 0,\ c \neq 0$. Set $s = a/c \in \mathbb{Q}$. Then, we see $\gamma = c \begin{pmatrix} s & t \\ 1 & 0 \end{pmatrix}$ where $t = \gamma \cdot 1 - s$.

If $\gamma \cdot \infty = \infty$, so $c = 0, a \neq 0, d \neq 0$, and similarly $\gamma = d \begin{pmatrix} n & m \\ 0 & 1 \end{pmatrix}$ where $b = dm$, and $n = \gamma \cdot 1 - m$. Therefore we may assume $\gamma \cdot 0 \neq \infty$ and $\gamma \cdot \infty \neq \infty$. In this case $\gamma \cdot \infty = a/c,\ \gamma \cdot 0 = b/d$ are in $\mathbb{Q}$, say $b = rd,\ a = tc$ for some $r, t \in \mathbb{Q}$. Now, let $p \in \mathbb{Q}$ such that $\gamma \cdot p = \infty$, so that $cp + d = 0$, i.e. $d = -cp$. Hence $\gamma = c \begin{pmatrix} t & -rp \\ 1 & -p \end{pmatrix}$ as needed. □

This lemma implies that a congruence subgroup G of $\mathrm{PSL}_2(\mathbb{R})$ is, in fact, a subgroup of $\mathrm{PGL}_2^+(\mathbb{Q})$.

In the rest of this section, G will be a genus zero congruence subgroup of $\mathrm{PSL}_2(\mathbb{R})$ containing a $\Gamma_0(N)$ with finite index and the transformation $z \mapsto z + k$ if and only if $k \in \mathbb{Z}$ and with Hauptmodul f. Such a group will said to be of Moonshine type.

Definition 4.1.2. Let $\gamma \in G$. We say that γ is written in lowest terms over $\mathbb{Z}$ if γ is represented by a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in $\mathbb{Z}$ such that $(a, b, c, d) = 1$. If the meaning is clear, we omit the term over $\mathbb{Z}$. In this case we define $|\gamma|$ to be the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Lemma 4.1.2 ([21], Lemma 1). *Let $\gamma \in G$. Then any prime p dividing $|\gamma|$ also divides N.*

Now, let G be a group of Moonshine type, and recall the action of the Galois automorphism $*k$ of $\mathfrak{F}_N$ induced by the element $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z})$, so $(k, N) = 1$. If we denote by $G * k$, as in Corollary 2.4.4 of chapter 2, the fixing group of the image $f*k$ of f under that automorphism, then $G*k$ contains $\Gamma(N)$. Moreover, we have

Lemma 4.1.3 ([9], Corollary 6.6, b). *The group $G * k$ also contains $\Gamma_0(N)$.*

Proof. First, note that if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, then $\alpha\gamma\alpha^{-1} = \begin{pmatrix} a & b/k \\ kc & d \end{pmatrix}$, therefore, $\mod (N)$, $\alpha\gamma\alpha^{-1} \in \Gamma_0(N)$, i.e. α normalizes $\Gamma_0(N) \mod (N)$, and so there is $\gamma' \in \Gamma_0(N)$ such that $\alpha\gamma \equiv \gamma'\alpha(\mod N)$. Now, since the j-function has rational integer coefficients, so $(j * k) \circ \gamma = j \circ \gamma = j = (j \circ \gamma') * k$, and for any $Na \in (\mathbb{Z}/N\mathbb{Z})^2$, $a \neq (0, 0)$, we have $(f_a * k) \circ \gamma = (f_a \circ \gamma') * k = f_a * k$. Therefore, since $\mathfrak{F}_N$ is generated over $\mathbb{Q}$ by the f_a and j and $f \in \mathfrak{F}_N$, we have $(f * k) \circ \gamma = (f \circ \gamma') * k = f * k$, and the result follows. □

Proposition 4.1.4 ([10]). *Let k and G be as above. If $\gamma = \begin{pmatrix} ka & b \\ c & d \end{pmatrix} \in G$ is written in lowest terms, then $\beta = \begin{pmatrix} a & b \\ c & kd \end{pmatrix} \in G * k$.*

Proof. Define two elements $u = (..., u_p, ...)$, $v = (..., v_p, ...) \in U$, where U is as defined

in §2.5 of chapter 2, by

$$u_p = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}, & \text{if } p|N; \\ \beta, & \text{if } p \nmid N \text{ and } p = \infty. \end{cases}$$

and

$$v_p = \begin{cases} \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}, & \text{if } p|N; \\ \gamma, & \text{if } p \nmid N \text{ and } p = \infty. \end{cases}$$

