Canad. Math. Bull. Vol. **45** (1), 2002 pp. 36–45

Modular Equations and Discrete, Genus-Zero Subgroups of $\mathrm{SL}(2,\mathbb{R})$ Containing $\Gamma(N)$

C. J. Cummins

Abstract. Let G be a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ which contains $\Gamma(N)$ for some N. If the genus of $X(G)$ is zero, then there is a unique normalised generator of the field of G-automorphic functions which is known as a normalised Hauptmodul. This paper gives a characterisation of normalised Hauptmoduls as formal q series using modular polynomials.

1 Introduction

Let G be a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ which contains $\Gamma(N)$ for some N. The index of $\Gamma(N)$ in G is necessarily finite and G acts on the extended upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$ (*cf.* Lemma 3.2). The quotient $G \setminus \mathcal{H}^*$ has the structure of a compact Riemann surface and will be denoted by $X(G)$. If the genus of $X(G)$ is zero then there is a unique generator f of the field of G-automorphic functions which is analytic on $\mathcal{H}$ and which has Fourier expansion:

$$f = q^{-1/s} + a_1 q^{1/s} + a_2 q^{2/s} + \cdots, \quad q = e^{2\pi i z},\ a_i \in \mathbb{C},\ i = 1, 2, \ldots$$

where $s \in \mathbb{Q}^{>0}$ is called the *width of the cusp at infinity* (s is the smallest positive rational such that the transformation $z \mapsto z + s$ is in G). This function is called the *normalised Hauptmodul* of G.

The aim of this paper is to give a characterisation of these normalised Hauptmoduls as *formal* q series using modular polynomials, which are defined as follows: Given a formal q series of the form

$$h(q) = q^{-1} + \sum_{i=1}^{\infty} a_i q^i$$

with $a_i \in \mathbb{C}$, $i = 1, 2, \ldots$, a modular polynomial of order $n > 1$ for h is a polynomial $F_n(x, y) \in \mathbb{C}[x, y]$ such that:

(M.1) $F_n(x, y)$ is a monic polynomial of degree $\psi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} (1 + \frac{1}{p})$ in y.

(M.2) For all $a, b, d \in \mathbb{Z}$ such that $ad = n$, $\gcd(a, b, d) = 1$ and $0 \le b < d$, $F_n\big(h(q), h(\zeta_d^b q^{\frac{a}{d}})\big) = 0$ as formal $q^{1/d}$ series where $\zeta_d = e^{2\pi i/d}$.

Received by the editors October 10, 1998.
The author was supported by NSERC and FCAR grants.
AMS subject classification: 11F03, 11F22, 30F35.
©Canadian Mathematical Society 2002.

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

It follows from these properties that $F_n(x, y) = F_n(y, x)$ (see [K]). An equivalent, and sometimes more convenient, property of $h(q)$ is that $\prod\bigl(y - h(\zeta_d^b q^{a/d})\bigr)$ is a polynomial in y and $h(q)$ where the product is taken over all $a, b, d \in \mathbb{Z}$ such that $ad = n$, $\gcd(a, b, d) = 1$ and $0 \le b < d$.

If $h(q)$ has a modular polynomial of order n then we also say that $h(q)$ satisfies a modular equation of order n. If the coefficients of $h(q)$ are the Fourier coefficients of a function $f(z)$ which is analytic on the upper half plane so that $f(z) = h(e^{2\pi i z})$ then we also call $F_n(x, y)$ a modular polynomial for $f(z)$ and say that $f(z)$ satisfies a modular equation of order n.

Modular equations for the j function, the normalised Hauptmodul for $\mathrm{SL}(2, \mathbb{Z})$, have a long history, see for example [Sh, Section 4.6], [L, Chapter 5 Section 2], [C]. Modular equations for the Hauptmoduls arising in moonshine have also be studied [Mar, CY].

In [CG] it was shown that normalised Hauptmoduls for discrete, genus-zero subgroups of $\mathrm{SL}(2, \mathbb{R})$ containing some $\Gamma_0(N)$ and such that the width of the cusp at infinity is 1, may be characterised by the property of satisfying a modular equation of order n for all $n \equiv 1 \pmod{N}$. By a Theorem of Thompson [T] there are only finitely many such groups.

