On the Galois group of the modular equation

Barry, Catherine Jane

On the Galois Group of the Modular Equation

by

Catherine Jane Barry

**A Thesis submitted in fulfilment
of the requirement for the degree of
Master of Science in Pure Mathematics**

Department of Mathematical Sciences

University of Durham
1992

ABSTRACT

On the Galois Group of the Modular Equation

by

Catherine Jane Barry

This thesis looks at a method of generating infinitely many extensions of the rationals with Galois group $PGL_2(\mathbb{Z}_n)$. Firstly, the Galois group of the modular equation over $\mathbb{Q}(j)$ is shown to be $PGL_2(\mathbb{Z}_n)$, by considering the n-th division points on an elliptic curve. Then, using Hilbert's Irreducibility Theorem and work discussed by Lang, we show that there are infinitely many rational values of j such that this Galois group does not reduce in size. Finally, an equation whose roots generate the same extension as the modular equation but which has much smaller coefficients is found, based on work by Cohn.

ACKNOWLEDGEMENTS

Firstly I wish to acknowledge the invaluable help of my supervisor, Dr. S.M.J. Wilson, without whose comments and guidance this thesis would not have been completed. I am also grateful to Dr. Vernon Armitage for his suggestions and continual support.

My warmest thanks to my family and friends, and especially to Tony, who has put up with so much. I also wish to thank my fellow research students and other members of the department, most notably Dr. Iain MacPhee, Tex Warnes and Uli Harder for providing light relief in the form of cryptic crosswords.

Lastly, I thank the University of Durham Studentship for their greatly appreciated financial support.

I declare that this thesis has not been submitted for a degree at any university other than the University of Durham.

INTRODUCTION

This thesis is concerned with the 'inverse Galois problem', that is, finding field extensions with a certain given Galois group. In this thesis that group is $PGL_2(\mathbb{Z}_n)$, the projective general linear group of 2×2 matrices with entries in $\mathbb{Z}_n$. This thesis is divided into four chapters.

Chapter 1 comprises of relevant background material on elliptic and modular functions. Most of the results are standard, and so the proofs are only sketched. Further details can be found in [1], [13], [15] and [17].

Chapter 2 is concerned with the work of Macbeath in [11], in which he proves that the Galois group of the modular polynomial $\Phi_n(j, j(\tau/n))$ over $\mathbb{Q}(j)$ is $PGL_2(\mathbb{Z}_n)$. In this chapter a parallel approach is adopted, using the n-th division points on an elliptic curve, as studied by Lang in [9], and the connection with Macbeath's work is shown.

Chapter 3 is devoted to two different methods of obtaining infinitely many extensions of the rationals with the same Galois group, $PGL_2(\mathbb{Z}_n)$. The first relies on Hilbert's Irreducibility Theorem, (see [10]), and shows that for a fixed n there are infinitely many rational values of j where the modular polynomial generates such an extension. The second method relies on work discussed by Lang, [9], to show that there is only a finite set of primes p for which the Galois group of $\Phi_p(j, j(\tau/p))$ over $\mathbb{Q}$ does reduce in size. Using this method, two examples of curves which generate the required extension are given.

In looking at all the relevant research carried out subsequent to Macbeath's paper, it was found that a paper by Cohn, [3], which is itself based on work by Fricke, [4], would lend itself to further study. Thus, in the final chapter, a method of deriving an alternative modular polynomial, f_n, with smaller coefficients is investigated, since the usual modular polynomial Φ_n is known to have extremely large coefficients,

making any computations for large n cumbersome. Φ_n is defined to be the product of differences between $j(\tau)$ and the conjugates of $j(\tau/n)$, where $j(\tau/n)$ is invariant under the subgroup $\Gamma^0(n)$ of Γ, and the quotient space $\mathbf{H}/\Gamma^0(n)$ is a Riemann surface over $\mathbf{H}/\Gamma$ of genus g. By considering the Atkin-Lehner involution, another quotient space, G^*, is found, of genus g^*, over which $\mathbf{H}/\Gamma^0(n)$ is a double covering. For the cases where $g^* = 0$, a pair of rational functions $F_n(t, \pm s)$ are found, where t is a single-valued function on G^* which becomes double-valued on $\mathbf{H}/\Gamma^0(n)$. These two functions then generate the 'two-valued' modular equation.

Two cases are looked at; $n = 13$, where $g = 0$, and $n = 11$, where $g = 1$. For the first case it was actually found that the function s could be dispensed with, in that $\overline{\mathbb{Q}(j, t, s)} = \overline{\mathbb{Q}(j, t)}$. In order to examine the second case it was necessary to consult Fricke, to find how the functions t are s were chosen.

Finally, in Chapter 4, the discriminants of the two modular equations were investigated. The discriminant, d, of Φ_n is divisible by many squares of primes, which are found not to ramify, whereas the discriminant, d^*, of f_n is found to divide d, and thus f_n has smaller coefficients. The values of τ for which $j(\tau)$ may appear in the discriminant are found in both cases.

CONTENTS

CHAPTER 1

1.1 Elliptic Functions

We start by denoting by

$\mathbb{Z}$ the ring of integers,

$\mathbb{Q}$ the ring of rational numbers,

$\mathbb{R}$ the ring of real numbers,

$\mathbb{C}$ the ring of complex numbers,

$\bar{\mathbb{C}} = \mathbb{C} \cup \{i\infty\}$, the extended complex plane,

$\mathbf{H} = \{z \in \mathbb{C},\ \mathrm{Im}\, z > 0\}$, the upper half plane,

and $\mathbf{H}^* = \mathbf{H} \cup \{i\infty\} \cup \mathbb{Q}$.

We also denote by

$M_2(R)$ the set $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,\ b,\ c,\ d \in R \right\}$,

$GL_2(R)$ the set $\{A \in M_2(R) \mid \det A = \pm 1\}$,

$SL_2(R)$ the set $\{A \in M_2(R) \mid \det A = 1\}$.

for a field R.

We start by defining a **lattice** in $\mathbb{C}$: let $\omega_1, \omega_2 \in \mathbb{C}$, with $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$. Then the free abelian group, or lattice, Λ, is defined by

$$\Lambda \;=\; \Lambda(\omega_1, \omega_2) \;=\; \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\} \,.$$

Two pairs, (ω_1, ω_2), (ω_1', ω_2') with $\omega_1, \omega_2, \omega_1', \omega_2' \in \mathbb{C}$, $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$, $\mathrm{Im}(\frac{\omega_1'}{\omega_2'}) > 0$, define the same lattice if and only if there exists $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ such that $A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$, i.e.,

$$\omega_1' \;=\; a\omega_1 + b\omega_2$$

$$\omega_2' = c\omega_1 + d\omega_2 .$$

A function f of a complex variable is called **periodic** with period ω, if

$$f(z+\omega) = f(z)$$

whenever $z, z+\omega$ are in the domain of f.

A function f is **doubly periodic** if it has two periods ω_1, ω_2, such that $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Thus, a doubly periodic function with periods ω_1, ω_2 takes the same value on all points of the lattice $\Lambda(\omega_1, \omega_2)$. Let f have periods ω_1, ω_2, $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Then (ω_1, ω_2) is called a **fundamental pair** of periods if every period of f is of the form $m\omega_1 + n\omega_2$, with $m, n \in \mathbb{Z}$. Every fundamental pair of periods forms a lattice of parallelograms, which are called **period parallelograms** .

A function f is called **elliptic** if
(i) f is doubly periodic,
(ii) f is meromorphic (i.e. its only singularities in the finite plane are poles).
Constant functions are examples of elliptic functions. In order to find examples of non-constant elliptic functions we need:

Theorem 1.1.1: If an elliptic function f has no poles in a period parallelogram, then f is constant.

Proof: Clear from Liouville's theorem, since if the function has no poles, it must be analytic, and bounded.

Theorem 1.1.2: The sum of the residues of an elliptic function at its poles in any period parallelogram is zero.

Proof: Since a meromorphic function has only a finite number of poles or zeroes, the period parallelogram may be translated to a congruent parallelogram with no poles or zeroes on the boundary. The contour integral around any such parallelogram will be zero, by periodicity. Now apply Cauchy's residue theorem.

Theorem 1.1.3: The number of zeroes of an elliptic function in a period par-

allelogram is equal to the number of poles, each counted with multiplicities.

Proof: Apply the principle of the argument to the period parallelogram.

The number of zeroes (or poles) in any period parallelogram is called the order of the function. Thus every non-constant elliptic function has at least two zeroes (or poles) in each period parallelogram. Weierstrass decided to construct an elliptic function with a double pole at $z = 0$, and thus considered the function

$$\sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^2} .$$

However, we have

Lemma 1.1.4: If α is real, the infinite series

$$\sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^\alpha}$$

converges absolutely if and only if $\alpha > 2$.

Thus, the series

$$\sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{(z-\omega)^2}$$

does not converge absolutely. So instead we consider

$$m(z) = \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) .$$

Since

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{z\,(2\omega - z)}{\omega^2 (z-\omega)^2} \approx \frac{1}{\omega^3} \quad \text{as } |\omega| \to \infty,$$

we know that $m(z)$ converges absolutely and uniformly, by the Weierstrass M-test. However, $m(z)$ is not periodic, but $\frac{1}{z^2} + m(z)$ is, as will be shown. Thus we define

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) .$$

This function is known as the **Weierstrass $\wp$ function.**

Theorem 1.1.5: The function $\wp(z)$ defined above is an even function of z with periods ω_1 and ω_2. It is analytic except for a double pole at each period ω in Λ.

Proof: The only point at issue is the periodicity of $\wp(z)$. Since $\wp(z)$ is uniformly convergent, we can differentiate term by term to get

$$\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}.$$

Then, for all $\lambda \in \Lambda$,

$$\begin{aligned}\wp'(z+\lambda) &= -2\sum_{\omega\in\Lambda}\frac{1}{(z+\lambda-\omega)^3},\\ &= -2\sum_{\sigma\in\Lambda}\frac{1}{(z-\sigma)^3},\\ &= \wp(z)\end{aligned}$$

for $\sigma = \omega - \lambda \in \Lambda$. Thus $\wp'(z)$ is Λ-periodic. Putting $\lambda = \omega$ and integrating, we get

$$\wp(z+\omega) = \wp(z) + c,$$

for a constant c. Now, for $z = -\omega/2$ we get

$$\wp(\omega/2) = \wp(-\omega/2) + c = \wp(\omega/2) + c,$$

since $\wp(z)$ is even. Thus $c = 0$, and this establishes the periodicity of $\wp(z)$.

Theorem 1.1.6: Let $r = \min\{\,|\omega| : \omega \neq 0\}$. Then for $0 < |z| < r$ we have

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2k+1)\,G_{2k+1}z^{2k}$$

where

$$G_k = \sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{\omega^k} \qquad \text{for } k \geq 3.$$

G_k is called an **Eisenstein series of order k.**

Proof: Consider $m(z) = \wp(z) - \frac{1}{z^2}$. This is holomorphic in a neighbourhood of 0, has a simple zero at 0, and is even. Hence

$$m(z) = \sum_{k=1}^{\infty}\frac{m^{(2k)}(0)\,z^{2k}}{(2k)!}.$$

Since $m(z)$ is absolutely convergent, we can differentiate term by term 2k times. Thus

$$m^{(2k)}(z) = \sum_{\omega \in \Lambda, \omega \neq 0} \frac{(2k+1)!}{(z-\omega)^{2k+2}}.$$

So

$$\begin{aligned} \frac{m^{(2k)}(0)}{(2k)!} &= (2k+1) \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^{2k+2}} \\ &= (2k+1)\, G_{2k+2}. \end{aligned}$$

where G_k is defined as in the theorem. Hence the result.

Theorem 1.1.7: The function $\wp(z)$ satisfies the non linear differential equation

$$[\wp'(z)]^2 = 4\,\wp^3(z) - 60\,G_4\,\wp(z) - 140\,G_6.$$

Proof: By the previous theorem, the Laurent expansion at $z = 0$ is

$$\wp'(z) = \frac{-2}{z^3} + 6\,G_4\,z + 20\,G_6\,z^3 + F(z),$$

where $F(z)$ is some power series in z which vanishes at $z = 0$. Therefore

$$[\wp'(z)]^2 = \frac{4}{z^6} - \frac{24\,G_4}{z^2} - 80\,G_6 + F(z).$$

Also

$$4\,\wp^3(z) = \frac{4}{z^6} + \frac{36\,G_4}{z^2} + 60\,G_6 + F(z),$$

and hence

$$[\wp'(z)]^2 - 4\,\wp^3(z) + 60\,G_4\,\wp(z) = -140\,G_6 + F(z).$$

Since the left hand side has no pole at $z = 0$, it can have no poles anywhere in a period parallelogram, and so must be constant. Therefore this constant must be $-140\,G_6$, and so

$$[\wp'(z)]^2 = 4\,\wp^3(z) - 60\,G_4\,\wp(z) - 140\,G_6.$$

We now let $g_2 = 60\,G_4$ and $g_3 = 140\,G_6$. We call g_2, g_3 the **Eisenstein invariants** . Then $\wp(z)$ satisfies

$$[\wp'(z)]^2 = 4\,\wp^3(z) - g_2\,\wp(z) - g_3.$$

Let

$$e_1 = \wp\left(\frac{\omega_1}{2}\right), \quad e_2 = \wp\left(\frac{\omega_2}{2}\right), \quad e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right).$$

Then these are the distinct roots of the cubic equation for $\wp'(z)$:

Theorem 1.1.8: $$4\,\wp^3(z) - g_2\,\wp(z) - g_3 = 4\prod_{i=1}^{3}(\wp(z) - e_i),$$

where the e_i are distinct. Hence ${g_2}^3 - 27\,{g_3}^2 \neq 0$.