The elements u, and v are well-defined since, by Lemma 4.1.2 $\det\beta = \det\gamma$ divides N, therefore $\beta,\ \gamma \in GL_2(\mathbb{Z}_p)$. Now, recall the action of the group U on $\mathfrak{F}_N$ given in Proposition 2.5.1 of chapter 2. If N' is an integer dividing N, and since $u_p \equiv \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \mod (N'.M_2(\mathbb{Z}_p))$ for all primes p, we have that if $h \in \mathfrak{F}_{N'}$ then $h^{\sigma(u)} = h*k$. In particular, for any $Na \in (\mathbb{Z}/N\mathbb{Z})^2,\ a \neq (0,0)$, we have $(f_a \circ \gamma)^{\sigma(u)} = (f_a \circ \gamma) * k$, since by Corollary 2.5.3 of chapter 2 $f_a \circ \gamma \in \mathfrak{F}_{(N\det\beta)}$, and so by Lemma 4.1.1 we still have $u_p \equiv \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \mod ((N\det\gamma).M_2(\mathbb{Z}_p))$ for all primes p. Next, let $\delta \in \Gamma_0(N)$ such that $\delta \equiv \begin{pmatrix} k^{-1} & 0 \\ 0 & k \end{pmatrix} (\mod N)$, then for any $Na \in (\mathbb{Z}/N\mathbb{Z})^2,\ a \neq (0,0)$, we have $f_{av} \circ \beta = f_{av\delta} \circ \delta^{-1}\beta = (f_a * k) \circ \delta^{-1}\beta$, since $v_p\delta \equiv \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \mod (N.M_2(\mathbb{Z}_p))$. Therefore, by Theorem 2.5.2, (2) of chapter 2, we have $(f_a \circ \beta) * k = (f_a * k) \circ \delta^{-1}\beta$. Similarly, we have $(j \circ \beta) * k = (j * k) \circ \delta^{-1}\beta = j \circ \delta^{-1}\beta$, and hence for any $h \in \mathfrak{F}_n$, we have in particular $f * k = (f \circ \beta) * k = (f * k) \circ \delta^{-1}\beta$, and so $\delta^{-1}\beta \in G * k$. Finally, by Lemma 4.1.3, we have $\beta \in G * k$. □

4.2 REPLICABILITY OF HAUPTMODULS

The goal of this section is to prove that Haupmoduls with rational coefficients are replicable. The idea of the proof is to construct iteratively the replicates $f^{(n)}$ of the

Haupmodul f.

We suppose G is a genus zero subgroup of $\mathrm{PSL}_2(\mathbb{R})$ containing a $\Gamma_0(N)$ and the transformation $z \mapsto z+k$ if and only if $z \in \mathbb{Z}$ and with a Hauptmodul f with rational coefficients. We adopt the notation $a(t) = b(t) + o(1)$ to say that the difference between $a(t)$ and $b(t)$ is bounded as t tends to 0 along the imaginary axis.

Lemma 4.2.1. *For any positive integers m and L there exists a non-zero integer s such that $(1+sm, L) = 1$ and $(s, L) = (2, L)/((2, L), m)$.*

Proof. Let $m' = m/((2, L), m)$ and take $s = k(2, L)/((2, L), m)$ where

$$k \equiv \begin{cases} 1(\mod p) & \text{if } p|L, p|m, \text{ and } p \neq 2; \\ -2/m'(2,L)(\mod p), & \text{if } p|L, p \nmid m, \text{ and } p \neq 2; \\ 1(\mod (2, L)) & . \end{cases}$$

Then s satisfies the required properties. □

Proposition 4.2.2.

1. *If f is singular at r/m, where $(r, m) = 1$, then there exists $M \in G$ of the form $\begin{pmatrix} d & e \\ -lm & lr \end{pmatrix}$ when written in lowest terms such that*

   $$f(r/m + t) = \exp(2\pi i d/lm) \exp(2\pi i D/tm^2l^2) + o(1)$$

   where $D = |M|$.

2. *Also, for any integer k with $(k, lm) = 1$,*

   $$f(kr/m + t) = \exp(2\pi i dk'/lm) \exp(2\pi i D/tm^2l^2) + o(1),$$

   where $kk' \equiv 1(\mod lm)$.

3. Moreover, when written in lowest terms over $\mathbb{Z}$, M has the form

$$M = \begin{pmatrix} \psi\lambda\delta & \epsilon \\ -\psi\lambda\phi\nu & \lambda\phi\alpha \end{pmatrix}$$

where $(\delta, \phi\nu) = (\alpha, \psi\nu) = (\psi, \phi) = 1$, *and* $(2, \nu)\psi\phi|2$. *Also, if* $2|\psi\phi$ *then* $2|\lambda$.