Theorems 1.1 and 1.2 extend these results to the general case described above. If G contains $\Gamma(N)$ then, as is shown in Lemma 1.4, a conjugate of G contains $\Gamma_1(N') = \bigl\langle \Gamma(N'), \bigl(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\bigr) \bigr\rangle$ for some N' and has width 1 at infinity. So without loss of generality we can consider the case when G is a discrete, genus-zero subgroup of $\mathrm{SL}(2, \mathbb{R})$ which contains $\Gamma_1(N)$ for some N and such that the width of the cusp at infinity is 1. Unlike the $\Gamma_0(N)$ case there are infinitely many such groups.

In order to state the main result we introduce some notation. Given a meromorphic function f defined on the upper half plane $\mathcal{H}$, let

$$G(f) = \bigl\{ m \in \mathrm{SL}(2, \mathbb{R}) \mid f\bigl(m(z)\bigr) = f(z) \bigr\}.$$

For a positive integer K let $\mathcal{X}_K$ be the set of positive integers n such that all positive divisors of n are congruent to 1 modulo K.

Theorem 1.1 *Let $h(q) = q^{-1} + \sum_{i=1}^{\infty} a_i q^i$ $a_i \in \mathbb{C}$, $i = 1, 2, \ldots$ be a formal q series and let $K > 0$ be an integer. Suppose $h(q)$ satisfies a modular equation of order n for all $n \in \mathcal{X}_K$. Then $f(z) = h\bigl(\exp(2\pi i z)\bigr)$ is analytic on the upper half plane, $G(f)$ is a discrete subgroup of* $\mathrm{SL}(2, \mathbb{R})$ *and*

(A) *if $G(f) \neq \Bigl\{ \pm \bigl(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\bigr) \Bigm| t \in \mathbb{Z} \Bigr\}$ then*

- (a) *$G(f)$ contains $\Gamma_1(N)$ for some N with N coprime to any element of $\mathcal{X}_K$,*
- (b) *$G(f)$ contains $\bigl(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\bigr)$ if and only if $k \in \mathbb{Z}$,*
- (c) *the genus of $X\bigl(G(f)\bigr)$ is zero,*
- (d) *f is a normalised Hauptmodul for $G(f)$;*

(B) *if $G(f) = \Bigl\{ \pm \bigl(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\bigr) \Bigm| t \in Z \Bigr\}$ and the coefficients a_i, $i = 1, 2, \ldots$ are algebraic integers, then $f(z) = q^{-1} + \zeta q$ with $\zeta^{dK+1} = \zeta$ where $d = 1$ if $K = 1$ and $d = \gcd(K-1, 2)K$ otherwise.*

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

Theorem 1.2

(1) *If f is a normalised Hauptmodul for a discrete, genus-zero subgroup G of* $\mathrm{SL}(2,\mathbb{R})$ *satisfying:*

- (a) *G contains $\Gamma_1(N)$ for some N,*
- (b) *G contains $\left(\begin{smallmatrix}1&k\\0&1\end{smallmatrix}\right)$ if and only if $k \in \mathbb{Z}$,*
- (c) *H is a subfield of $\mathbb{Q}(\zeta_N)$, where H is the field generated over $\mathbb{Q}$ by the coefficients of f,*

then there exists a modular polynomial $F_n(x,y)$ for f of order n for all $n \in \mathcal{X}_N$. Also $F_n(f,y)$ is irreducible over $\mathbb{C}(f)$.

(2) *Let $K > 0$ be an integer. If $f = q^{-1} + \zeta q$ where $\zeta^{K+1} = \zeta$, then there exists a modular polynomial for f of order n for all $n \in \mathcal{X}_K$.*

It should perhaps be noted that in [CG] it was shown that in the case of Hauptmoduls for groups containing $\Gamma_0(N)$ it is possible to introduce "generalised" modular polynomials $F_n(x,y)$ when $n \not\equiv 1 \pmod{N}$. In general this does not seem to be possible. See Section 3 for a discussion of this point.