Proof: $\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}$, and thus $\wp'(z)$ has a pole of order 3 at each $\omega \in \Lambda$. Also, since $\wp(z)$ is even, $\wp'(z)$ is odd. Let $\omega_3 = \omega_1 + \omega_2$. Therefore, for $i = 1,2,3$, $\wp'(\frac{1}{2}\omega_i) = \wp'(\omega_i - \frac{1}{2}\omega_i) = \wp'(-\frac{1}{2}\omega_i)$, by periodicity. But, since $\wp'(z)$ is odd, $\wp'(-\frac{1}{2}\omega_i) = -\wp'(\frac{1}{2}\omega_i)$. Therefore, $\wp'(\frac{1}{2}\omega_i) = 0$ for $i = 1,2,3$, and so $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, $\frac{1}{2}\omega_3$ are zeroes of $\wp'(z)$. Since $\wp'(z)$ has order 3, these must be simple zeroes of $\wp'$, and so $\wp'$ has no other zeroes in a period parallelogram with vertices $0, \omega_1, \omega_2, \omega_3$.

Now consider the elliptic function $\wp(z) - e_i$ for $i = 1,2,3$, which has a double pole at each $\omega \in \Lambda$. Thus, by Theorem 1.1.3, $\wp(z) - e_i$ must have two zeroes in the period parallelogram. Since $\wp(z) - e_i = 0$ for $z = \frac{1}{2}\omega_i$, and $\wp'(\frac{1}{2}\omega_i) = 0$, then $\frac{1}{2}\omega_i$ is a double zero of $\wp(z) - e_i$, and so $\wp(z) - e_i$ can have no other zeroes in the period parallelogram. Thus the e_i are all distinct, and $\prod_{i=1}^{3}(\wp(z) - e_i)$ has the same zeroes and poles as $[\wp'(z)]^2$.

The discriminant of the cubic polynomial

$$4x^3 - g_2x - g_3$$

is ${g_2}^3 - 27\,{g_3}^2$. The discriminant of a polynomial with distinct roots does not vanish, so with $x = \wp(z)$, we have $\Delta = {g_2}^3 - 27\,{g_3}^2 \neq 0$.

In the next section we will show that g_2, g_3 and the modular invariant, j, defined as

$$j = \frac{12^3 {g_2}^3}{{g_2}^3 - 27\,{g_3}^2}$$

are all examples of modular functions, and derive some properties of them.

1.2 The Modular Group, Modular Functions and Modular Forms

The **homogeneous modular group** , Γ, is defined to be $SL_2(\mathbb{Z})$. Thus Γ acts on the set of pairs (ω_2, ω_2) with $\omega_1, \omega_2 \in \mathbb{C}, \mathrm{Im}\,(\frac{\omega_1}{\omega_2}) > 0$ by

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \qquad \text{for } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

This is well defined, since

$$\begin{aligned} \mathrm{Im}\left(\frac{\omega_1'}{\omega_2'}\right) \;=\; \mathrm{Im}\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right) \;&=\; \mathrm{Im}\left(\frac{(a(\frac{\omega_1}{\omega_2}) + b)\,(c(\overline{\frac{\omega_1}{\omega_2}}) + d)}{(c(\frac{\omega_1}{\omega_2}) + d)\,(c(\overline{\frac{\omega_1}{\omega_2}}) + d)}\right), \\ &= \frac{\mathrm{Im}\,(ad(\frac{\omega_1}{\omega_2}) - bc(\frac{\omega_1}{\omega_2}))}{|c(\frac{\omega_1}{\omega_2}) + d|^2}, \\ &= \frac{\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right)}{\left| c\left(\frac{\omega_1}{\omega_2}\right) + d \right|^2} \;>\; 0\ , \end{aligned}$$

since $ad - bc = 1$. Corresponding to each homogeneous transformation there is an inhomogeneous, or Möbius transformation,

$$z \longmapsto \bar{A}(z) = \frac{az + b}{cz + d} \qquad \text{for } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\ .$$

The Möbius transformation is defined for all $z \in \bar{\mathbb{C}}$ except for $z = -d/c$ and $z = i\infty$. We extend the definition to all of $\bar{\mathbb{C}}$ by defining

$$\left.\begin{aligned} \bar{A}(i\infty) &= \frac{a}{c} \\ \bar{A}(-\frac{d}{c}) &= i\infty \end{aligned}\right\} \qquad \text{if c} \neq 0,$$

and

$$\bar{A}(i\infty) = i\infty \qquad \text{if c} = 0.$$

These Möbius transformations form a group under composition of mappings, and we call this group the **inhomogeneous modular group**, $\bar{\Gamma}$.

Clearly $\bar{A}$ and $-\bar{A}$ determine the same Möbius transformation, for $A \in \Gamma$, so we define the homomorphism $\phi : \Gamma \longrightarrow \bar{\Gamma}$ by

$$z \longmapsto \bar{A}(z) = \frac{az + b}{cz + d} \qquad \text{for } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\ ,$$

which has kernel $\{\pm I\}$. Thus

$$\bar{\Gamma} \cong \frac{\Gamma}{\{\pm I\}} .$$

Theorem 1.2.1: The homogeneous modular group Γ is generated by the elements

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad , \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

of infinite order and order 4, respectively. Thus $\bar{\Gamma}$ is generated by transformations $\bar{T} : z \mapsto z+1$ and $\bar{S} : z \mapsto -\frac{1}{z}$ of infinite order and order 2 respectively.

Proof: By the reduction theory of integral matrices we can diagonalize any matrix in Γ by premultiplying and postmultiplying by the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, V = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} .$$

But the only diagonal matrices in Γ are I and $-I = V$, and $V = S^2$, $U = TST$, hence our result.

Since $\bar{T}, \bar{S}$ generate $\bar{\Gamma}$, so do $\bar{S}$ and $\bar{S}\bar{T}$ of order 2 and 3 respectively. In fact $\bar{\Gamma}$ is isomorphic to the free product

$$\bar{\Gamma} \cong < \bar{S} > \times < \bar{S}\bar{T} > .$$

Let $\tau, \tau' \in \mathbf{H}^*$. Then τ, τ' are said to be **equivalent** under $\bar{\Gamma}$ if $\tau' = \bar{A}(\tau)$ for some $\bar{A} \in \bar{\Gamma}$. This is an equivalence relation, since $\bar{\Gamma}$ is a group, which divides $\mathbf{H}^*$ into disjoint equivalence classes, known as **orbits.** The orbit $\bar{\Gamma}\tau$ is the set of all points of the form $\bar{A}\tau$ where $\bar{A} \in \bar{\Gamma}$.

Definitions: A **fundamental set** of $\bar{\Gamma}$ for $\mathbf{H}^*$ is a set containing exactly one point from each orbit of $\mathbf{H}^*$.

A **fundamental region** of $\bar{\Gamma}$ for $\mathbf{H}^*$ is an open subset $F_{\bar{\Gamma}}$ of $\mathbf{H}^*$ such that

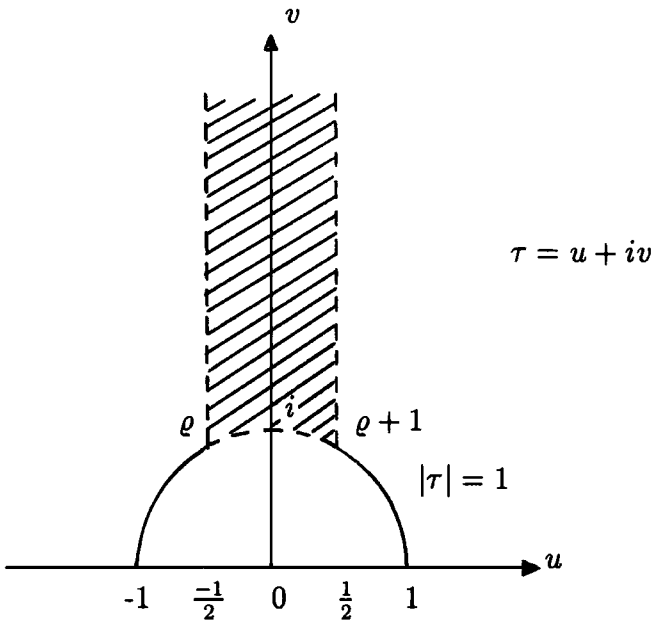
(i) no two distinct points of $F_{\bar{\Gamma}}$ are equivalent under Γ,

(ii) if $\tau \in \mathbf{H}$, there is a point τ' in the closure of $F_{\bar{\Gamma}}$ such that τ' is equivalent to τ under $\bar{\Gamma}$.

$\bar{\Gamma}$ has infinitely many fundamental regions, of which the following is the standard:

$$F_{\bar{\Gamma}} = \left\{ \tau \in \mathbf{H} \;\middle|\; |\tau| > 1, |\mathrm{Re}\tau| < \frac{1}{2} \right\}.$$

This is shown by the shaded area below:



Definition: A function f is called a **modular function** (of level one) if

(i) f is meromorphic in $\mathbf{H}$ (i.e. holomorphic except for poles),

(ii) $f(\bar{A}(\tau)) = f(\tau)$ for all $\bar{A} \in \bar{\Gamma}, \tau \in \mathbf{H}^*$,

(iii) f has a Fourier expansion of the form

$$\begin{aligned} f(\tau) &= \sum_{n=-m}^{\infty} a(n)\, e^{2\pi i n \tau} \qquad m \in \mathbb{Z}, \\ &= \sum_{n=-m}^{\infty} a(n)\, q^n, \end{aligned}$$

where we define $q = e^{2\pi i \tau}$, and $q^\alpha = e^{2\pi i \alpha \tau}$ for all $\alpha \in \mathbb{C}$.

Thus f is analytic in $\mathbf{H}$, except possibly for poles, and is invariant under all transformations of Γ. A function satisfying the third condition is said to be meromorphic at $i\infty$. If $m > 0$ with $a(-m) \neq 0$, we say that f has a pole of order m at $i\infty$, and that $f(i\infty) = \infty$. If $m \leq 0$ we say that f is analytic at $i\infty$, and that

$f(i\infty) = 0$ if $m < 0$, $f(i\infty) = a(0)$ if $m = 0$.

Definitions: A complex valued function f of two complex variables ω_1, ω_2, defined for $\omega_1/\omega_2 \in \mathbf{H}$, is called a **homogeneous modular form of weight 2k,** $k \in \mathbb{Z}$ if

(i) $f(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k} f(\omega_1, \omega_2) \qquad \forall\, 0 \neq \lambda \in \mathbb{C}$,

(ii) $f(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2) = f(\omega_1, \omega_2) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,

(iii) $f(\tau, 1)$ is holomorphic in $\mathbf{H}$,

(iv) $f(\tau, 1)$ has Fourier expansion

$$f(\tau, 1) = \sum_{n=0}^{\infty} b(n)\, q^n .$$

Thus, by (ii), f is a function of the lattice $\Lambda(\omega_1, \omega_2)$.

A function g of one complex variable $\tau = \omega_1/\omega_2$ is called an **inhomogeneous modular form** if $\omega_2^{-2k}\, g\left(\frac{\omega_1}{\omega_2}\right) = f(\omega_1, \omega_2)$ for $f(\omega_1, \omega_2)$ a homogeneous modular form. Thus, $f(\tau, 1)$ is an inhomogeneous modular form.

If g is an inhomogeneous modular form, then (i) and (ii) imply that g satisfies

$$\text{(v)}\ g\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k}\, g(\tau) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Conversely, (v) implies (ii), and (i) is trivial.

The Eisenstein invariants:

Since

$$G_{2k} = \sum_{\omega \neq 0, \omega \in \Lambda} \frac{1}{\omega^{2k}} = \sum_{(c,d) \neq (0,0)} \frac{1}{(c\tau + d)^{2k}}$$

is absolutely convergent for $k \geq 2$, we see that G_{2k} is an inhomogeneous modular form of weight 2k. Thus

$$g_2 = 60 G_4 ,$$

$$g_3 = 140 G_6 ,$$

are modular forms of weight 4 and 6 respectively, i.e.,

$$\begin{aligned} g_2(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-4} g_2(\omega_1, \omega_2), \\ g_3(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-6} g_3(\omega_1, \omega_2). \end{aligned}$$

They can also be thought of as functions of one variable by putting $g(\tau) = g(\tau, 1)$ for $\tau = \omega_1/\omega_2$.