Proof. (1) Since f is singular at r/m, there exists $M \in G$ such that $Mr/m = \infty$. Set $M = \begin{pmatrix} d & e \\ w & x \end{pmatrix}$ when written in lowest terms, then $wr/m + x = 0$, $dr/m + e \neq 0$, and so $w = -ml$, $x = lr$, for some $l \in \mathbb{Z}$. Now, f is invariant under M, so

$$f(r/m + t) = f\left(M(r/m + t)\right) = f\left(-\frac{dr + em}{lm^2t} - \frac{d}{lm}\right)$$

$$= f\left(-\frac{D}{l^2m^2t} - \frac{d}{lm}\right).$$

As $t \longrightarrow 0$ the results follows.

(2) Let $k \in \mathbb{Z}$, $(k, lm) = 1$, then there are integers u, v such that $ku + vlm = 1$. Let $A = \begin{pmatrix} 1 & dv \\ 0 & 1 \end{pmatrix}$, the element $B = AM = \begin{pmatrix} dkk' & e' \\ -lm & lr \end{pmatrix}$ belongs to G, where $kk' = 1 - lmv$. Therefore, by Proposition 4.1.4, $C = \begin{pmatrix} d\overline{k} & e' \\ -lm & klr \end{pmatrix} \in G * k = G$. Similarly, using

$$f(kr/m + t) = f(C(rk/m + t)) = f(-\frac{dk'}{lm} - \frac{D}{tm^2l^2})$$

the result follows as $t \longrightarrow 0$.

(3) We will prove this part in two steps.

STEP 1:

In this step, we prove that if M is written in lowest terms, then $l|\,(2/(2, m), l)\,d$.

We consider the following cases.

If $m = 0$, so $r = 1$ and by [28], Proposition 1.17 all elements of G that fix ∞ are either parabolic or the identity and therefore $l = d$.

If $r = 0$, then we take instead M the translation $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

If $mr \neq 0$, by the previous lemma there exists an integer $s \neq 0$ such that $(1 + sm, lm) = 1$ and (s, l) divides $(2, lm)/((2, lm), m)$ which divides $2/(2, m)$, and so $(s, l) \mid (2/(2, m), l)$. Let k be such that $k(1 + sm) \equiv 1(\mod lm)$. Therefore, by (1) and (2),

$$f\left(\frac{kr}{m} + t\right) = f\left(\frac{r}{m} + t\right) = \exp\left(\frac{2\pi id}{lm}\right) \exp\left(\frac{2\pi iD}{tm^2l^2}\right) + o(1)$$

$$= \exp\left(\frac{2\pi id(1 + sm)}{lm}\right) \exp\left(\frac{2\pi iD}{tm^2l^2}\right) + o(1).$$

Hence $l \mid sd$ and so $l \mid (s, l)d$.

STEP 2:

In this step we prove (3). Write $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and let $\lambda = ((a, c), (d, c))$, $\psi = (a, c)/\lambda$, and $\phi = (d, c)/\lambda$ so that $(\psi, \phi) = 1$ and so $\lambda\psi\phi \mid c$. Set $\nu = -c/\lambda\psi\phi$, $\alpha = d/(d, c)$, and $\delta = a/(a, c)$. Then M has the required form with $(\delta, \phi\nu) = (\alpha, \psi\nu) = 1$. Now, to show that $(2, \nu)\psi\phi \mid 2$, $M^{-1} \in G$, applying step 1 to both M and M^{-1}, we have $\phi \mid 2/(2, \nu)$ and $\psi \mid 2/(2, \nu)$, and therefore $(2, \nu)\psi\phi \mid 2$.

Finally, if for example $\phi = 2$, then $\psi = 1$ and $(2, \nu) = (2, \delta) = 1$. Hence $M = \begin{pmatrix} \psi\lambda\delta & \epsilon \\ -\psi\lambda\phi\nu & \lambda\phi\alpha \end{pmatrix} \equiv \begin{pmatrix} \lambda & \epsilon \\ 0 & 0 \end{pmatrix} (\mod 2)$, and $2 \mid |M|$, so by similar argument as in [21], lemma 1.

Suppose to the contrary that $2 \nmid \lambda$. Then, M has rank 1 in $GL(\mathbb{Z}/2\mathbb{Z})$ since ϵ is odd, and so $\Gamma(\lambda)$ projects onto the whole of $PSL_2(\mathbb{Z}/2\mathbb{Z})$, so

$$M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} (\mod 2).$$

Then the powers of M will also be congruent to this matrix modulo 2. However $2 \mid |M^i|$ for every i. Therefore, the cosets $\{M^i | i \geq 0\}$ are all distinct and so the index of $\Gamma(\lambda)$ in G is infinite, a contradiction, since in particular $\Gamma(\lambda)$ is a subgroup of G of finite index. Therefore, $2 \mid \lambda$. A similar argument gives the result in the case $\psi = 2$. □

Before proceeding to the main theorem of this section, we give a definition and some results on sums of roots of unity using modular functions.