The results of [CG] were motivated by Borcherds' proof [BR] of the moonshine conjectures of Conway and Norton [CN]. The denominator formula for the Monster Lie algebra implies that the Monstrous moonshine functions satisfy modular equations of order n for all n coprime to the order of the Monster group and so these functions are normalised Hauptmoduls. In generalised [N] and modular moonshine [BR] it is more difficult to show that the functions which arise are Hauptmoduls and part of the motivation for this paper is to give weaker conditions under which formal series are known to be Hauptmoduls. It seems probable that further progress can be made in this direction. Cohn and McKay [CM] have used a computer to find all the formal series of the form given in Theorem 1.1 which satisfy modular equations of order 2 and 3 with the restriction that the coefficients are rational integers. Based on this they conjecture that given any two primes p_1 and p_2 there are only finitely many series which satisfy modular equations of order p_1 and p_2. Theorems 1.1 and 1.2 suggest a more precise conjecture:

Conjecture 1.3 *Let $h(q) = q^{-1} + \sum_{i=1}^{\infty} a_i q^i$ $a_i \in \mathbb{C}$, $i = 1, 2, \ldots$ be a formal q series and let p_1 and p_2 be any two distinct primes. Suppose $h(q)$ satisfies modular equations of order p_1 and p_2. Then $f(z) = h\big(\exp(2\pi i z)\big)$ is analytic on the upper half plane, $G(f)$ is a discrete subgroup of* $\mathrm{SL}(2,\mathbb{R})$ *and*

(A) *if $G(f) \neq \left\{\pm\left(\begin{smallmatrix}1&t\\0&1\end{smallmatrix}\right) \,\middle|\, t \in \mathbb{Z}\right\}$ then*

- (a) *$G(f)$ contains $\Gamma_1(N)$ for some N with p_1 and p_2 coprime to N,*
- (b) *$G(f)$ contains $\left(\begin{smallmatrix}1&k\\0&1\end{smallmatrix}\right)$ if and only if $k \in \mathbb{Z}$,*
- (c) *the genus of $X\big(G(f)\big)$ is zero,*
- (d) *f is a normalised Hauptmodul for $G(f)$;*

(B) *if $G(f) = \left\{\pm\left(\begin{smallmatrix}1&t\\0&1\end{smallmatrix}\right) \,\middle|\, t \in Z\right\}$ then $f(z) = q^{-1} + \zeta q$ with $\zeta^{\gcd(p_1-1,p_2-1)+1} = \zeta$.*

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

We conclude this introduction with the Lemma mentioned above: Let 1_2 denote the identity 2×2 matrix and for any subgroup G of $\mathrm{SL}(2,\mathbb{R})$ define G_∞ to be the subgroup of G which fixes $i\infty$.

Lemma 1.4 *If G is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ which contains $\Gamma(N)$ for some N then G is conjugate to a group G' which contains $\Gamma_1(N')$ for some N' and such that the width of the cusp $i\infty$ is 1.*

Proof By [Sh Proposition 1.17], $G_\infty = \big\langle (G \cap \{\pm 1_2\}), \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \big\rangle$, with $h \in \mathbb{R}$. As $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in G$ we have $h = N/t \in \mathbb{Q}$, for some $t \in \mathbb{Z}$. Let $\alpha = \left(\begin{smallmatrix} N/t & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so $(\alpha^{-1}G\alpha)_\infty = \big\langle (G \cap \{\pm 1_2\}), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \big\rangle$ and $\alpha^{-1}G\alpha \supseteq \alpha^{-1}\Gamma(N)\alpha \supseteq \Gamma(tN^2)$. Since $\Gamma_1(tN^2)$ is generated by $\Gamma(tN^2)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ the result follows. ■

Acknowledgements I thank Terry Gannon for many useful comments.

2 Proof of Theorem 1.1

Mahler [Mah, Theorem 8] has shown that if $h(q)$ satisfies a modular equation for some prime p, then it is the Laurent expansion of a meromorphic function defined in some neighbourhood of $q = 0$. Kozlov [K, Proposition 3.3, see also CG Section 2] shows that if $h(q)$ satisfies a modular equation of order p for infinitely many primes p, then it is the Laurent expansion of a function analytic on the interior of the unit disc $|q| < 1$, except for a pole at $q = 0$ and so if $h(q)$ is a formal q series satisfying the hypotheses of Theorem 1.1 then $f(z) = h\big(\exp(2\pi i z)\big)$ is an analytic function on the upper half plane. This shows the first part of Theorem 1.1.