The Fourier expansions for g_2, g_3 are given by

$$\begin{aligned} g_2(\tau) &= \frac{4\pi^4}{3}\left\{1 + 240\sum_{k=1}^{\infty}\sigma_3(k)\, q^k\right\} \\ g_3(\tau) &= \frac{8\pi^6}{27}\left\{1 - 504\sum_{k=1}^{\infty}\sigma_5(k)\, q^k\right\} \end{aligned}$$

where

$$\sigma_\alpha(k) = \sum_{d|k} d^\alpha .$$

(see [1], p.20, Theorem 1.18)

The discriminant:

The discriminant was defined in 1.1 to be

$$\Delta(\tau) = {g_2}^3(\tau) - 27{g_3}^2(\tau) .$$

Since $\Delta(\tau) \neq 0$, and g_2, g_3 are modular forms of level 4 and 6 respectively, $\Delta(\tau)$ is a modular form of weight 12.

$\Delta(\tau)$ has Fourier expansion

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)\, q^n$$

where $\tau(n) \in \mathbb{Z}$, with $\tau(1) = 1, \tau(2) = -24$.
(see [1], p.20, Theorem 1.19.)

The modular invariant:

The modular invariant, j, is defined to be

$$j(\omega_1, \omega_2) = \frac{12^3 g_2{}^3(\omega_1, \omega_2)}{\Delta(\tau)}.$$

Since $\Delta(\omega_1, \omega_2) \neq 0$, and $g_2(\omega_1, \omega_2), \Delta(\omega_1, \omega_2)$ are homogeneous modular forms of the same weight, we have that $j(\omega_1, \omega_2)$ is a modular function of level one, i.e.,

$$j(\lambda\omega_1, \lambda\omega_2) = j(\omega_1, \omega_2) \qquad \forall\, 0 \neq \lambda \in \mathbb{C},$$

and

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A \in \Gamma.$$

In particular, for $\tau \in \mathbf{H}$, we have

$$j(1, \tau) = j(\omega_1, \omega_2).$$

Thus, j is effectively a function of one complex variable, $\tau = \omega_1/\omega_2$.

Using the Fourier expansions for $g_2(\tau)$ and $\Delta(\tau)$, we can derive the Fourier expansion for $j(\tau)$: Let $q = e^{2\pi i\tau}$. Then

$$\begin{aligned} g_2{}^3(\tau) &= \frac{64}{27}\pi^{12}(1 + 240q + \cdots)^3 \\ &= \frac{64}{27}\pi^{12}(1 + 720q + \cdots) \end{aligned}$$

and

$$\Delta(\tau) = 2^{12}\pi^{12}(q - 24q^2 + \cdots).$$

So

$$\begin{aligned} j(\tau) &= \frac{1}{q}(1 + 720q + \cdots)(1 + 24q + \cdots) \\ &= \frac{1}{q}(1 + 744q + \cdots) \\ &= \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)\, q^n \end{aligned}$$

where $c(n) \in \mathbb{Z}$. Thus $j(\tau)$ has a simple pole at $i\infty$.

The $c(n)$ have been calculated for $n \leq 100$, and various congruence conditions have been found, for example

$$c(5n) \equiv 0 \,(\mathrm{mod}\, 25)\ .$$

The values of $c(n)$ for $0 \leq n \leq 6$ are given here, as they are used in later calculations.

$c(0) = 744,$

$c(1) = 196,884,$

$c(2) = 21,493,760,$

$c(3) = 864,299,970,$

$c(4) = 20,245,856,256,$

$c(5) = 333,202,640,600,$

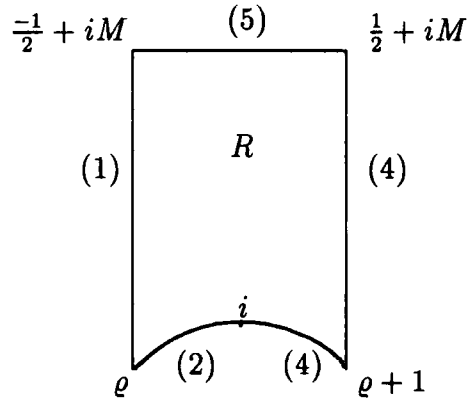
$c(6) = 4,252,023,300,096.$

Definition: Let f be a modular form of weight $2k$, not identically zero, and let $\tau \in \mathbf{H} \setminus \{i\infty\}$. The smallest integer n such that $\dfrac{f}{(z-\tau)^n}$ is holomorphic and non-zero at τ is called the **order of f at τ**, and is denoted by $v_\tau(f)$.

If f is a modular form of weight $2k$, then $f(\tau) = f(\tau+1)$, so we can express f as a function of $q = e^{2\pi i\tau}$, and we denote this function by $\tilde{f}$. Thus $\tilde{f}(q) = \sum_{-\infty}^{\infty} a_n q^n$. Using this we can define $v_{i\infty}(f)$ as the order for $q = 0$ of the function $\tilde{f}(q)$.

Theorem 1.2.2: For a non-zero modular function f, the number of zeroes of f is equal to the number of poles of f, in the closure of $F_{\bar{\Gamma}}$, taking into account their orders.

Proof: Since f has only finitely many poles and zeros, we integrate around the contour R:



where we take M large enough that all the zeros and poles of f are inside R. The edges (1),(4) and (2),(3) are equivalent in that if f has a zero of pole on any of these edges, then it also has a zero or pole on the equivalent edge. Only one of the zeros of poles is counted as belonging to $F_{\bar{\Gamma}}$. Also, the order of the zero or pole at $\varrho = e^{2\pi i/3}$ is to be divided by 3 since the angle at ϱ is $\pi/3$ and ϱ is equivalent to $\varrho+1$, and the order of the zero or pole at i is to be divided by 2 since the angle at i is π. Suppose that f has a zero or pole of order m at $i\infty$. Then f has Fourier expansion of the form $\sum_{m}^{\infty} a_m\, q^m$. Substituting for this we see that

$$\int_{(5)} \frac{f'}{f} dz = \int_{\frac{1}{2}+iM}^{-\frac{1}{2}+iM} \frac{f'}{f} dz = -2\pi i m\,.$$

Then we apply the principal of the argument.

We now prove

Theorem 1.2.3: Let f be a non-zero modular form of weight $2k$. Then

$$v_{i\infty}(f) \;+\; \frac{1}{2} v_i(f) \;+\; \frac{1}{3} v_\varrho(f) \;+\; \sum_{\substack{\tau \in F_{\bar{\Gamma}} \\ \tau \neq i, \varrho, i\infty}} v_\tau(f) \;=\; \frac{k}{6}\,.$$

where $\varrho = e^{2\pi i/3}$.

Proof: Since f has weight $2k$ and Δ is a modular form of weight 12, then $g = f^{12}/\Delta^{2k}$ is a modular function. Thus we can apply Theorem 1.2.2 to g. But Δ only has a simple pole at $i\infty$, and so $v_{i\infty}(\Delta^{2k}) = 2k$. Thus we must have that

$$v_{i\infty}(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\varrho(f) + \sum_{\substack{\tau \in F_{\bar{\Gamma}} \\ \tau \neq i, \varrho, i\infty}} v_\tau(f) = \frac{2k}{12} = \frac{k}{6}.$$

We use this to prove

Theorem 1.2.4: The function j takes every value exactly once in the closure of $F_{\bar{\Gamma}}$. At the vertices,

$$j(i\infty) = \infty, \qquad j(\varrho) = 0, \qquad j(i) = 1728,$$

and $j(\tau)$ has a first order pole at $\tau = i\infty$, a triple zero at $\tau = \varrho$, and $j(\tau) - 1728$ has a double zero at $\tau = i$.

Proof: Let $f(\tau) = j(\tau) - c$ for $c \in \mathbb{C}$. Then $f(\tau)$ is a modular function, which has a simple pole at $i\infty$. Applying Theorem 1.2.3,

$$\frac{1}{2}v_i(f) + \frac{1}{3}v_\varrho(f) + \sum_{\substack{\tau \in F_{\bar{\Gamma}} \\ \tau \neq i, \varrho, i\infty}} v_\tau(f) = 1.$$

Since $f(\tau)$ is holomorphic on $\mathbf{H}$, all the terms on the LHS are ≥ 0. Thus there is only one term on the LHS, and so

$$(v_i(f),\ v_\varrho(f),\ v_\tau(f)) = (2,0,0),\ (0,3,0) \text{ or } (0,0,1). \qquad (*)$$

Thus f is zero exactly once in $F_{\bar{\Gamma}} \setminus \{i\infty\}$, and adding $j(i\infty) = \infty$ gives a unique $\tau \in F_{\bar{\Gamma}}$ such that $j(\tau) = c$. The multiplicities follow from $(*)$.

Theorem 1.2.5: Every modular function can be expressed as a rational function of j, and conversely.

Proof: Suppose f is a modular function, with zeroes z_k of order r_k, $(k =$

$1, \ldots, m)$ and poles p_l of order s_l, $(l = 1, \ldots, n)$. Let

$$g(\tau) = \frac{\prod_{k=1}^{m} (j(\tau) - j(z_k))^{r_k}}{\prod_{l=1}^{n} (j(\tau) - j(p_k))^{s_l}},$$

where a factor 1 is inserted whenever z_k or p_k equals $i\infty$. Then g is a modular function with the same zeroes and poles as f on the finite plane, with the same multiplicities. By Theorem 1.2.2, if f has a zero or pole at $i\infty$ then g also has a zero or pole there, with the same multiplicity. Thus f/g has no zeroes or poles, and so must be constant. Hence f is a rational function of j.

This result shows that the field of modular functions of level one is $\mathbb{C}(j)$. Macbeath's paper actually requires a more specific result, for which we need some more theory:

Definition: An inhomogeneous modular form is called a **cusp form** if it is zero at $i\infty$. By this, we mean that in the Fourier expansion

$$f(\tau) = \sum_{n=0} b(n) q^n,$$

we have that $b(0) = 0$.

Let M_k denote the $\mathbb{C}$-vector space of modular forms of weight $2k$,and M_k^0 denote the $\mathbb{C}$-vector space of cusp forms of weight $2k$. Then we have:

Theorem 1.2.6: (i) The only modular forms of weight 0 are the constant functions.
(ii) If $k < 0$ or $k = 1$, the only modular form of weight $2k$ is the zero function, i.e., $M_k = 0$ for $k < 0, k = 1$.
(iii) The only cusp form of weight $2k, k \leq 5$, is the zero function, i.e., $M_k^0 = 0$ for $k \leq 5$.

Proof: (i) A modular form of weight 0 is a modular function, and since it is analytic everywhere, including $i\infty$, it must be constant.

(ii) Let f be a non-zero element of M_k. Applying Theorem 1.2.3,

$$v_{i\infty}(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\varrho(f) + \sum_{\substack{\tau \in F_\Gamma \\ \tau \neq i,\varrho,i\infty}} v_\tau(f) = \frac{k}{6},$$

all the terms on the LHS are ≥ 0. Thus, $k \geq 0$, and $k \neq 1$, since $1/6$ cannot be written in the form $l + m/2 + n/3$, with $l, m, n \geq 0$.
(iii) If $k \leq 5$, then $v_{i\infty}(f) = 0$, by Theorem 1.2.3, and so f is not a cusp form unless $f = 0$.

We can now state the result used by Macbeath:

Theorem 1.2.7: Any modular function $f(\tau)$ which is holomorphic on $\mathbf{H}$ can be written as a polynomial in $j(\tau)$, with coefficients in the field generated by the Fourier coefficients of $f(\tau)$.

Proof: Suppose $f(\tau)$ has Fourier expansion

$$f(\tau) = \sum_{n=-m}^{\infty} a_n q^n, \qquad q = e^{2\pi i \tau}.$$

Also, $j(\tau)$ is holomorphic on $\mathbf{H}$ with Fourier expansion

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n, \qquad \text{with } c_n \in \mathbb{Z}.$$

Then, the new function

$$f(\tau) - a_{-m}[j(\tau)]^m = \sum_{n=-m+1}^{\infty} b_n q^n$$

is also holomorphic on $\mathbf{H}$.

Continuing in this way, we find a function

$$g(\tau) = f - a_{-m} j^m - b_{-m+1} j^{m-1} - \cdots\cdots - y_1 j - z$$

which is a modular function of weight 0, which is holomorphic at $i\infty$, and vanishes there. Thus $g(\tau)$ is a cusp form of weight 0. By Theorem 1.2.6 (iii), $M_k^0 = 0$ and so $g(\tau) = 0$, and so f is a polynomial in $j(\tau)$, with coefficients in the field generated by the a_n's.

Macbeath also uses a corollary to this theorem,

Corollary 1.2.8: Any modular function having Fourier series with rational coefficients belongs to the field $\mathbb{Q}(j(\tau))$.