Definition 4.2.1. For $r/m \in \mathbb{Q}$, define $\tau(r,m) = x/m'$ for some x such that $xr' \equiv 1(\mod m')$ and $x \equiv 1(\mod 2)$, where $m' = m/(m,r)$, $r' = r/(m,r)$.

We define $\xi(m) = \begin{cases} \exp(2\pi i\delta/\phi\nu), & \text{if } 1/m \text{ is G-equivalent to } \infty\ ; \\ 0, & \text{otherwise.} \end{cases}$

and

$$A(m) = 2\pi i|M|/\psi^2\lambda^2\phi^2\nu^2,$$

where $m = \psi\nu$ and

$$M = \begin{pmatrix} \psi\lambda\delta & \epsilon \\ -\psi\lambda\phi\nu & \lambda\phi \end{pmatrix}$$

is the element of G that maps $1/m$ to ∞.

Note that $\tau(r,m)$ changes by an integer for different choices of x, which does not change $\exp(2\pi i\tau(r,m))$, as we require.

Lemma 4.2.3. *We have*

$$\sum_{\substack{ad=n \\ 0\le b<d}} \exp\left(2\pi i\tau(ar+bm, dm)\right) = \begin{cases} \exp\left(2\pi i\tau(r,m)\right), & \textit{if } g=n(r,m); \\ 0, & \textit{otherwise.} \end{cases}$$

where $g = (ar+bm, dm)$.

Proof. Since the j-function is replicable, it satisfies the identity

$$\sum_{\substack{ad=n \\ 0\le b<d}} j\left(\frac{az+b}{d}\right) = F_n\left(j(z)\right).$$

Let $M = \begin{pmatrix} x & y \\ m' & r' \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$ that maps r/m to ∞. Evaluating both sides at $M(r/m+t)$ and taking t to 0, we get

$$F_n\left(j(M(r/m+t))\right) = \exp\left(2\pi inx/m'\right)\exp\left(\frac{2\pi i(m,r)^2 n}{tm^2}\right) + o(1)$$

$$= \exp\left(2\pi i n \tau(r,m)\right) \exp\left(\frac{2\pi i (m,r)^2 n}{tm^2}\right) + o(1)$$

with $x/m' = \tau(r,m)$, since F_n the n-th Faber polynomial associated with j. Similarly for $(ar+bm)/dm$, we have

$$\sum_{\substack{ad=n \\ 0\le b<d}} j\left(\frac{ar+bm}{dm} + \frac{at}{d}\right) = \sum_{\substack{ad=n \\ 0\le b<d}} \exp\left(2\pi i \tau(ar+bm, dm)\right) \exp\left(\frac{2\pi i g^2}{tnm^2}\right) + o(1).$$

By comparing the coefficients, we have the two possibilities $g = n(m,r)$ or $g \neq n(m,r)$, hence the result follows. □

Lemma 4.2.4. *Let*

$$s(n,g) = \sum_{d|n} (-1)^{n/d} \mu(d/g), n, \ g \in \mathbb{N}$$

where $\mu(x)$ is the Möbius function, defined to be zero for non-integral values x. Then $s(n,g) = -\delta_{n,g} + 2\delta_{n,2g}$, where $\delta_{l,k}$ is the Kronecker delta.

Proof. We have

$$s(n,g) = \sum_{\substack{d|n \\ g|d}} (-1)^{n/d} \mu(d/g),$$

put $d = d'g$ so $s(n,g) = \sum_{d'g|n} (-1)^{n/d'g} \mu(d') = s(n/g, 1)$.
Therefore it suffices to compute $s(k,1)$. We distinguish the following cases.

- If k is odd, $s(k,1) = \sum_{d|k} (-1)^{k/d} \mu(d) = -\sum_{d|k} \mu(d) = -\delta_{n,1}$.
- $k \equiv 0(\mod 4)$. In this case we have

$$s(k,1) = \sum_{\substack{d|k \\ 4\nmid d}} (-1)^{k/d} \mu(d) + \sum_{\substack{d|k \\ 4|d}} (-1)^{k/d} \mu(d)$$

$$= \sum_{\substack{d|k \\ 4\nmid d}} \mu(d) + 0 = \sum_{d|k} \mu(d) = 0$$

- If $k \equiv 2(\mod 4)$, we have

$$\begin{aligned} s(k,1) &= \sum_{\substack{d|k \\ 2\nmid d}} (-1)^{k/d}\mu(d) + \sum_{\substack{d|k \\ 2|d}} (-1)^{k/d}\mu(d) \\ &= \sum_{d|k/2} \mu(d) - \sum_{\substack{d|k \\ 2|d}} \mu(d) \\ &= \delta_{k/2,1} - (\delta_{k,1} - \delta_k/2, 1) \\ &= 2\delta_{k/2,1} = 2\delta_{k,2}. \end{aligned}$$

□

Lemma 4.2.5.