In outline the proof of Theorem 1.1B is similar to the corresponding result of [CG]. In particular the results of Sections 2, 3 and 4 of [CG] require only that $f(z)$ satisfies a modular equation for infinitely many primes and so these results continue to hold in the case under consideration. It follows from these results that f has the following property (**P**): if $z_1, z_2 \in \mathcal{H}$ and $f(z_1) = f(z_2)$ then there exists $g \in G(f)$ such that $g(z_1) = z_2$. The next step is to show that $G(f)$ contains some $\Gamma_1(N)$. The key result is the following [*cf.* CG Proposition 5.1]:

Proposition 2.1 *Let G be a subgroup of $\mathrm{SL}(2,\mathbb{R})$ and K be a positive integer. Suppose*

(1) *G is a discrete subgroup.*
(2) *$G_\infty = \big\langle -1_2, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \big\rangle$.*
(3) *For all $n \in \mathcal{X}_K$ and all $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, there exist integers ℓ and k such that $\ell | n$, $0 \le -k < n/\ell$ and such that*

$$\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \begin{pmatrix} \ell & -k \\ 0 & n/\ell \end{pmatrix}^{-1} = \begin{pmatrix} na/\ell & ka+\ell b \\ c/\ell & (kc+\ell d)/n \end{pmatrix} \tag{2.1}$$

is in G.

Then either $G = \big\langle -1_2, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \big\rangle$ or G contains $\pm\Gamma_1(N)$ where $K|N$.

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

Proof For any discrete subgroup G of $\mathrm{SL}(2,\mathbb{R})$ there is an $r > 0$ such that if $m = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in G$ and $c' \neq 0$ then $|c'| > r$ (see [Sh, p. 11]). We shall use the following result which follows from the proof of [CG, Lemma 5.7 c]: If G satisfies the hypotheses of this proposition and G contains an element $\left(\begin{smallmatrix} a & * \\ c & pd \end{smallmatrix}\right)$ where $p \in \mathfrak{X}_K$ is a prime such that $|c|/r < p$ then G contains an element of the form $\left(\begin{smallmatrix} pa & * \\ c & d \end{smallmatrix}\right)$.

If all $m \in G$ fix $i\infty$ then $G = \left\langle -1_2, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$. Otherwise, using an identical argument to the start of the proof of [CG, Proposition 5.1], G contains $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G \cap \mathrm{SL}(2,\mathbb{Z})$ such that $K|c$, $c \neq 0$, c coprime to any element of $\mathfrak{X}_K$ and $d \equiv 1 \pmod{K}$.

As c and d are coprime, by considering $m\left(\begin{smallmatrix} 1 & kK \\ 0 & 1 \end{smallmatrix}\right)$ for a suitable choice of k we find, by Dirichlet's Theorem, that G contains $g = \left(\begin{smallmatrix} a & * \\ c & p \end{smallmatrix}\right)$ with p a prime with $p \equiv 1 \pmod{K}$ and $p > |c|/r$. Thus G contains $\left(\begin{smallmatrix} ap & * \\ c & 1 \end{smallmatrix}\right)$. All operations used preserve determinants, hence, pre-multiplying by a suitable translation, we see that G contains $\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right)$.

Consider any nonzero $a, b \in \mathbb{Z}$ with $\gcd(a, bc) = 1$ and $a \equiv 1 \pmod{c}$ and hence $a \equiv 1 \pmod{K}$ since $K|c$. Choose any prime $q > |bc|/r$, such that $q \equiv a \pmod{bc}$. Then $q \in \mathfrak{X}_K$. From above $G \cap \mathrm{SL}(2,\mathbb{Z})$ contains $\left(\begin{smallmatrix} 1 & 0 \\ bc & 1 \end{smallmatrix}\right)$ and so by post-multiplying by a suitable translation $G \cap \mathrm{SL}(2,\mathbb{Z})$ also contains an element of the form $\left(\begin{smallmatrix} 1 & * \\ bc & q* \end{smallmatrix}\right)$. Again using the result at the start of this proof, $G \cap \mathrm{SL}(2,\mathbb{Z})$ contains an element of the form $\left(\begin{smallmatrix} q & * \\ bc & * \end{smallmatrix}\right)$ and hence also $\left(\begin{smallmatrix} a & * \\ bc & * \end{smallmatrix}\right)$. As these matrices together with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (and if $|c| = 1$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$) are a complete set of coset representatives for the subgroup $\left\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$ in $\Gamma_1(c)$ the result follows with $N = c$. ■

Proof [**(of Theorem 1.1A)**] The proof of [CG, Lemma 7.1] shows that $G(f)$ is a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. Thus by [Sh Proposition 1.17] $G_\infty = \left\langle \pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$ and as f has a simple pole at infinity we have $G_\infty = \left\langle \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$. So if $G \neq G_\infty$ then G contains an element $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \neq 0$. From Proposition 2.1 and [CG Lemma 7.1] $G(f)$ contains $\Gamma_1(N)$ for some N, with $K|N$ and N coprime to any element of $\mathfrak{X}_K$.