Proof: Suppose $f(\tau)$ has poles $p_i \in \mathbf{H}$, of orders z_i. Let

$$g(\tau) = f(\tau) \prod_{p_i} (j(\tau) - j(p_i))^{z_i},$$

with the product being taken over all the poles of $f(\tau)$. Then $g(\tau)$ is a modular function having no poles on $\mathbf{H}$, and is thus a polynomial in $j(\tau)$, by the above theorem, with coefficients in $\mathbb{C}$. Thus $f \sum_i c_i j^i = \sum_i d_i j^i$ for a finite sum over i, where $c_i, d_i \in \mathbb{C}$, $j^i \in \mathbb{Q}((q))$. Thus the c_i, d_i generate a vector space over $\mathbb{Q}$, which we denote by $< r_1, \ldots, r_n >$, and so $c_i = \sum_k \gamma_{ik} r_k$, $d_i = \sum_k \delta_{ik} r_k$ for $\gamma_{ik}, \delta_{ik} \in \mathbb{Q}$. Thus

$$\sum_k \left(\sum_i \gamma_{ik} j^i f - \sum_i \delta_{ik} j^i \right) r_k = 0.$$

Since the r_k are linearly independent over $\mathbb{Q}$, they must be linearly independent over $\mathbb{Q}((q))$, and so $\sum_i \gamma_{ik} j^i f - \sum_i \delta_{ik} j^i = 0$ for all k. But for some $k = k_0$ we must have that $\sum_i \gamma_{ik} j^i \neq 0$, and so

$$f = \frac{\sum_i \delta_{ik_0} j^i}{\sum_i \gamma_{ik_0} j^i} \in \mathbb{Q}(j).$$

1.3 Transformations of order n, and the Modular Polynomial

Before we can define the modular polynomial, we must first introduce transformations of order n. Let

$$\Delta_n = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z}, |M| = n \geq 1, (a,b,c,d) = 1 \right\}$$

We call M a **matrix of order n**, and the corresponding linear transformation a **transformation of order n**. Clearly, multiplication on the left or right by elements of Γ maps Δ_n into itself. Thus we study the right cosets ΓM for $M \in \Delta_n$.

Two transformations $M, M' \in \Delta_n$ are **congruent modulo** Γ,

$$M' \sim M \qquad \text{or} \qquad M' \equiv M \bmod \Gamma,$$

if and only if there is an $S \in \Gamma$ such that $M' = SM$, i.e., they lie in the same orbit of Δ_n under Γ. This defines an equivalence relation.

Theorem 1.3.1: The set

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; 0 < a,\ 0 \leq b < d,\ ad = n,\ (a,b,d) = 1 \right\}$$

is a complete system of representatives of the equivalence classes of $\Delta_n \bmod \Gamma$.

Proof: Firstly, for any $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_n$, there is a matrix $M' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in \Delta_n$ such that $M \sim M'$:
We need $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$ such that $SM = M'$, i.e,

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}.$$

Choose γ, δ such that $\gamma a + \delta c = 0$, $(\gamma, \delta) = 1$, and then choose α, β such that $\alpha\delta - \beta\gamma = 1$.

Secondly, any two transformations in Δ_n,

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \qquad M' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$$

are congruent if and only if

$$a = \pm a', \qquad d = \pm d', \qquad b = \pm b' (\mathrm{mod}\, d), \tag{$*$}$$

with the same sign taken in each case:

If $M' \sim M$ then there exists $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$ such that

$$\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b + \beta d \\ \gamma a & \gamma b + \delta d \end{pmatrix}.$$

Thus $\gamma = 0$, and $\alpha\delta - \gamma\delta = 1$ gives $\alpha = \delta = \pm 1$, so $a' = \pm a, d' = \pm d$. Hence,

$$\begin{aligned} b' &= \pm b + \beta d \\ &\equiv \pm b \,(\mathrm{mod}\, d) \end{aligned}$$

Conversely, if $(*)$ holds, then

$$M' M^{-1} = \frac{1}{n} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{a'd}{n} & \frac{-a'b + ab'}{n} \\ 0 & \frac{ad'}{n} \end{pmatrix}$$
$$= \begin{pmatrix} \pm 1 & \beta \\ 0 & \pm 1 \end{pmatrix} \in \Gamma$$

Thus $M' = TM$ for some $T \in \Gamma$.

The theorem follows directly from these two results.

The number of equivalent transformations is given by:

Theorem 1.3.2: The number $\psi(n)$ of equivalence classes of Δ_n mod Γ is given by

$$\psi(n) = n \prod_{p|n} \left(1 + \frac{1}{p}\right).$$

Proof: Firstly, we consider the case for $n = p$, a prime. Then by Theorem 1.3.1, the representatives of the equivalence classes are given by

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & t \\ 0 & p \end{pmatrix} \quad \text{for} \quad 0 \leq t < p.$$

Thus $\psi(p) = p + 1$.

For n a positive integer, we must count the number of matrices of the type in Theorem 1.3.1. For fixed $d, a = n/d$ is determined, so we must find the number of possibilities for b. Let $e = (a, d)$. Then there are $\frac{d}{e}\phi(e)$ integers which are relatively prime to e. Hence

$$\psi(n) = \sum_{d|n} \frac{d}{e}\phi(e).$$

Since ϕ is a multiplicative function, then so is ψ i.e., if $(n_1, n_2) = 1$ then $\psi(n_1, n_2) = \psi(n_1)\psi(n_2)$. For,

$$\begin{aligned}
\psi(n_1)\psi(n_2) &= \sum_{d_1|n_1} \frac{d_1}{e_1}\phi(e_1) \sum_{d_2|n_2} \frac{d_2}{e_2}\phi(e_2) \\
&= \sum_{d_1|n_1, d_2|n_2} \frac{d_1 d_2}{e_1 e_2}\phi(e_1)\phi(e_2) \\
&= \sum_{d_1 d_2|n_1 n_2} \frac{d_1 d_2}{e_1 e_2}\phi(e_1 e_2) \\
&= \psi(n_1, n_2)
\end{aligned}$$

Thus it suffices to study the case when $n = p^k, p$ prime, $k \in \mathbb{N}$.

$$\begin{aligned}
\psi(p^k) &= \sum_{v=0}^{k} \frac{p^v}{(p^{k-v}, p^v)}\psi((p^{k-v}, p^v)) \\
&= \sum_{v=0}^{k} \psi(p^v) \\
&= 1 + p^k + \sum_{v=1}^{k-1} p^v(1 - \frac{1}{p}) \\
&= 1 + p^k + p^{k-1} - 1 \\
&= p^k(1 + \frac{1}{p})
\end{aligned}$$

Hence the result.

We can also show that Γ acts transitively on the left and right cosets of Δ_n:

Theorem 1.3.3: For every $M \in \Delta_n$ there exist $\gamma, \gamma' \in \Gamma$ such that

$$\gamma M \gamma' = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix},$$

i.e., Γ acts transitively on the left and right cosets of Δ_n.

Proof: Since, in the proof of Theorem 1.3.1, we showed that every $M \in \Delta_n$ is equivalent to a matrix of the form $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in \Delta_n$, we can take M to be $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$ without loss of generality.

We must show that for every $M = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in \Delta_n$ there is a $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ such that

$$M^{-1}\gamma \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma .$$

But

$$M^{-1}\gamma \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{n} \begin{pmatrix} \delta & -\beta \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a\alpha - c\beta & \dfrac{b\delta - d\beta}{n} \\ c\alpha & \dfrac{d\alpha}{n} \end{pmatrix} = \gamma' .$$

For the r.h.s. to be in Γ, we must have

$b\delta - d\beta \equiv 0 \pmod{n}$,

$d\alpha \equiv 0 \pmod{n}$, i.e., $d \equiv 0 \pmod{\delta}$.

We can choose $d = \delta$, and then $b - \beta \equiv 0 \pmod{\alpha}$. Choosing $b = \beta + t\alpha$ for $t \in \mathbb{Z}$ gives $\det(\gamma') = 1$, and hence $\gamma' \in \Gamma$. Thus $M^{-1}\gamma \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} = \gamma'$, so $\gamma^{-1}M\gamma' = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, i.e.,

$$\Delta_n = \Gamma \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \Gamma .$$

Hence Γ acts transitively on Δ_n.

Let

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_{\psi(n)}$$

be a complete set of coset representatives for Δ_n under the action of Γ. Define $j_\circ\alpha$ to be $j(\alpha(\tau))$ for $\alpha \in \Delta_n$. Then the functions $j_\circ\alpha_i$, $(i = 1, \ldots, \psi(n))$ are distinct, by Theorem 1.2.4, and are permuted transitively by the action of Γ, by Theorem 1.3.3.

Definition: Let $\Phi_n(X) = \prod_{i=1}^{\psi(n)} (X - j_\circ\alpha)$.

This polynomial is called the **modular polynomial of order n.** The equation $\Phi_n(X) = 0$ is called the **modular equation of order n.**

Theorem 1.3.4: The coefficients of $\Phi_n(X)$ in terms of X are in $\mathbb{Z}[j]$, i.e., are polynomials in j with integer coefficients.

Proof:

$$\Phi_n(X) = \prod_{i=1}^{\psi(n)} (X - j_\circ\alpha_i) = \sum_{m=1}^{\psi(n)} s_m X^{\psi(n)-m}, \qquad s_0 = 1.$$

The coefficients s_m are the elementary symmetric functions of the $j_\circ\alpha_i$, and are therefore holomorphic on $\mathbf{H}$, and are invariant under Γ. Thus they are modular functions, and so are polynomials in j, by Theorem 1.2.7, i.e., $s_m = s_m(j)$.

Let

$$j(\tau) = \sum_{m=-1}^{\infty} c_m q^m, \qquad q = e^{2\pi i\tau},\ c_m \in \mathbb{Z},\ c_{-1} = 1.$$

Then

$$j_\circ\alpha_i = j(\alpha_i(\tau)) = j\left(\frac{a\tau + b}{d}\right), \qquad \text{for } \alpha_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Delta_n,$$

where

$$a, b, d \in \mathbb{Z},\ \ 0 < a,\ \ 0 \le b < d,\ \ ad = n,\ \ (a, b, d) = 1.$$

So

$$\begin{aligned} j\left(\frac{a\tau + b}{d}\right) &= \sum_{m=-1}^{\infty} c_m e^{2\pi i(a\tau + b/d)m} \\ &= \sum_{m=-1}^{\infty} c_m q^{\frac{am}{d}} \xi_d^{bm}, \qquad \text{where } \xi_d = e^{\frac{2\pi i}{d}} \end{aligned} \tag{$*$}$$

Thus, by Theorem 1.2.7, the $s_m(j)$ are in $\mathbb{Z}[\xi_n]$, where $\xi_n = e^{\frac{2\pi i}{n}}$, and are hence in $\mathbb{Q}(\xi_n)$.

Let σ be an automorphism on $\mathbb{Q}(\xi_n)$,

$$\sigma :\ \xi_n \longrightarrow \xi_n{}^r$$

for some $r \in \mathbb{Z}$ with $(r, n) = 1$. By $(*)$ we see that σ permutes the $j_\circ\alpha_i$. Therefore, the $s_m(j)$ are invariant under such an automorphism, so have Fourier coefficients in $\mathbb{Z}$, so by Theorem 1.2.7, $s_m(j) \in \mathbb{Z}$. Thus we may regard $\Phi_n(X)$ as a polynomial in the two independant variables X and j over $\mathbb{Z}$, i.e.,

$$\Phi_n(X) = \Phi_n(X, j) = \prod_{i=1}^{\psi(n)} (X - j_\circ\alpha_i) \in \mathbb{Z}[X, j].$$

Since Γ permutes the $j_\circ\alpha$ transitively, and acts as a group on automorphisms on the field $\mathbb{C}(j, j_\circ\alpha_1, \ldots, j_\circ\alpha_{\psi(n)})$, then $\Phi_n(X,j)$ has degree $\psi(n)$.

Theorem 1.3.5: (i) $\Phi_n(X,j) = \Phi_n(j,X)$,
(ii) If n is not a square, then $\Phi_n(j,j)$ is a polynomial in j of degree > 1, and with leading coefficient ± 1.

Proof: (i) Let $\alpha_r = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$, $1 \leq r \leq \psi(n)$. Then $j_\circ\alpha_r$ is a root of $\Phi_n(X,j)$, i.e.,

$$\Phi_n(j(\tau/n), j(\tau)) = 0.$$

Hence

$$\Phi_n(j(\tau), j(n\tau)) = 0.$$

So $j_\circ\alpha_s$ is a root of $\Phi_n(j,X)$, where $\alpha_s = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, $1 \leq s \leq \psi(n)$, $s \neq r$, but it is also a root of $\Phi_n(X,j)$. Since $\Phi_n(X,j)$ is irreducible, we must have that $\Phi_n(X,j) \mid \Phi_n(j,X)$, i.e.,

$$\Phi_n(j,X) = g(X,j)\,\Phi_n(X,j)$$

for some $g(t,j) \in \mathbb{Z}[t,j]$. Then

$$\Phi_n(j,X) = g(X,j)\,g(j,X)\,\Phi_n(j,X),$$

so

$$g(X,j)\,g(j,X) = 1.$$

So

$$g(X,j) = \pm 1.$$

If $g(X,j) = -1$, then $\Phi_n(j,j) = -\Phi_n(j,j)$, i.e., $\Phi_n(j,j) = 0$, so j must be a root of $\Phi_n(X,j)$, but $\Phi_n(X,j)$ is irreducible over $\mathbb{C}(j)$, so this is not possible. Hence $g(X,j) = 1$ and so

$$\Phi_n(X,j) = \Phi_n(j,X).$$

(ii) Let $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $\alpha \in \Delta_n$
As in the proof of Theorem 1.3.4, we have that

$$j_\circ\alpha = \frac{1}{q^{\frac{a}{d}}\xi_d{}^b} + \left(\sum_{m=0}^{\infty} c_m\, q^{\frac{am}{d}}\, \xi_d{}^{bm}\right),$$

and so

$$j - j_\circ\alpha = \frac{1}{q} + \cdots - \frac{1}{q^{\frac{a}{d}}\,\xi_d{}^b} - \cdots$$

Since n is not a square, $a \neq d$, and so there is no cancellation in the polar term, and so the leading term in this expansion is either q^{-1} if $a < d$, or $\xi_d{}^b q^{\frac{-a}{d}}$, if $a > d$. Thus the leading coefficient in either case is a root of unity. But,

$$\Phi_n(j,j) = \prod_{i=1}^{\psi(n)} (j - j_\circ\alpha_i),$$

and so the expansion of $\Phi_n(j,j)$ starts with

$$\frac{c_m}{q^m} + \cdots$$

Since $\Phi_n(j,j) \in \mathbb{Z}[j]$, c_m must be both a root of unity and an integer. Hence $c_m = \pm 1$, as required.