1. *The function*

$$h_n(z) = \sum_{\substack{ad=n \\ 0\le b<d}} (-1)^a j\left(\frac{az+b}{d}\right)$$

is invariant under $\Gamma_0(2)$.

2. *Moreover, as* $z \to \infty$

$$h_n(z) = (-1)^n \exp(2\pi i n z) + o(1),$$

and as $z \to 0$

$$h_n(z) = \begin{cases} -\exp(2\pi i n/z) + o(1), & \text{if } n \text{ is odd;} \\ -\exp(2\pi i n/z) + 2\exp(\pi i n/2z) + o(1), & \text{if } n \text{ is even.} \end{cases}$$

Proof. 1. The invariance of h_n under $\Gamma_0(2)$ follows from Corollary 3.4.2 of chapter 3 (see also the proof of Proposition 3.5.2, (2)).

2. For fixed a and d,

$$\sum_{0\le b<d} j\left(\frac{az+b}{d}\right) = \sum_{k\ge -1} dH_{dk} q^{ak}$$

so that the only non negative exponent in the q-expansion occurs for $d = 1$, $a = n$ and $k = -1$ (see Lemma 3.5.1 of chapter 3). Therefore, as $z \to \infty$ the result

follows.

For the second equality, as in the previous lemma, but this time applied to b/d, we have, as $z \to 0$

$$j\left(\frac{az+b}{d}\right) = \exp(2\pi i\tau(b,d))\exp(2\pi i(b,d)^2/nz) + o(1).$$

Therefore,

$$h_n(z) = \sum_{\substack{ad=n \\ 0\le b<d}} (-1)^a \exp(2\pi i\tau(b,d))\exp(2\pi i(b,d)^2/nz) + o(1)$$

$$= \sum_{d|n}(-1)^{n/d}\left(\sum_{0\le b<d}\exp(2\pi i\tau(b,d))\exp(2\pi i(b,d)^2/nz)\right) + o(1)$$

$$= \sum_{\substack{k|n \\ d|n}}(-1)^{n/d}\left(\sum_{0\le b<d}\exp(2\pi i\tau(b,d))\right)\exp(2\pi ik^2/nz) + o(1)$$

$$= \sum_{k|n}\left(\sum_{d|n}\mu(d/g)\right)\exp(2\pi ik^2/nz) + o(1),$$

where $k = (b,d)$. By the previous lemma, the result follows.

□

Lemma 4.2.6.

1. *If m' is odd and n is even, $m' = m/(m,r)$, then*

$$\sum_{\substack{ad=n \\ 0\le b<d}} (-1)^a \exp(2\pi i\tau(ar+bm,dm)) = \begin{cases} -\exp(2\pi in\tau(r,m)), & \text{if } g=n(r,m); \\ 2\exp(\pi ikn\tau(r,m)), & \text{if } g=n(m,r)/2; \\ 0, & \text{otherwise.} \end{cases}$$

where $g = (ar+bm,dm)$, and $2k \equiv 1(\mod m')$.

2. *If m' and n are even, then*

$$\sum_{\substack{ad=n \\ 0\le b<d}} (-1)^a \exp(2\pi i\tau(ar+bm,dm)) = \begin{cases} -\exp(2\pi in\tau(r,m)), & \text{if } g=n(r,m); \\ 0, & \text{otherwise.} \end{cases}$$

where also $g = (ar+bm,dm)$.

Proof. 1. Since m is odd, $m' = m/(m,r)$ is also odd, so there are integers $x,\ y$ such that $m'y + 2r'x = 1$, $r' = r/(m,r)$, i.e.

$$A = \begin{pmatrix} m' & -r' \\ 2x & y \end{pmatrix} \in \Gamma_0(2).$$

Therefore, by the previous lemma, we get

$$h_n(r/m + t) = h_n\left(A(r'/m' + 1)\right) = h_n\left(\frac{mm't}{(m,r) + 2xmt}\right)$$

$$= -\exp(4\pi i x n/m)\exp(2\pi i n/m'^2 t)$$

$$+2\exp(\pi x n/m')\exp(\pi i n/2m'^2 t) + o(1),$$

and

$$h_n(r/m + t) = \sum_{\substack{ad=n \\ 0\le b<d}} (-1)^a j\left(\frac{ar + bm}{dm} + \frac{at}{d}\right)$$

$$= \sum_{\substack{ad=n \\ 0\le b<d}} \exp(2\pi i\tau(ar + bm, dm))\exp(2\pi i g^2/tnm^2) + o(1)$$

where $g = (ar + bm, dm)$. The result follows by comparing the coefficients.