Thus $f(z)$ gives rise to a function $\hat{f}$ on $X(G)$ that is analytic except possibly at the cusps. At the cusp corresponding to infinity $\hat{f}$ has a simple pole. By property (**P**) (see above) at the other cusps, if any, $\hat{f}$ is bounded and hence has removable singularities. It follows that f is an automorphic function. Again by property (**P**) $\hat{f}$ maps $X(G)$ isomorphically to a subset of the Riemann sphere and since $X(G)$ is compact this must be the whole of the Riemann sphere. Thus the genus of $X(g)$ is zero and f is a Hauptmodul for G, as required. ■

To prove Theorem 1.1B we need the following:

Lemma 2.2 *Let f and K be as in as in Theorem 1.1 and suppose $G(f)$ is trivial (i.e. consists only of translations by integers) and that all the coefficients a_i of f are algebraic integers. Then $f(z) = q^{-1} + \zeta q$ where $\zeta^{dK+1} = \zeta$, $q = \exp(2\pi i z)$ where $d = 1$ if $K = 1$ and $d = \gcd(K-1, 2)K$ otherwise.*

Proof If $f = q^{-1}$ then we are done, so assume otherwise. The same proof as in [CG: Proposition 7.2] shows that $f(z) = q^{-1} + \zeta q$ with $|\zeta| = 1$, $q = \exp(2\pi i z)$. For any

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

prime $p \equiv 1 \pmod{K}$ the sum of the zeros of the modular equation $F_p\big(f(z), x\big) = 0$ is a polynomial in $f(z)$. This gives

$$1/q^p + \zeta q^p = Q_{p,f}(f)$$

where $Q_{p,f}$ is the unique polynomial such that

$$Q_{p,f}\big(f(q)\big) = q^{-p} + \text{terms of positive degree}$$

Comparing the coefficients of q^p shows that $\zeta^p = \zeta$. If $K = 1$ then we have $\zeta^2 = \zeta^3 = 1$ and so $\zeta = 1$ as require. If $K > 1$ then by Dirichlet's Theorem there is some integer r such that $p = rdK + 1$ with p a prime. Since dK is even there is an integer t such that $\gcd(r, t) = 1$ and $tdK + 1 \equiv -1 \pmod{\ell}$ for all (necessarily odd) primes ℓ such that $\ell | r$ and $\ell \nmid dK$ and hence $\gcd(rdK, tdK + 1) = 1$. So again by Dirichlet's Theorem there is an integer r' such that $p' = r'(rdK) + tdK + 1$ is a prime. Since $p, p' \in \mathcal{X}_K$ we have $\zeta^{rdK} = \zeta^{r'rdK+tdK} = 1$ and hence $\zeta^{dK} = 1$, since $\gcd(r, r'r + t) = 1$, as required. ■

This completes the proof of Theorem 1.1B.

3 Proof of Theorem 1.2

In this section if m is a nonsingular 2×2 integer matrix with positive determinant then $\langle m \rangle$ will denote the corresponding element of $\mathrm{PGL}(2, \mathbb{Q})^+$. For any such m we have $m = \lambda m'$ where m' is a primitive integer matrix and m' is unique up to a sign. Write $|m| = \det(m')$.

For any positive integer n define $A(n) = \{\langle \begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix} \rangle \bigm| ad = n, \gcd(a, b, d) = 1, 0 \leq b < d\}$. Also fix $\beta_n = \langle \begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix} \rangle$.

Let $\mathcal{F}_N$ be the field of automorphic functions of $\Gamma(N)$ with Fourier coefficients in $\mathbb{Q}(\zeta_N)$ (See [Sh, Chapter 6]). For n coprime to N, $*n$ will denote the Galois automorphism of $\mathbb{Q}(\zeta_N)$ such that $\zeta_N * n = \zeta_N^n$. In the rest of this section f will be a non-constant element of $\mathcal{F}_N$ and $f * n$ will be the function obtained by applying $*n$ to the Fourier coefficients of f. Where no confusion can arise we shall write G for $G(f)$ and $G * n$ for $G(f * n)$.