Theorem 1.3.6: If $\tau \in \mathbf{H}$ is imaginary quadratic, then $j(\tau)$ is an algebraic integer.

Proof: Let $\tau \in K$, $R = \mathrm{int}(K)$, and z be an algebraic integer such that

$$K = \mathbb{Q}(z), \qquad R = \mathbb{Z}[z].$$

It is always possible to find an element $x \in R$ such that the norm of x is a squarefree integer: If $K = \mathbb{Q}(i)$, then take $x = 1+i$, if $K = \mathbb{Q}(\sqrt{-d})$, where $d > 1$ is squarefree, then take $x = \sqrt{-d}$. Then we can find $a, b, c, d \in \mathbb{Z}$, with $(a, b, c, d) = 1$, such that

$$\begin{aligned} xz &= az + b \\ x &= cz + d. \end{aligned}$$

Put $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Then $N_{K/\mathbb{Q}}(x) = \det(\alpha) = ad - bc$. Put $ad - bc = n$, and so n is not a square. Then $\alpha \in \Delta_n$, and $\alpha(z) = z$. Let $\alpha_1, \ldots, \alpha_{\psi(n)}$ be a complete set of inequivalent representatives of Δ_n. Then there exists a $\mu \in \Gamma$ such that $\alpha = \mu\alpha_i$ for some $1 \leq i \leq \psi(n)$. Then

$$j(z) = j(\alpha(z)) = j(\mu\alpha_i(z)) = j(\mu(\alpha_i(z)) = j(\alpha_i(z)),$$

and so $j(z)$ is a zero of the polynomial $\Phi_n(j,j)$ which lies in $\mathbb{Z}[j]$, and has leading coefficient ± 1, by Theorem 1.3.5 (ii), and hence $j(z)$ is an algebraic integer. To show that $j(\tau)$ is also an algebraic integer, we have that $\tau \in \mathbb{Q}(z)$, and so there

exist $r, s \in \mathbb{Q}$ such that $\tau = rz + s$, i.e., $\tau = \beta(z)$ for some primitive $\beta \in GL_2(\mathbb{Z})$. Then $j_\circ\beta$ is integral over $\mathbb{Z}[j]$, since we can assume $\det(\beta) = n$, and then $j_\circ\beta$ is a root of $\Phi_n(X, j)$, which has leading coefficient ± 1, and lies in $\mathbb{Z}[X, j]$. Hence $j(\tau) = j(\beta(z))$ is integral over $\mathbb{Z}[j(z)]$, and so $j(z)$ is also an algebraic integer, as required.

1.4 Modular Functions of level n

We define

$$\Gamma_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; a \equiv d \equiv 1 \,(\mathrm{mod}\, n),\ c \equiv d \equiv 0 \,(\mathrm{mod}\, n) \right\}$$

for n a positive integer. This subgroup of Γ is called the **homogeneous principal congruence subgroup of level n**. Clearly, Γ_n is normal in Γ, and it is also, by definition, the kernel of the natural homomorphism

$$\Gamma \longrightarrow SL_2(\mathbb{Z}_n)$$

where $\mathbb{Z}_n$ denotes the ring of all residue classes modulo n. We have

Theorem 1.4.1: The natural homomorphism

$$\Gamma \longrightarrow SL_2(\mathbb{Z}_n)$$

is surjective.

Proof: Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}_n)$, i.e., $ad - bc \equiv 1 \,(\mathrm{mod}\, n)$. We need to show that there is a matrix $\alpha' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$, i.e., with $a'd' - b'c' = 1$, such that $\alpha \equiv \alpha' \,(\mathrm{mod}\, n)$.

Firstly, from matrix theory, we can diagonalise α, i.e., there exist $\gamma, \gamma' \in SL_2(\mathbb{Z})$ such that $\gamma\alpha\gamma'$ is diagonal, and so if we can find $\beta \in SL_2(\mathbb{Z})$ such that $\beta \equiv \gamma\alpha\gamma' \,(\mathrm{mod}\, n)$, then $\alpha' = \gamma^{-1}\beta\gamma'^{-1}$. Thus we may assume that α is diagonal, so $\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, and $ad \equiv 1 \,(\mathrm{mod}\, n)$. Let

$$\alpha' = \begin{pmatrix} a + xn & yn \\ n & d \end{pmatrix}$$

so $\alpha' \equiv \alpha \,(\mathrm{mod}\, n)$.

We need to find integers x, y such that $\det(\alpha') = 1$. Putting $ad = 1 + qn$, we have that

$$\det(\alpha') = 1 + qn + xdn - yn^2 .$$

Thus, for $\det(\alpha') = 1$, we need to solve

$$q + xd - yn = 0 .$$

Since $(d, n) = 1$, this has a solution for $x, y \in \mathbb{Z}$. This proves the theorem.

Thus, we have that

$$\frac{\Gamma}{\Gamma_n} \cong SL_2(\mathbb{Z}_n).$$

Definition: A function f, meromorphic on $\mathbf{H}$, is called a **modular function of level** n if

(i) $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma_n$, $\tau \in \mathbf{H}$,

(ii) $(f_\circ\gamma)^* = \sum_{n=-m}^{\infty} a_n q^{\frac{1}{n}}$ for all $\gamma \in SL_2(\mathbb{Z})$,

where $q^{\frac{1}{n}} = e^{2\pi i\tau/n}$, and f^* is the meromorphic function induced by f on the punctured disc defined by $\tau \mapsto q^{\frac{1}{n}}$ for $\tau \in \mathbf{H}$ with $\operatorname{Im}\tau > B$.

Theorem 1.4.2: $GL_2(\mathbb{Z}_n) = G_n.SL_2(\mathbb{Z}_n)$ where

$$G_n = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \;\middle|\; d \in (\mathbb{Z}_n)^* \right\}$$

Proof: Let $A \in GL_2(\mathbb{Z}_n)$. Then we can find a matrix $G \in G_n$ such that $|GA| = 1$, i.e., $GA = B$ for some $B \in SL_2(\mathbb{Z}_n)$. Then $A = G^{-1}B$, and $G^{-1} \in G_n$. The product decomposition is clearly unique, hence the result.

CHAPTER 2

The Galois group of the modular equation over $\mathbb{Q}(j)$

We now turn to the result proved by A.M.Macbeath in his paper, [11], namely that

The Galois group of the modular equation $\Phi_n(j(\tau), j(\tau/n)) = 0$, *over* $\mathbb{Q}(j(\tau))$ *is* $PGL_2(\mathbb{Z}_n)$.

Then we have a result from algebraic geometry, Hilbert's irreducibility theorem, which shows that there are infinitely many specialisations of $j(\tau)$ into the rationals

$$j(\tau) \longrightarrow r \in \mathbb{Q}$$

such that $\Phi_n(r, j(\tau/n)) = 0$ also has Galois group $PGL_2(\mathbb{Z}_n)$ over $\mathbb{Q}$.

Macbeath achieves his result by studying sublattices of index n. However, we shall adopt a parallel approach, using the n^{th} division points of elliptic curves, (cf Lang, [9]). We let $F_{n,\mathbf{C}}$ denote the field of modular functions of level n, as defined in chapter 1.4. Then Γ acts as a group of automorphisms of $F_{n,\mathbf{C}}$: Let $f \in F_{n,\mathbf{C}}$, $\gamma \in \Gamma$, $\alpha \in \Gamma_n$. Then, since Γ_n is normal in Γ, we have that $\gamma\alpha = \alpha'\gamma$ for some $\alpha' \in \Gamma_n$. Then

$$f(\gamma\alpha\tau) = f(\alpha'\gamma\tau) = f(\gamma\tau).$$

Thus $f_\circ\gamma$ is invariant under Γ_n. Also, $f_\circ\gamma$ is meromorphic on $\mathbf{H}$, and satisfies the condition about expansions in powers of $q^{\frac{1}{n}}$, $q = e^{2\pi i\tau}$. Thus $f_\circ\gamma$ is a modular function of level n, and so Γ acts by composition as a group of automorphisms of $F_{n,\mathbf{C}}$.

$F_{1,\mathbf{C}}$ is by definition the field of modular functions of level 1, and so by Theorem 1.2.5 we have that

$$F_{1,\mathbf{C}} = \mathbb{C}(j).$$

We shall show that the Galois group of $F_{n,\mathbf{C}}$ over $\mathbb{C}(j)$ is $\frac{SL_2(\mathbb{Z}_n)}{\{\pm 1\}}$.

We define the function

$$f(z;\omega_1,\omega_2) = \frac{g_2(\omega_1,\omega_2)\, g_3(\omega_1,\omega_2)}{\Delta(\omega_1,\omega_2)}\, \wp(z;\omega_1,\omega_2)$$

for $z \in \mathbb{C}$, $\omega_1, \omega_2 \in \mathbf{H}$, and call this function the **Weber function.** Then $f(z;\omega_1,\omega_2)$ is homogeneous of degree 0, since g_2, g_3, Δ and $\wp$ are homogeneous of degrees $4, 6, 12$ and 2 respectively. We then let $f(z;\tau) = f(z;1,\tau)$ for $\tau = \omega_2/\omega_1$, and define $f_{r/n,s/n}(\tau)$ by

$$f_{r/n,s/n}(\tau) = f\left(\frac{r+s\tau}{n};\tau\right)$$

for $1 < n \in \mathbb{N}$, $r, s \in \mathbb{Z}$ not both divisible by n. The function $f_{r/n,s/n}(\tau)$ is called **primitive** if $(r,s,n) = 1$. Since $\wp$ is Λ-periodic, then $f_{r/n,s/n}$ only depends on the residue class of $r, s \bmod n$. Thus we let

$$a = (\frac{a_1}{n}, \frac{a_2}{n}) \in \frac{1}{n}\mathbb{Z}^2,\ \notin \mathbb{Z}^2,$$

and

$$f_a(\tau) = f(a;\tau) = f(\frac{a_1 + a_2\tau}{n};\tau).$$

The functions f_a are called the **Fricke functions**. They are holomorphic on $\mathbf{H}$, since $\Delta(\tau)$ has no zeros, and depend only on the residue class of $a \,(\mathrm{mod}\ \mathbb{Z}^2)$. Clearly

$$f_{a\gamma}(\tau) = f_a(\gamma\tau) \qquad \text{for } \gamma \in \Gamma.$$

We will require a result about the Fourier expansions of the Fricke functions:

Theorem 2.1.1: The Fourier coefficients of the Fricke functions in powers of $q^{\frac{1}{n}} = e^{\frac{2\pi i\tau}{n}}$ belong to the field $\mathbb{Q}(\xi_n)$, where $\xi_n = e^{\frac{2\pi i}{n}}$.

Proof: We need to derive the Fourier expansion for $\wp(z;\tau)$. We use the fact that

$$\sum_{n=-\infty}^{\infty} \frac{1}{(\omega+n)^2} = (2\pi i)^2 \sum_{n=1}^{\infty} n e^{2\pi i n\omega} = (2\pi i)^2 \frac{e^{2\pi i\omega}}{(1-e^{2\pi i\omega})^2}$$

and let $q = e^{2\pi i\tau}$, $q_z = e^{2\pi iz}$.