2. Similarly, as in (1) and since m' is even there exist $x,\ y \in \mathbb{Z}$ so that $\begin{pmatrix} x & y \\ -m' & r' \end{pmatrix} \in \Gamma_0(2)$. Once again, the result follows by computing $h_n(r'/m' + t)$ in two ways, as we did for (1).

□

Lemma 4.2.7. *For any $r,\ m,\ n \in \mathbb{Z}$, $m, n > 0$, and a positive divisor k of n, there exists a matrix*

$$S = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $ad = n,\ 0 \le b < d$ such that

$$(ar + bm, dm) = k(m,r).$$

Proof. Let $u_1,\ u_2,\ v_1$, and v_2 be such that $m = u_1 n + v_1,\ r = u_2 n + v_2$ so that

$$mv_2/(v_1, v_2) - u_1 v_2 n/(v_1, v_2) = lcm(v_1, v_2) = rv_1/(v_1, v_2) - u_2 v_1 n/(v_1, v_2).$$

Set $e = v_1/(v_1, v_2)$ and $f = -v_2/(v_1, v_2)$, so that $(e, f) = 1$. Thus, there are integers $g,\ h$ such that $\begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Next, let $S' = \begin{pmatrix} n/k & 0 \\ 0 & k \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, and $S' \begin{pmatrix} r \\ m \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$. Then, $(p, q) = k(m, r)$. Finally, by Proposition 3.4.1 in chapter 3, there exists $B \in \mathrm{SL}_2(\mathbb{Z})$ such that $S = BS'$ is upper triangular. □

Now, we proceed to the main theorem of this section.

Theorem 4.2.8. *If f is a Haupmodul with rational coefficients for a subgroup G of $PSL_2(\mathbb{R})$ such that G has genus zero, contains a $\Gamma_0(N)$ with finite index, and the transformations $z \mapsto z + k$ if and only if $k \in \mathbb{Z}$, i.e. G is of Moonshine type, then f is replicable.*

Proof. We will prove by induction on n that the n-th replicate $f^{(n)}$ of f exists, has no singularities in the upper half plane, and is invariant for $\Gamma(K)$, for some M, and also that $f^{(n)}$ satisfies

$$f^{(n)}(r/m + t) = \xi(nm')^{n\tau(r,m)} \exp(A(nm')n^2/t) + o(1)$$

where ξ is as in definition 4.2.1.
For $n = 1$, $f^{(1)} = f$, so we only need to verify the property

$$f(r/m + t) = \xi(m')^{\tau(r,m)} \exp(A(m')/t) + o(1).$$

We distinguish the following cases, according to Proposition 4.2.2, (3).

- If $\xi(m')$ is a primitive m'-th root of unity, this is the case $\psi = \phi = 1$, then the result follows from Proposition 4.2.2, (2).

- If $\psi = 2$, then $\phi = 1$ and $\xi(m')$ is a primitive $m'/2$-th root of unity. Once again, by Proposition 4.2.2, (2), the result follows.

- If $\phi = 2$, then $\psi = 1$ and $\xi(m')$ is a primitive $2m'$-th root of unity, and the result follows from Proposition 4.2.2, (2), except if m' is odd. However, in this case, by Proposition 4.2.2, (2), we have

$$f(r/m + t) = f(r'/m' + t) = \exp(4\pi i\delta k/2\nu)\exp(A(m')/t) + o(1),$$

where k is an integer such that $kr' \equiv 1(\mod \lambda m')$ and $k \equiv 1 \mod (2)$. We take $\tau(r, m) = k/m'$, then the result follows (recall our definition of $\tau(r, m)$).

Now, assume the result true for all $a < n$, in fact we need only that it holds for all proper divisors a of n and let us prove the result for $f^{(n)}$. Let

$$Q_n(z) = F_n(f(z)) - {\sum_{\substack{ad=n \\ 0\le b<d}}}' f^{(a)}\left(\frac{az+b}{d}\right). \tag{17}$$

We have to show that $Q_n(z + 1/n) = Q_n(z)$ so $f^{(n)}(z) = Q_n(z/n)$ has integral q-expansion, i.e. $f^{(n)}$ exists. From above we have

$$F_n(f(r/n + t)) = \xi(m')^{nm'\tau(r,m)}\exp(A(m')n/t) + o(1).$$

By the induction hypothesis, we have

$${\sum_{\substack{ad=n \\ 0\le b<d}}}' f(a)(\frac{ar+bm}{dm} + \frac{at}{d}) = \sum_{\substack{ad=n \\ 0\le b<d}} \xi(nm/g)^{(mn/g)\tau(ar+bm,dm)}\exp(A(mn/g)n/t)$$