For proofs of the following two Lemmas see [CG; Section 6]:

Lemma 3.1 *G is a discrete subgroup of* $\mathrm{SL}(2, \mathbb{R})$ *which contains* $\Gamma(N)$ *with finite index.*

Lemma 3.2 *There is a group homomorphism $\phi \colon G \to$* $\mathrm{PGL}(2, \mathbb{Q})^+$ *with* $\ker(\phi) = \{\pm 1_2\}$. *$\bar{G} = \phi(G)$ is a discrete subgroup of* $\mathrm{PGL}(2, \mathbb{Q})^+$.

Let $T = \big\{\big(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\big) \in \mathrm{SL}(2, \mathbb{R}) \mid t \in \mathbb{Z}\big\}$ and $\bar{T} = \phi(T)$. For each integer a coprime to N fix an element $\sigma_a \in \mathrm{SL}(2, \mathbb{Z})$ such that $\sigma_a \equiv \big(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\big) \pmod{N}$. For $\alpha = \big\langle \begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix} \big\rangle \in A(n)$ we also write σ_α for σ_a.

Proposition 3.3 *Let n be any integer coprime to N. If G contains $\Gamma_1(N)$, then the following are equal:*

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

(1) $\bigcup_{\alpha\in A(n)} \bar{G}\sigma_\alpha\alpha$
(2) $\bigcup_{\alpha\in A(n)} \bar{T}\alpha\sigma_\alpha\overline{G*n}$
(3) $\bigcup_{\alpha\in A(n)} \bar{T}\sigma'_\alpha\alpha\overline{G*n}$
(4) $\bar{\Gamma}_1(N)\beta_n\overline{G*n}$.

where $\sigma'_a \in \mathrm{SL}(2,\mathbb{Z})$ *also satisfies* $\sigma'_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \pmod N$, *but is not necessarily equal to* σ_a.

Proof We begin by showing that these sets are equal when $G*n$ and G are replaced by $\Gamma_1(N)$. The equality

$$(3.1).\qquad \bigcup_{\alpha\in A(n)} \overline{\Gamma_1(N)}\sigma_\alpha\alpha = \overline{\Gamma_1(N)}\beta_n\overline{\Gamma_1(N)}$$

follows from [Sh, Propositions 3.36 and 3.32(1)] and the observation that a matrix $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $ad = n$, $a > 0$, has the same elementary divisors as β iff $\gcd(a,b,d) = 1$. Shimura's Propositions also show that the two sets are equal to:

$$\Delta = \Big\{ \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_{2\times 2}(\mathbb{Z}) \mid \\ \det(\alpha) = n, a \equiv 1 \pmod N, c \equiv 0 \pmod N, \gcd(a,b,c,d) = 1 \Big\}.$$

From the definition of σ_a it follows that

$$\bigcup_{\alpha\in A(n)} \bar{T}\alpha\sigma_\alpha\overline{\Gamma_1(N)} \subseteq \Delta = \bigcup_{\alpha\in A(n)} \overline{\Gamma_1(N)}\sigma_\alpha\alpha.$$

Conversely for any $\alpha \in A(n)$ and $\gamma_1 \in \Gamma_1(N)$ we have from [CG, Proposition 6.8] that $\gamma_1\sigma_\alpha\alpha = t\alpha'\gamma_0$ for some $t \in \bar{T}$, $\alpha' \in A(n)$ and $\gamma_0 \in \Gamma_0(N)$. Reducing modulo N we find that $\gamma_0 = \sigma_{\alpha'}\gamma'_1$ for some $\gamma'_1 \in \Gamma_1(N)$. This establishes the equality

$$\bigcup_{\alpha\in A(n)} \overline{\Gamma_1(N)}\sigma_\alpha\alpha = \bigcup_{\alpha\in A(n)} \bar{T}\alpha\sigma_\alpha\overline{\Gamma_1(N)}$$

Again from [CG, Proposition 6.8] we have that for any $\alpha \in A(n)$, $\alpha\sigma_\alpha = \gamma\alpha'$ for some $\gamma \in \Gamma_0(N)$ and $\alpha' \in A(n)$. Reducing modulo N we find that we can write $\gamma = t\sigma'_{\alpha'}$ for some translation t and $\sigma'_{\alpha'} \equiv \begin{pmatrix} a'^{-1} & 0 \\ 0 & a' \end{pmatrix} \pmod N$. This shows $\bigcup_{\alpha\in A(n)} \bar{T}\alpha\sigma_\alpha\overline{\Gamma_1(N)} \subseteq \bigcup_{\alpha\in A(n)} \bar{T}\sigma'_\alpha\alpha\overline{\Gamma_1(N)}$ and the reverse inclusion again follows from the fact that $\bigcup_{\alpha\in A(n)} \bar{T}\sigma'_\alpha\alpha\overline{\Gamma_1(N)} \subseteq \Delta$.