From the definition of the Weierstrass $\wp$-function, we have that

$$\begin{aligned}
\wp(z;\tau) &= \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left[\frac{1}{(z-m\tau+n)^2} - \frac{1}{(m\tau+n)^2}\right], \\
&= \frac{1}{z^2} + \sum_{m=0}\sum_{n\neq 0} [\quad] + \sum_{m\neq 0}\sum_{n\in\mathbf{Z}} [\quad], \\
&= (2\pi i)^2 \frac{q_z}{(1-q_z)^2} - \frac{2\pi^2}{6} \\
&\qquad + \sum_{m=1}^{\infty}\sum_{n\in\mathbf{Z}} \left[\frac{1}{(z+m\tau+n)^2} + \frac{1}{(-z+m\tau+n)^2} - 2\frac{1}{(m\tau+n)^2}\right], \\
&= (2\pi i)^2 \frac{q_z}{(1-q_z)^2} - \frac{2\pi^2}{6} + (2\pi i)^2 \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n\left(q_z^n q^{nm} + q_z^{-n} q^{nm} - 2q^{mn}\right), \\
&= (2\pi i)^2 \left[\frac{q_z}{(1-q_z)^2} + \frac{1}{12} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} nq^{nm}(q_z^n + q_z^{-n} - 2)\right].
\end{aligned}$$

We also have from 1.2 the expansions for g_2, g_3 and Δ;

$$\begin{aligned}
g_2(\tau) &= \frac{4\pi^4}{3}\left\{1 + 240\sum_{n=1}^{\infty}\sigma_3(n)\,q^n\right\} \\
g_3(\tau) &= \frac{8\pi^6}{27}\left\{1 - 504\sum_{n=1}^{\infty}\sigma_5(n)\,q^n\right\} \\
\Delta(\tau) &= (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)\,q^n
\end{aligned}$$

where $\sigma_\alpha(k) = \sum_{d|k} d^\alpha$ and $\tau(n) \in \mathbb{Z}$, with $\tau(1) = 1$.
Substituting these into the expression for $f(z;\tau)$ gives us the following Fourier expansion;

$$f(z;\tau) = g(q)\left[1 + \frac{12q_z}{(1-q_z)^2} + 12\sum_{r,s=1}^{\infty} sq^{rs}({q_z}^s + {q_z}^{-s} - 2)\right]$$

where $q = e^{2\pi i\tau}$, $q_z = e^{2\pi iz}$, and $g(q) = \sum_{r=1}^{\infty} c_r q^r$, with $c_r \in \mathbb{Z}$, $c_1 = 1$,
Thus, letting $a = \dfrac{a_1 + a_2\tau}{n}$, $\xi_n = e^{\frac{2\pi i}{n}}$,

$$f_a(\tau) = g(q)\left[1 + \frac{12\xi_n^{a_1} q^{\frac{a_2}{n}}}{(1-\xi_n^{a_1} q^{\frac{a_2}{n}})^2} + 12\sum_{r,s=1}^{\infty} sq^{rs}(\xi_n^{sa_1} q^{\frac{sa_2}{n}} + \xi_n^{-sa_1} q^{\frac{-sa_2}{n}} - 2)\right].$$

Since $g(q)$ is a power series in q, with integer coefficients, then $f_a(\tau)$ has a power series in $q^{\frac{1}{n}}$, with coefficients in $\mathbb{Q}(\xi_n)$.

The Fricke functions f_a, for $a \in \frac{1}{n}\mathbb{Z}^2, \notin \mathbb{Z}^2$ are modular functions of level n, since if, for $\gamma \in \Gamma$, $\gamma \equiv 1 (\mathrm{mod}\, n)$, then $a\gamma \equiv a\,(\mathrm{mod}\,\mathbb{Z}^2)$, and so

$$f_a(\gamma\tau) = f_{a\gamma}(\tau) = f_a(\tau)\,,$$

so $f_a(\tau)$ is invariant under Γ_n. Also, since $f_{a\gamma}(\tau) = f_a(\gamma\tau)$, we see that Γ permutes the f_a. Particularly, if $a \in n^{-1}\mathbb{Z}^2$, $\notin \mathbb{Z}^2$, is primitive of level n, i.e., if $a = (a_1/n, a_2/n)$ with $(a_1, a_2, n) = 1$, then $a\gamma$ is primitive of level n, and so Γ permutes the primitive Fricke functions of level n amongst themselves. Thus we see that

$$\mathbb{C}\,(j, f_a | a \in n^{-1}\mathbb{Z}^2,\ \notin \mathbb{Z}^2) \ \subseteq\ F_{n,\mathbf{C}}\,.$$

We have already seen that Γ acts as a group of automorphisms of $F_{n,\mathbf{C}}$, and that Γ_n acts trivially. Thus Γ/Γ_n acts as a group of permutations on $F_{n,\mathbf{C}}$, with kernel containing ± 1. The fixed field is the field of elements invariant under Γ/Γ_n, i.e., the field of modular functions of level 1, which is equal to $\mathbb{C}\,(j)$. Thus we have that $\Gamma/\pm\Gamma_n$ maps onto $\mathrm{Gal}\,(F_{n,\mathbf{C}}/\mathbb{C}(j))$.

We can now prove

Theorem 2.1.2: $F_{n,\mathbf{C}} = \mathbb{C}\,(j, f_a | a \in n^{-1}\mathbb{Z}^2,\ \notin \mathbb{Z}^2)$ and the Galois group of $F_{n,\mathbf{C}}$ over $\mathbb{C}\,(j)$ is

$$\frac{\Gamma}{\pm\Gamma_n} \cong \frac{SL_2(\mathbb{Z}_n)}{\{\pm 1\}}\,.$$

Proof: Let $E = \mathbb{C}\,(j, f_a | a \in n^{-1}\mathbb{Z}^2,\ \notin \mathbb{Z}^2)$ so that $E \subseteq F_{n,\mathbf{C}}$. Since Γ permutes the f_a, then Γ/Γ_n acts as a group of automorphisms of E. Since $\wp$ is even, $\wp(-w) = \wp(w)$, so $f_{-a} = f_a$, i.e. ± 1 act trivially on E. We need to show that if $\gamma \in \Gamma$, and $f_{a\circ}\gamma = f_a$ for all $a \in n^{-1}\mathbb{Z}^2$, $\notin \mathbb{Z}^2$, then $\gamma \in \Gamma_n.\{\pm 1\}$.

Since $\wp\,(u;\Lambda) = \wp\,(v;\Lambda)$ if and only if $u \equiv \pm v\,(\mathrm{mod}\Lambda)$, then

$$f_a = f_b \qquad \Leftrightarrow \qquad a \equiv \pm b (\mathrm{mod}\mathbb{Z}^2)\,.$$

We also have that $f_{a\circ}\gamma = f_{a\gamma}$ for all $\gamma \in \Gamma$, $a \in \mathbb{Q}^2$, $\notin \mathbb{Z}^2$. Thus if γ leaves f_a fixed, then

$$f_a = f_{a\circ}\gamma = f_{a\gamma} \quad \Leftrightarrow \quad a\gamma \equiv \pm a\,(\mathrm{mod}\mathbb{Z}^2)\,.$$

Taking $a = (1/n,\, 0)$ and $(0, 1/n)$, we see that

$$\gamma \equiv \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} (\mathrm{mod} n)\,.$$

Since $\gamma \in \Gamma$, then $\gamma \equiv \pm \mathrm{I}\,(\mathrm{mod} n)$, and hence $\gamma \in \pm\Gamma_n$. Thus the map

$$\frac{\Gamma}{\pm\Gamma_n} \longrightarrow \mathrm{Gal}\,(E/\mathbb{C}\,(j))$$

is injective, with fixed field $\mathbb{C}\,(j)$,, since j is invariant under Γ, but the f_a are permuted by Γ. However, we already have that $|\Gamma/\pm\Gamma_n| \geq |\mathrm{Gal}\,(F_{n,\mathbf{C}}/\mathbb{C}\,(j))|$, and since $E \subseteq F_{n,\mathbf{C}}$, we must have that $E = F_{n,\mathbf{C}}$, and $\mathrm{Gal}\,(F_{n,\mathbf{C}}/\mathbb{C}\,(j)) = \Gamma/\pm\Gamma_n$, and so the theorem is proved.

We now define the extension F_n of $\mathbb{Q}$ to be the field of modular functions of level n with coefficients in their expansions in terms of $q^{\frac{1}{n}}$ in the field $\mathbb{Q}\,(\xi_n)$, and call F_n the **modular function field of level n over** $\mathbb{Q}$. Thus $F_n \subseteq F_{n,\mathbf{C}}$. We also know that $j \in F_n$, since j has rational coefficients in its expansion in powers of q, and that $f_a \in F_n$, from Theorem 2.1.1.

Theorem 2.1.3: (i) $F_n = \mathbb{Q}\,(j, f_a \,|\, a \in n^{-1}\mathbb{Z}^2,\ \notin \mathbb{Z}^2)$,

(ii) $\mathrm{Gal}\ (F_n/\mathbb{Q}\,(j)) = \dfrac{GL_2(\mathbb{Z}_n)}{\{\pm 1\}}$,

(iii) The Galois group of F_n over $\mathbb{Q}\,(j, \xi_n)$ is $\dfrac{SL_2(\mathbb{Z}_n)}{\{\pm 1\}}$.

Proof: (i) The proof of this part is very similar to the proof of Corollary 1.2.8. We know $\mathbb{Q}\,(j, f_a) \subseteq F_n \subseteq \mathbb{C}\,(j, f_a)$. Let $f \in F_n$, and so

$$f = \frac{\phi_1\,(j, f_a)}{\phi_2\,(j, f_a)}\,,$$

where $\phi_1, \phi_2 \in \mathbb{C}\,(j, f_a)$. Thus $f\sum\limits_k c_k\, m_k = \sum\limits_k d_k\, n_k$ where the m_k, n_k are monomials in j and the f_a, i.e., in $\mathbb{Q}\,[\xi_n]((q^{\frac{1}{n}}))$. Let the vector space generated by c_k, d_k over $\mathbb{Q}\,[\xi_n]$ be denoted by $< r_1, \ldots, r_n >$. Thus $c_k = \sum\limits_k \gamma_{kl}\, r_l$, $d_k = \sum\limits_k \delta_{kl}\, r_l$, with $\gamma_{kl}, \delta_{kl} \in \mathbb{Q}\,[\xi_n]$. Then we have that

$$\sum_l \left(\sum_k \gamma_{kl}\, m_k f - \sum_k \delta_{kl}\, n_k \right) r_l = 0\,,$$

where the content of the bracket is in $\mathbb{Q}[\xi_n]((q^{\frac{1}{n}}))$. But the r_l are linearly independent over $\mathbb{Q}[\xi_n]$, and so are linearly independent over $\mathbb{Q}[\xi_n]((q^{\frac{1}{n}}))$, so we must have that $\sum_k \gamma_{kl} m_k f - \sum_k \delta_{kl} n_k = 0$ for all l. But $\sum_k \gamma_{kl} m_k \neq 0$ for some $l = l_0$, and then

$$f = \frac{\sum \delta_{kl_0} n_k}{\sum \gamma_{kl_0} m_k} \in \mathbb{Q}(j, f_a).$$

(ii) Let $G = \mathrm{Gal}(F_n/\mathbb{Q}(j))$. So G contains a copy of $\frac{SL_2(\mathbb{Z}_n)}{\{\pm 1\}}$, which we denote by SL'. We will show that G contains a copy of G_n, where

$$G_n = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix},\ k \in (\mathbb{Z}_n)^* \right\}.$$

We consider the automorphism σ_k of $\mathbb{Q}(\xi_n)$ given by

$$\sigma_k : \xi_n \longrightarrow \xi_n{}^l, \qquad \text{for } k \in (\mathbb{Z}_n)^*, \text{ where } kl \equiv 1 \,(\mathrm{mod}\, n).$$

and extend this automorphism to $f \in F_n$ by defining σ_k as acting on the coefficients of f. This automorphism leaves j fixed, since $j(\tau) \in \mathbb{Q}[[q]]$, $q = e^{2\pi i \tau}$. However, from the expansion of f_a in the proof of Theorem 2.1.1,

$$\sigma_k : f_a(\tau) = f_{\left(\frac{a_1 + a_2\tau}{n}\right)}(\tau) \longrightarrow f_{\left(\frac{a_1 l + a_2 \tau}{n}\right)}(\tau),$$

so σ_k is an permutation of the Fricke functions, leaving $\mathbb{Q}(j)$ fixed. Thus σ_k is an element of G, and since

$$\begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \longrightarrow \begin{pmatrix} a_1 \\ ka_2 \end{pmatrix} = \begin{pmatrix} la_1 \\ a_2 \end{pmatrix},$$

since k is a unit, σ_k is represented by $\begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}$. Thus G contains a copy of G_n, which we denote by G_n'. We have to show how $G_n'.SL'$ acts on G.

We let GL and SL denote $\frac{GL_2(\mathbb{Z}_n)}{\{\pm I\}}$ and $\frac{SL_2(\mathbb{Z}_n)}{\{\pm I\}}$ respectively. Since SL is a normal subgroup of GL, and $SL \cap G_n = \{\pm 1\}$, then every element $g \in GL$ is represented in a unique way as $g = ds$, where $d \in G_n$, $s \in SL$.