$$-\xi(nm/(m, nr))^{(nm/(m,nr))\tau(nr,m)}\exp(A(nm/(m, nr))n/t) + o(1).$$

As for $f^{(1)}$, we have the following cases

- If $\xi(nm/g)$ is a primitive nm/g-th root of 1, we have by Lemma 4.2.7 there are integers a', b', d' such that $(a'r + b'm, d'm) = n(m, r)$, and so by Lemma 4.2.3

$$\sum_{\substack{ad=n \\ 0\le b<d}} \xi(nm/g)^{(mn/g)\tau(ar+bm,dm)}\exp(A(mn/g)n/t)$$

$$= \xi(m')^{m'\tau(a'r+b'm,d'm)}\exp(A(m')n/t).$$

Therefore, applying a Galois automorphism, namely the one that maps $\xi(m')^{m'\tau(a'r+b'm,d'm)}$ to $\xi(m')^{nm'\tau(r,m)}$,

$$\sum_{\substack{ad=n\\0\le b<d}} \xi(nm/g)^{(mn/g)\tau(ar+bm,dm)} \exp(A(mn/g)n/t)$$

$$= \xi(m')^{nm'\tau(r,m)} \exp(A(m')n/t)$$

and the result follows.

- If $\xi(nm/g)$ is a $2nm/g$-th or $nm/2g$-th root of 1. In this case $-\xi(nm/g)$ is a primitive nm/g-th root of 1, similarly as above, by Lemma 4.2.7 and Lemma 4.2.6, (2), we obtain

$$\sum_{\substack{ad=n\\0\le b<d}} \xi(nm/g)^{(mn/g)\tau(ar+bm,dm)} \exp(A(mn/g)n/t)$$

$$= \xi(m')^{m'\tau(a'r+b'm,d'm)} \exp(A(m')n/t),$$

except in the case that n is even and m' is odd. However in this case, by Lemma 4.2.7, and Lemma 4.2.6, (1), we have

$$\sum_{\substack{ad=n\\0\le b<d}} \xi(nm/g)^{(mn/g)\tau(ar+bm,dm)} \exp(A(mn/g)n/t)$$

$$= -\xi(m')^{nm'\tau(r,m)} \exp(A(m')n/t) - 2\xi(2m')^{hnm'\tau(r,m)} \exp(A(2m')n/t),$$

where $2h \equiv 1(\mod m')$. However,

$$\begin{pmatrix} 2\lambda\delta & \epsilon \\ -2\lambda m' & \lambda \end{pmatrix}$$

is a matrix that maps $2m'$ to ∞, so $\xi(2m') = -\exp(2\pi i\delta/m')$ and $A(2m') = A(m')$. Once again, we find

$$\sum_{\substack{ad=n\\0\le b<d}} \xi(nm/g)^{a\tau(ar+bm,dm)} \exp(A(mn/g)n/t) = \xi(m')^{n\tau(r,m)} \exp(A(m')n/t)$$

and the result follows.

Therefore,

$$Q_n(r/m+t) = \xi(nm/(nr,m))^{(nm/(m,nr))\tau(nr,m)} \exp(A(nm/(nr,m))/t) + o(1).$$

Now, since the above expression is invariant under the substitution $r \mapsto rn + m$, $m \mapsto mn$,

$$Q_n(r/m+t) - Q_n(r/m+1/n+t) = o(1).$$

Hence, this difference is bounded on $\mathbb{Q}$. At infinity

$$Q_n(z) = \exp(-2\pi i n z) + o(1)$$

and so the difference is bounded at infinity.
Now, by hypothesis the right hand side of equation (4) is holomorphic on $\mathbb{H}$, $Q_n(z)$ is holomorphic too. Also $Q_n(z)$ is invariant under the intersection of the fixing group of each term on the right hand side each of of which contain a principal congruence group, say $\Gamma(M)$, for some M. Thus $Q_n(z) - Q_n(z+1/n)$ is invariant under $\Gamma(n^2M)$, bounded on a fundamental domain, so by Theorem 2.1.1 of chapter 2 this difference is constant, and the constant equals zero.
Finally, take $f^{(n)} = Q_n(z/n)$, then $f^{(n)}$ verifies the property

$$f^{(n)}(r/m+t) = \xi(nm')^{n\tau(r,m)} \exp(A(nm')n^2/t) + o(1)$$

also $f^{(n)}$ is a modular function with no poles on the upper half plane $\mathbb{H}$. □

4.3 FURTHER DEVELOPMENTS

The question on whether replicable functions are modular seems to be a difficult one. If we are provided with a specific replicable function, then it is not difficult to check its modularity because of the dependence of both types of functions on the first few coefficients. In 1994, Y. Martin provided a proof of the modularity of the completely replicable functions, which has been widely cited in the literature. However, while we were reviewing the details of the proof during the preparation of this thesis, my advisor and I noticed that Proposition 16 in [14] on which the final argument relies entirely

is completely false. This leaves the converse of Norton's conjecture completely open. We are trying to develop further techniques from the theory of differential equations to try to prove this conjecture.