To show equality in the general case, choose any $\alpha \in A(n)$ and $g \in \bar{G}$. By equation (3.1) we know $g\sigma_\alpha\alpha = gh\beta_n h'$ for some $h, h' \in \overline{\Gamma_1(N)}$. By [CG, Lemma 6.4] we may write $gh \in \bar{G}$ as $h''m$ where $m = \left\langle\begin{smallmatrix} a & nb \\ nc & d \end{smallmatrix}\right\rangle$, with $\left(\begin{smallmatrix} a & nb \\ nc & d \end{smallmatrix}\right)$ a primitive integer matrix and $h'' \in \overline{\Gamma_1(N)}$. Now $m\beta_n = \beta_n m'$ where $m' = \left\langle\begin{smallmatrix} a & n^2b \\ c & d \end{smallmatrix}\right\rangle \in \overline{G*n}$ by [CG, Corollary 6.7]. Thus we have shown that

$$\bigcup_{\alpha\in A(n)} \bar{G}\sigma_\alpha\alpha \subset \overline{\Gamma_1(N)}\beta_n\overline{G*n},$$

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

where we absorbed the h' because, by an argument identical to the proof of [CG, Corollary 6.6 **b**], $\overline{\Gamma_1(N)} \subseteq \overline{G * n}$. The reverse inclusion follows by identical arguments. Finally, the equalities

$$\bigcup_{\alpha\in A(n)} \bar{T}\alpha\sigma_\alpha\overline{\Gamma_1(N)} = \bigcup_{\alpha\in A(n)} \bar{T}\sigma'_\alpha\alpha\overline{\Gamma_1(N)} = \overline{\Gamma_1(N)}\beta_n\overline{\Gamma_1(N)},$$

have been established above and multiplying on the right by $\overline{G * n}$ gives the general result. ■

Corollary 3.4 *Let n be any integer such that every prime divisor of n is congruent to* 1 *modulo N. If G contains $\Gamma_1(N)$, then the following are equal:*

(1) $\bigcup_{\alpha\in A(n)} \bar{G}\alpha$
(2) $\bigcup_{\alpha\in A(n)} \bar{T}\alpha\bar{G}$
(3) $\bar{\Gamma}_1(N)\beta_n\bar{G}$.

Proof Clear.

To complete the proof of Theorem 1.2 define

$$F_n(y) = \prod_{\alpha\in A(n)} (y - f\circ\alpha)$$

Using Corollary 3.4 and the same proofs as in [CG, Propositions 6.16, 6.17 and 6.18], we obtain the following two results:

Proposition 3.5 *If n is such that every prime divisor of n is congruent to* 1 *modulo N and $f \in \mathfrak{F}_N$ is a normalised Hauptmodul for a group containing $\Gamma_1(N)$ then the polynomial $F_n(y)$ has coefficients in $H[f]$ and is irreducible over $\mathbb{C}(f)$.*

Proposition 3.6 *With f and n as in Proposition 3.6, $F_n(x, y)$ is a modular polynomial for f.*

This completes the proof of Theorem 1.2 1. The proof of Theorem 1.2 2 is essentially identical to the proof of [CG, Theorem 1.4 2].

In general it does not appear to be possible to define "generalised" modular polynomials. A natural candidate is

$$\prod_{\alpha\in A(n)} (y - f\circ\sigma_\alpha\alpha)$$

However, consider the case when $f(z)$ is the normalised Hauptmodul for $\Gamma_1(5)$ and $n = 2$. We can take $\sigma_2 = \left(\begin{smallmatrix} 2 & 1 \\ 5 & 3 \end{smallmatrix}\right)$. It is not difficult to see that the three roots, $f(\sigma_2 2z)$, $f(z/2)$ and $f\big((z+1)/2\big)$ are distinct and so by Proposition 3.3 $\Gamma_1(5) * 2 = \Gamma_1(5)$

permutes these zeros and so the symmetric functions of the roots are automorphic functions for $\Gamma_1(5)$. The symmetric function $s_1(z) = f(\sigma_2 2z) + f(z/2) + f\big((z+1)/2\big)$ has no pole at $i\infty$. So if we can write it as a polynomial in some (unnormalised) Hauptmodul for $\Gamma_1(5)$, $w(z)$ say, then $w(z)$ is finite at $i\infty$. But the symmetric function $s_2(z) = f^2(\sigma_2 2z) + f^2(z/2) + f^2\big((z+1)/2\big)$ has a pole at $i\infty$. So it cannot be written as a polynomial in $w(z)$. Thus there is no choice of an (unnormalised) Hauptmodul $w(z)$ such that the coefficients of $\prod_{\alpha \in A(2)}(y - f \circ \sigma_\alpha \alpha)$ can be written as polynomials in $w(z)$.