We construct a map, σ, from GL to $\mathrm{Gal}(F_n/\mathbb{Q}(j))$ by

$$\sigma : x = ds \longrightarrow d's'$$

where $d' \in G_n'$, $s' \in SL'$. Because of the unique representation of $g = ds$, the map σ is well defined. It remains to show that σ is a homomorphism, i.e., that

$$(d_1 s_1 d_2 s_2)' = d_1' s_1' d_2' s_2'$$

for all $d_1, d_2 \in G_n$, $s_1, s_2 \in SL$. Since SL is a normal subgroup of GL, so that $d_2^{-1} s_1 d_2 \in SL$, we have that

$$(d_1 s_1 d_2 s_2)' = (d_1 d_2 (d_2^{-1} s_1 d_2) s_2)' = d_1' d_2' (d_2^{-1} s_1 d_2)' s_2',$$

so we are required to show that

$$d_1' d_2' (d_2^{-1} s_1 d_2)' s_2' = d_1' s_1' d_2' s_2'$$

i.e.,

$$\begin{aligned} d'(d^{-1} s d)' &= s' d' \\ (d^{-1} s d)' &= d'^{-1} s' d' \end{aligned} \qquad (*)$$

for all $d \in G_n$, $s \in SL$.

We let $f(\tau) = \sum a_r q^{\frac{r}{n}}$ be in F_n, i.e., $a_r \in \mathbb{Q}(\xi_n)$, and $q = e^{2\pi i \tau}$. Then SL acts on F_n by

$$\gamma(f(\tau)) = \sum a_r e^{2\pi i (\frac{a\tau+b}{c\tau+d})\frac{r}{n}} \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in \Gamma.$$

Also, we know that G_n acts on F_n by permuting the coefficients of $f(\tau)$ using

$$\gamma' : \xi_n \longmapsto \xi_n^{\,c}, \text{ where } bc \equiv 1 (\mathrm{mod}\, n), \qquad \text{for} \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} = \gamma' \in G_n.$$

We know that SL is generated by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, by Theorem 1.2.1. Since $(*)$ asserts the equality on two homomorphisms, we only have to prove $(*)$ holds for the generators T, S of SL and a general matrix in G_n. We first consider the case

(1) $d = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$, $b \in (\mathbb{Z}_n)^*$, $s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then we have that $d^{-1} s d = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.

Thus, for $g(\tau) = \sum a_r q^{\frac{r}{n}} \in F_n$ we have that

$$\begin{aligned} s'(g(\tau)) &= \sum a_r q^{\frac{r}{n}} \xi_n^{\,r} \\ d'(g(\tau)) &= \sum a_r' q^{\frac{r}{n}}, \end{aligned}$$

where $a'_r = d'(a_r)$, and $d' : \xi_n \longmapsto \xi_n{}^c$, where $bc \equiv 1 (\mathrm{mod}\, n)$.
So,

$$\begin{aligned}(d^{-1}sd)'(g(\tau)) &= \sum a_r\, e^{2\pi i(\tau+b)\frac{r}{n}} \\ &= \sum a_r\, q^{\frac{r}{n}}\, \xi_n{}^{br}\,.\end{aligned}$$

Also, since $d'^{-1}(a'_r) = a_r$, and $d'^{-1} : \xi_n \longmapsto \xi_n{}^b$,

$$\begin{aligned}d'^{-1}s'd'(g(\tau)) &= d'^{-1}(\sum a_r\, e^{2\pi i(\tau+1)\frac{r}{n}}) \\ &= d'^{-1}(\sum a'_r q^{\frac{r}{n}}\, \xi_n{}^r)\,, \\ &= \sum a_r\, q^{\frac{r}{n}}\, \xi_n{}^{br}\,.\end{aligned}$$

and so $(*)$ holds.

(2) Let d be as above, so d', d'^{-1} acts as before, and let $s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $d^{-1}sd = \begin{pmatrix} 0 & b \\ -1/b & 0 \end{pmatrix}$. Thus we have that

$$s'(g(\tau)) = \sum a_r\, e^{2\pi i(-1/\tau)\frac{r}{n}}\,,$$

$$\begin{aligned}(d^{-1}sd)'(g(\tau)) &= \sum a_r\, e^{2\pi i\left(\frac{b}{-\tau/b}\right)\frac{r}{n}} \\ &= \sum a_r\, e^{2\pi i(-1/\tau)\frac{r}{n}}\,.\end{aligned}$$

Thus,

$$\begin{aligned}d'^{-1}s'd' &= d'^{-1}(\sum a'_r\, e^{2\pi i(-1/\tau)\frac{r}{n}}) \\ &= \sum a_r\, e^{2\pi i(-1/\tau)\frac{r}{n}}\,,\end{aligned}$$

so again $(*)$ holds.
Thus we have a homomorphism from $\dfrac{GL_2(\mathbb{Z}_n)}{\{\pm \mathrm{I}\}}$ into $\mathrm{Gal}\,(F_n/\mathbb{Q}(j))$. Thus

$$G \supseteq \frac{GL_2(\mathbb{Z}_n)}{\{\pm \mathrm{I}\}}\,.$$

Clearly $\mathbb{Q}(j) \subseteq \mathrm{Fix}\left(\dfrac{GL_2(\mathbb{Z}_n)}{\{\pm \mathrm{I}\}}\right)$. Also, the elements of F_n which are fixed under $\dfrac{GL_2(\mathbb{Z}_n)}{\{\pm \mathrm{I}\}}$ are the modular functions with rational coefficients, thus inside $\mathbb{Q}(j)$, by Corollary 1.2.8. Thus $\mathrm{Fix}\left(\dfrac{GL_2(\mathbb{Z}_n)}{\{\pm \mathrm{I}\}}\right) = \mathbb{Q}(j)$, and so

$$G = \mathrm{Gal}\,(F_n/\mathbb{Q}(j)) \cong \frac{GL_2(\mathbb{Z}_n)}{\{\pm \mathrm{I}\}}\,.$$

Hence (ii) is proved.

(iii) We let $K = \mathbb{C} \cap F_n$. Since $j \in \mathbb{Q}[[q]]$, $f_a \in \mathbb{Q}(\xi_n)[[q^{\frac{1}{n}}]]$, then $F_n \subseteq \mathbb{Q}(\xi_n)[[q^{\frac{1}{n}}]]$. Thus $K \subseteq \mathbb{Q}(\xi_n)$. Since $\mathbb{Q}(j)\mathbb{C} = \mathbb{C}(j)$, then $F_{n,\mathbf{C}}$ is the compositum of F_n and $\mathbb{C}$, and so

$$\mathrm{Gal}(F_n/K(j)) \cong \mathrm{Gal}(F_{n,\mathbf{C}}/\mathbb{C}(j)) \cong \frac{SL_2(\mathbb{Z}_n)}{\{\pm 1\}}. \qquad (**)$$

Thus

$$[K:\mathbb{Q}] = [K(j):\mathbb{Q}(j)] = \frac{GL_2(\mathbb{Z}_n)/\{\pm 1\}}{SL_2(\mathbb{Z}_n)/\{\pm 1\}} = |(\mathbb{Z}_n)^*| = [\mathbb{Q}(\xi_n):\mathbb{Q}],$$

so $[K:\mathbb{Q}] = [\mathbb{Q}(\xi_n):\mathbb{Q}]$, and so $K = \mathbb{Q}(\xi_n)$, and by $(**)$,

$$\mathrm{Gal}(F_n/\mathbb{Q}(j,\xi_n)) \cong \frac{SL_2(\mathbb{Z}_n)}{\{\pm 1\}}.$$

This proves (iii).

We now need to show how this is connected to Macbeath's work. Macbeath considers the sublattices, Λ_0, of index n of the lattice $\Lambda(\omega_1, \omega_2)$, defined by

$$\Lambda_0 = \Lambda_0(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$$

where $a, b, c, d \in \mathbb{Z}$, $ad - bc = n \geq 1$, $(a, b, c, d) = 1$. Then $\Lambda/\Lambda_0 \cong \mathbb{Z}_n$, and so we put $E_n = \{\Lambda_0 \subset \Lambda \mid \Lambda/\Lambda_0 \cong \mathbb{Z}_n\}$. Then Macbeath defines his extension L of $\mathbb{Q}(j)$ by

$$L = \mathbb{Q}(j, j(\Lambda_0), \text{ all } \Lambda_0 \in E_n),$$

where $j(\Lambda_0)$ is defined to be $j\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right)$. Let $\alpha_1, \ldots\ldots, \alpha_{\psi(n)}$ be a complete set of coset representations for Δ_n under the action of Γ, as in Theorems 1.3.1, 1.3.2. Then we have

Theorem 2.1.4: $j(\Lambda_0) = j_\circ \alpha_i$ for $\Lambda_0 \in E_n$ and some α_i, $1 \leq i \leq \psi(n)$.

Proof: Let $\Lambda_0 \in E_n$, and let $d > 0$ be the smallest integer such that $d\omega_2 \in \Lambda_0$. Then we can find a basis of Λ_0 in the form $(a\omega_1 + b\omega_2, d\omega_2)$, where $ad = n$ and

$(a,b,d) = 1$. Then $a > 0$ is uniquely determined, but b is only determined modulo d. Thus we choose $0 \leq b \leq d$. Then we have that

$$j(\Lambda_0) = j\left(\frac{a\tau + b}{d}\right) = j_0\alpha_i(\tau)\,,$$

where $ad = n,\ a > 0,\ 0 \leq b \leq d,\ (a,b,d) = 1$, and $1 \leq i \leq \psi(n)$.

Thus we have that

$$L = \mathbb{Q}(j, j(\Lambda_0),\ \text{all}\ \Lambda_0 \in E_n) = \mathbb{Q}(j,\ j_0\alpha_i,\ 1 \leq i \leq \psi(n))\,.$$

Lemma 2.1.5: The functions $j_0\alpha_i$ are modular functions of level n.

Proof: Let $\gamma \in \Gamma_n$, and write $\gamma = I + N\beta$, for some $\beta \in \Gamma$. Then

$$\gamma' = \alpha_i\gamma{\alpha_i}^{-1} = I + N\alpha_i\beta\alpha_i^{-1}$$

has components in $\mathbb{Z}$, and $\det(\gamma') = 1$, so $\gamma' \in SL_2(\mathbb{Z}_n)$. Thus

$$j_0\alpha_i\gamma = j_0\gamma'\alpha_i = j_0\alpha_i\,,$$

so that the $j_0\alpha_i$ are invariant under Γ_n. Also, the $j_0\alpha_i$ are meromorphic on $\mathbf{H}$, and satisfy the condition about expansions in powers of $q^{\frac{1}{n}}$. Thus, the $j_0\alpha_i$ are modular functions of level n.

Lemma 2.1.6: The coefficients of the expansions of $j_0\alpha_i$ in powers of $q^{\frac{1}{n}}$ lie in the field $\mathbb{Q}(\xi_n)$.

Proof: We know that $j(\tau)$ has the expansion $j(\tau) = \sum_{m=-1}^{\infty} c_m\, q^m$, for $q = e^{2\pi i\tau}$, $c_m \in \mathbb{Z}$. Then, since $ad = n$,

$$\begin{aligned}
j\left(\frac{a\tau + b}{d}\right) &= \sum_{m=-1}^{\infty} c_m\, e^{2\pi i m\,(a\tau+b)/d}\,, \\
&= \sum_{m=-1}^{\infty} c_m\, e^{2\pi i m a\tau/d}\, e^{2\pi i m b/d}\,, \\
&= \sum_{m=-1}^{\infty} c_m\, e^{2\pi i m a^2\tau/n}\, e^{2\pi i m a b/n}\,, \\
&= \sum_{m=-1}^{\infty} c_m\, q^{ma^2/n}\, \xi_n^{mab}\,.
\end{aligned}$$

Thus $j\left(\frac{a\tau+b}{d}\right) \in \mathbb{Q}(\xi_n)[[q^{\frac{1}{n}}]]$.

Theorem 2.1.7: Gal $(L/\mathbb{Q}(j)) \cong PGL_2(\mathbb{Z}_n)$.

Proof: From the above two lemmas we have that $j_\circ\alpha_i \in F_n$, and hence that $L \subseteq F_n$. We fix F_n by a subgroup of $\frac{GL_2(\mathbb{Z}_n)}{\{\pm I\}}$, namely $H = \left\{\frac{\lambda I}{\pm 1}\right\}$, where $\lambda \in \mathbb{Z}_n{}^*$. We already know that ± 1 act trivially on F_n. Then, for $h = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$, $r \in \mathbb{Z}_n{}^*$, we have that

$$h(j_\circ\alpha_i) = j_\circ(h\alpha_i) = j(\frac{ar\tau+br}{dr}) = j(\frac{a\tau+b}{d}) = j_\circ\alpha_i\,,$$

and so $j_\circ\alpha_i$ is invariant under H, i.e., $L \subseteq \text{Fix}\, H$. This gives us that $H \subseteq \text{Gal}(F_n/L)$, and thus that $\text{Gal}(L/\mathbb{Q}(j)) \subseteq \frac{GL_2(\mathbb{Z}_n)/\{\pm 1\}}{H} \cong PGL_2(\mathbb{Z}_n)$.