Bibliography

[1] D. Alexander, C. Cummins, J. McKay, C. Simons, *Completely replicable functions. Groups, combinatorics and geometry (Durham, 1990), 87–98, London Math. Soc. Lecture Note Ser., 165, Cambridge Univ. Press, Cambridge, 1992.*

[2] T.M. Apostol, *Modular Functions and Dirichlet Series in Number Theory* , Springer-Verlag, 2nd ed., 1990.

[3] R.E Borcherds, *Monstrous moonshine and monstrous Lie superalgebras* Invent. Math. 109 (1992), no. 2, 405–444.

[4] R.E Borcherds, *What is Moonshine?*, Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998).

[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *Atlas of finite groups*, Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985

[6] J.H. Conway, S.P. Norton, *Monstrous moonshine*, Bull. London Math. Soc. 11 (1979), no. 3, 308–339.

[7] J. Conway, J. McKay, A. Sebbar, *On the discrete groups of Moonshine.* Proc. Amer. Math. Soc. 132 (2004), no. 8, 2233–2240 (electronic).

[8] C. Cummins, *Some comments on replicable functions.* Modern trends in Lie algebra representation theory (Kingston, ON, 1993), 48–55, Queen's Papers in Pure and Appl. Math., 94, Queen's Univ., Kingston, ON, 1994.

[9] C. Cummins, T. Gannon, *Modular equations and the genus zero property of moonshine functions*, Invent. Math. 129 (1997), no. 3, 413–443.

[10] C. Cummins, S.P. Norton, *Rational Hauptmoduls are replicable*, Canad. J. Math. 47 (1995), no. 6, 1201–1218.

[11] D. Ford, J. McKay, S.P. Norton, *More on replicable functions*, Comm. Algebra 22 (1994), no. 13, 5175–5193.

[12] T. Gannon, *Monstrous Moonshine: The first twenty-five years*, arXiv:math.QA/0402345 v2 14 Apr 2004. 2004.

[13] S. Lang, *Elliptic Functions, with an appendix by J. Tate.* Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.

[14] Y. Martin, *On modular invariance of completely replicable functions*, Moonshine, the Monster, and related topics (South Hadley, MA, 1994), 263–286, Contemp. Math., 193, Amer. Math. Soc., Providence, RI, 1996.

[15] G. Mason, *Finite groups and modular functions. With an appendix by S. P. Norton*, Proc. Sympos. Pure Math., 47, Part 1, The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), 181–210, Amer. Math. Soc., Providence, RI, 1987.

[16] J. McKay, A. Sebbar, *Fuchsian groups, automorphic functions and Schwarzians*, Math. Ann. 318 (2000), no. 2, 255–275.

[17] J. McKay, A. Sebbar, *Replicable Functions: An Introduction*, preprint.

[18] J. McKay, H. Strauss, *The q-series of monstrous moonshine and the decomposition of the head characters*, Comm. Algebra 18 (1990), no. 1, 253–278.

[19] J.S. Milne, *Modular Functions and Modular Forms*, University of Michigan, 1990.

[20] S.P. Norton, *More on moonshine*, Computational group theory (Durham, 1982), 185–193, Academic Press, London, 1984.

[21] S.P. Norton, *Non-Monstrous Moonshine*, Groups, difference sets, and the Monster (Columbus, OH, 1993), 433–441, Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin, 1996.

[22] A.P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449–462.

[23] A.P. Ogg, *Automorphismes de courbes modulaires*, (French) Sminaire Delange-PisotPoitou (16e anne: 1974/75), Thorie des nombres, Fasc. 1, Exp. No. 7, 8 pp. Secrtariat Mathmatique, Paris, 1975.

[24] A.P Ogg, *Modular functions*, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), pp. 521–532, Proc. Sympos. Pure Math., 37, Amer. Math. Soc., Providence, R.I., 1980.

[25] R.A. Rankin, *Modular forms and functions.* Cambridge University Press, 1977. MR **58**:16518

[26] A. Sebbar, *Torsion-free genus zero congruence subgroups of* $\mathrm{PSL}_2(\mathbb{R})$. Duke Math. J. 110 (2001), no. 2, 377–396.

[27] A. Sebbar, *Classification of torsion-free genus zero congruence groups.* Proc. Amer. Math. Soc. 129 (2001), no. 9, 2517–2527 (electronic).

[28] G. Shimura, *Introduction to the Arithmethic Theory of Automorphic Functions*, Princeton University Press, Princeton, New Jersey, 1971. MR **47**:3318