Using some computer algebra we can be more explicit in this example. Set $g(z) = \frac{\eta(z)^6}{\eta(5z)^6} + 6$, which is the normalised Hauptmodul for $\Gamma_0(5)$. Then $g(z) = f(z) - 1/\big(f(z) + 5\big)$. Let

$$F_2(x, y) = y^3 - y^2(x^2 - 30) - \frac{(-1426 + 10\,x^3 + 40\,x^2 - 335\,x)y}{x + 5} - \frac{-1060\,x - 4030 + 25\,x^3 + 74\,x^2}{x + 5}$$

and define $w(z) = -1/\big(f(z) + 5\big) - 5 = f(\sigma_2 z)$, which is an unnormalised Hauptmodul for $\Gamma_1(5)$. Then $F_2\big(w(z), w(2z)\big) = F_2\big(w(z), f(z/2)\big)$, $F_2\Big(w(z), f\big((z+1)/2\big)\Big) = 0$ and so $\big(y - w(2z)\big)\big(y - f(z/2)\big)\Big(y - f\big((z+1)/2\big)\Big) = F_2\big(w(z), y\big)$. So the symmetric functions of the roots are rational functions of $w(z)$ even though the trace term is a polynomial.

References

[B] R. E. Borcherds, *Monstrous Moonshine and monstrous Lie superalgebras*. Invent. Math. **109**(1992), 405–444.

[BR] R. E. Borcherds and A. J. E. Ryba, *Modular Moonshine II*. Duke Math. J. **83**(1996), 435–459.

[CY] I. Chen and N. Yui, *Singular values of Thompson series*. In: Groups, Difference sets and the Monster, (eds. K. T. Arusu *et al*), de Gruyter, 1995.

[C] H. Cohn, *The primary role of modular equations*. Number Theory, New York, 1991–1995, (eds. D. V. Chudnovsky, G. V. Chudnovsky, M. B. Nathanson), 19–41, Springer, New York, 1996.

[CM] H. Cohn and J. McKay, *Spontaneous generation of modular invariants*. Math. Comp. **65**(1996), 1295–1309.

[CN] J. H. Conway and S. P. Norton, *Monstrous Moonshine*. Bull. London Math. Soc. **11**(1979), 308–339.

[CG] C. J. Cummins and T. Gannon, *Modular equations and the genus zero property of moonshine functions*. Invent. Math. **129**(1997), 413–443.

[K] D. N. Kozlov, *On completely replicable functions and extremal poset theory*. M.Sc. thesis, Department of Math., University of Lund, Sweden, 1994.

[L] S. Lang, *Elliptic functions*. 2nd edition, Addison-Wesley, Reading, Massachusetts, 1987.

[Mah] K. Mahler, *On a class of non-linear functional equations connected with modular functions*. J. Austral. Math. Soc. Ser. A **22**(1976), 65–118.

[Mar] Y. Martin, *On modular invariance of completely replicable functions*. In: Moonshine, the Monster, and related Topics, (eds. C. Dong and G. Mason), Contemporary Mathematics **193**, Amer. Math. Soc., Providence, RI, 1996, 263–286.

[N] S. P. Norton, *Generalised Moonshine*. Proc. Symp. Pure Math. **47**, Part 1, The Arcata Conference on Representations of Finite Groups, Arcata, Calif., 1986, **210**, Amer. Math. Soc., Providence, RI, 1987.

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press

[Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Princeton University Press, 1971.

[T] J. G. Thompson, *A finiteness theorem for subgroups of* $\mathrm{PSL}(2,\mathbb{R})$ *which are commensurable with* $\mathrm{PSL}(2,\mathbb{Z})$. Proc. Sym. Pure. Math., **37**, Santa Cruz Conference on finite groups, Amer. Math. Soc., Providence RI, 1980, 533–555.

e-mail: cummins@mathstat.concordia.ca

https://doi.org/10.4153/CMB-2002-004-6 Published online by Cambridge University Press