We must now show that $PGL_2(\mathbb{Z}_n)$ acts faithfully on L. Thus we must show that for all $\alpha \in \Delta_n$, for all $\gamma \in PGL_2(\mathbb{Z}_n)$, $\gamma \neq \text{id}$, and for all $\tau \in \mathbf{H}$,

$$\gamma(j(\alpha(\tau))) \neq j(\alpha(\tau))\,,$$

i.e.,

$$j(\gamma\alpha(\tau)) \neq j(\alpha(\tau))\,,$$

i.e., by Theorem 1.2.4,

$$\alpha\gamma^{-1}\alpha^{-1} \notin SL_2(\mathbb{Z})\,.$$

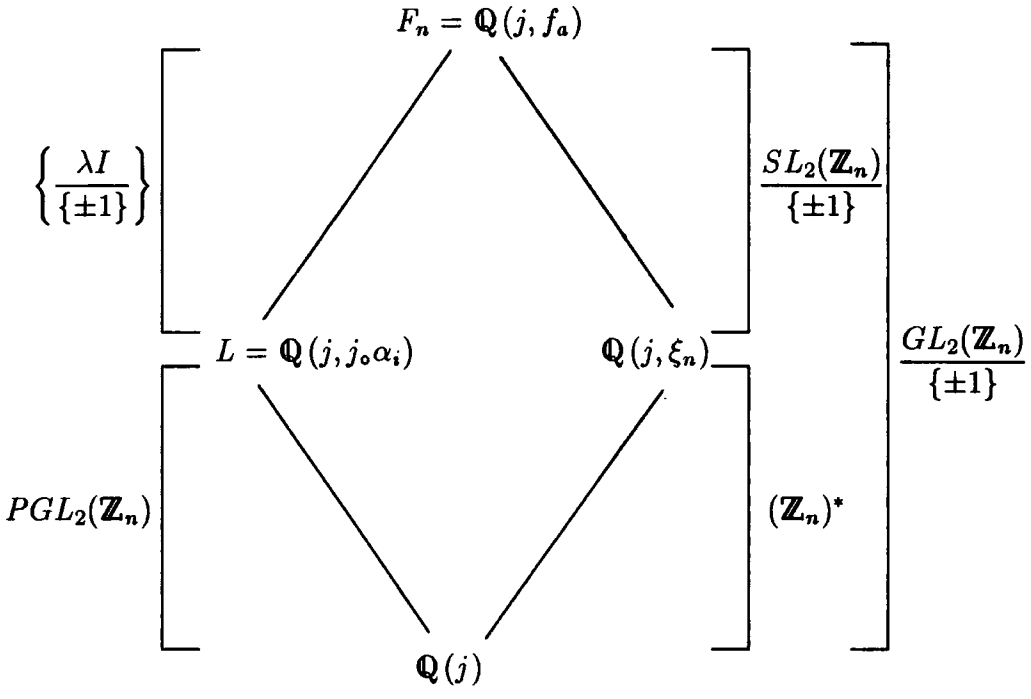
So, suppose that $\alpha\gamma^{-1}\alpha^{-1} \in SL_2(\mathbb{Z})$ for all $\gamma \in PGL_2(\mathbb{Z}_n)$, $\gamma \neq \text{id}$, and for all $\alpha \in \Delta_n$. Letting $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $ad = n$, $a \geq 0$, and $\gamma^{-1} = \begin{pmatrix} u & v \\ x & y \end{pmatrix}$ where $|\gamma| = \pm 1$ and $(u, v, x, y) = 1$, then

$$\begin{aligned} \alpha\gamma^{-1}\alpha^{-1} &= \frac{1}{n}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} u & v \\ x & y \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \qquad (*) \\ &= \frac{1}{n}\begin{pmatrix} adu+bdx & -abu+a^2v-b^2x+aby \\ d^2x & -bdx+ady \end{pmatrix} \end{aligned}$$

We need to find the neccesary conditions on u, v, x, y for $\alpha\gamma^{-1}\alpha^{-1} \in SL_2(\mathbb{Z})$. Choosing $\alpha = \begin{pmatrix} n & b \\ 0 & 1 \end{pmatrix}$ gives us $x \equiv 0 \,(\text{mod}\, n)$ for all $a|n$ and all b. Choosing $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ gives us $v \equiv 0 \,(\text{mod}\, n)$ and $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & n \end{pmatrix}$ gives $u \equiv y \,(\text{mod}\, n)$.

From $(*)$, these three congruences are sufficient for $\alpha\gamma^{-1}\alpha^{-1}$ to be in $SL_2(\mathbb{Z})$. Thus we have that $\gamma^{-1} \equiv \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \bmod n$. But $\gamma^{-1} \in PGL_2(\mathbb{Z}_n)$, and so $\gamma^{-1} = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}$, which means that γ^{-1} and hence γ is the identity element in $PGL_2(\mathbb{Z}_n)$. This contradiction shows that $PGL_2(\mathbb{Z}_n)$ acts faithfully on L, and thus the Galois group of L over $\mathbb{Q}(j)$ is $PGL_2(\mathbb{Z}_n)$.

We have therefore proved Macbeath's result using an alternative method. The situation we have is shown in the following diagram:



CHAPTER 3

Rational values of j where the modular equation has Galois group $PGL_2(\mathbb{Z}_n)$

3.1 Specialisations for fixed n and infinitely many j - an application of Hilbert's Irreducibility Theorem

In his paper, [11], Macbeath uses Hilbert's Irreducibility Theorem, which in its simplest form can be stated as:

Theorem 3.1.1: Let $f(t, X)$ be an irreducible polynomial in $\mathbb{Q}[t, X]$. Then there exist infinitely many rational numbers, t_0, such that $f(t_0, X)$ is irreducible over $\mathbb{Q}$.

This result assures us that there are infinitely many rational values of $j(\tau) = r \in \mathbb{Q}$, such that $\Phi_n(r, j(\tau/n)) = 0$ also has Galois group $PGL_2(\mathbb{Z}_n)$.

To study Hilbert's Irreducibility Theorem, we first of all require some elementary definitions from Algebraic Geometry. We let K be a field, and define **affine n-space over K**, denoted by $\mathbf{A}^n_K$, or just $\mathbf{A}^n$, to be the set of all n-tuples of elements of K.

Let $A = K[x_1, \ldots, x_n]$. We define $f(P) = f(a_1, \ldots, a_n)$ where $f \in A$, $P \in \mathbf{A}^n$, i.e., we view the elements of A as functions from $\mathbf{A}^n$ to A. If $f \in A$ is a polynomial, we define the set of **zeroes** of f by

$$Z(f) = \{P \in \mathbf{A}^n \mid f(P) = 0\}.$$

Also, if $T \subseteq A$, then we define the **zero set of T** to be

$$Z(T) = \{P \in \mathbf{A}^n \mid f(P) = 0 \quad \text{for all } f \in T\}.$$

Definition: A subset S of $\mathbf{A}^n$ is called an **algebraic set** if there exists a subset

$T \subseteq A$ such that $S = Z(T)$.

Definition: A **Zariski open subset** is the complement of an algebraic set.

Thus we have that a set of the form $\mathbf{A}^n \setminus \{P_1, \ldots, P_r\}$ is a Zariski open subset of $\mathbf{A}^n$, where $\{P_1, \ldots, P_r\}$ is a finite set of points in $\mathbf{A}^n$. This defines a topology, i.e., the intersection of two open sets is open, and the union of any number of open sets is open.

Let $f(t_1, \ldots, t_n, X) \in K(t_1, \ldots, t_n)[X]$. We define a **basic Hilbert set**, $U_{f,K}$, by

$$U_{f,K} = \{(t_1', \ldots, t_n'),\ t_1', \ldots, t_n' \in K \mid f(t_1', \ldots, t_n', X) \text{ is irreducible in } K[X] \text{ over } K\}.$$

A **Hilbert subset** of $\mathbf{A}^n$ is defined to be the intersection of a finite number of basic Hilbert sets with a finite number of non-empty Zariski open subsets of $\mathbf{A}^n$. A field K is called **Hilbertian** if the Hilbert subsets of $\mathbf{A}^n$ are non-empty.

Lemma 3.1.2: If K is Hilbertian then every Hilbert subset of $\mathbf{A}^n$ is infinite.

Proof: Let K be Hilbertian, X be a non-empty Hilbert subset of $\mathbf{A}^n$, and suppose that X is *finite*, i.e., $X = \{P_1, \ldots, P_r\}$. Let Z be the non-empty Zariski open subset of $\mathbf{A}^n$ given by $\mathbf{A}^n \setminus \{P_1, \ldots, P_r\}$. Then $X \cap Z$ is the intersection of a Hilbert subset with a non-empty Zariski open subset, so is another Hilbert subset of $\mathbf{A}^n$. But $X \cap Z = \{P_1, \ldots, P_r\} \cap \mathbf{A}^n \setminus \{P_1, \ldots, P_r\} = \emptyset$, contradicting the fact that K is Hilbertian. Thus X is infinite.

We want to show that $U_{f,K}$ is infinite in the case where $K = \mathbb{Q}$ and $n = 1$, i.e., $\mathbf{A}^n = K = \mathbb{Q}$. This is equivalent to showing that $\mathbb{Q}$ is Hilbertian, since if the Hilbert subsets of $\mathbb{Q}$ are infinite, then the $U_{f,K}$ are infinite. Thus we must show that the Hilbert subsets are non-empty.

Suppose that $f(t, X) \in \mathbb{Q}(t)[X]$, i.e., its coefficients are in $\mathbb{Q}(t)$, and that $f(t, X)$ is irreducible over $\mathbb{Q}(t)$. Then we can multiply f by a suitable polynomial to make the coefficients lie in $\mathbb{Q}[t]$ without changing this irreducibility. Dividing the resulting polynomial by the greatest common divisor of its coefficients gives us a polynomial

in $\mathbb{Q}[t, X]$ which is irreducible over $\mathbb{Q}$. Conversely, if $f(t, X) \in \mathbb{Q}[t, X]$ is irreducible over $\mathbb{Q}$, then it is irreducible in $\mathbb{Q}(t)[X]$. Let $f(t, X) \in \mathbb{Q}(t, X)$ be an irreducible polynomial. If t is transcendental over $\mathbb{Q}$, then we call the curve defined by the equation $f(t, X) = 0$ an **affine plane curve**, C. For $R \subseteq \mathbb{Q}$, we define $U_{t,R}(C)$ by

$$U_{t,R}(C) = \{t_0 \in R \,|\, \text{there is no } P \in C(\mathbb{Q}) \text{ such that } t(P) = t_0\}$$

Then we have

Lemma 3.1.3: Every Hilbert subset of $\mathbb{Q}$ contains a finite intersection of $U_{t,R}(C)$ for a finite number of affine plane curves C over $\mathbb{Q}$.

Proof: We let $f(t, X) \in \mathbb{Q}[t, X]$ be irreducible over $\mathbb{Q}(t)$, and write

$$f(t, X) = a_n(t)X^n + \cdots + a_0(t),$$

so $a_i(t) \in \mathbb{Q}[t]$. Suppose f has factorisation

$$f(X) = a_n(t) \prod_{i=1}^{n} (X - \alpha_i)$$

in the algebraic closure of $\mathbb{Q}(t)$. Then choosing $t = t_0$ where $t_0 \in \mathbb{Q}$ gives a homomorphism $\mathbb{Q}[t] \longmapsto \mathbb{Q}[t_0] = \mathbb{Q}$. We choose the values $t_0 \in \mathbb{Q}$ such that $a_n(t_0) \neq 0$. Then the homomorphism can be extended to the ring generated by the roots $\alpha_1, \ldots, \alpha_n$ of f, because these roots are integral over $\mathbb{Q}[t, a_n(t)^{-1}]$. Let $\alpha_1', \ldots, \alpha_n'$ be the images of these roots. If $f(t_0, X)$ factorizes as

$$f(t_0, X) = g_0(X)h_0(X)$$

in $\mathbb{Q}[X]$, then the coefficients of g_0 and h_0 are polynomial functions of the α_i'. This gives rise to a factorisation of $f(t, X)$,

$$f(t, X) = g(X)\, h(X)$$

in the algebraic closure of $\mathbb{Q}(t)$, where g, h are polynomials corresponding to g_0, h_0. Since f is irreducible over $\mathbb{Q}(t)$ then at least one of the coefficients of g or h cannot lie in $\mathbb{Q}(t)$. Suppose $u \notin \mathbb{Q}(t)$, where u is a coefficient of g or h. Then the ring $\mathbb{Q}[t, u]$ is the affine ring of a curve C over $\mathbb{Q}$. The factorisation $f(t_0, X) = g_0(X)h_0(X)$ thus gives us a point (t_0, y_0) on C, with $t_0, y_0 \in \mathbb{Q}$.

Writing $f(t,X) = g(X)h(X)$ in all possible ways in the algebraic closure of $\mathbb{Q}(t)$, with degree g, degree $h \geq 1$ will give rise each time to a coefficient of g or h which does not lie in $\mathbb{Q}(t)$. Thus we will obtain a finite number of curves C_i, with affine rings $\mathbb{Q}[t,u_i]$, where $u_i \notin \mathbb{Q}(t)$. Thus, any $t_0 \in \mathbb{Q}$ such that there is no point (t_0,y_0) on any C_i, with $y_0 \in \mathbb{Q}$, will be such that $f(t_0,X)$ is irreducible in $\mathbb{Q}[X]$. Since a Hilbert subset contains a finite intersection of basic Hilbert sets, it must contain a finite intersection of $U_{t,R}(C)$, as required.

We let (t,y) be a point of an affine plane curve C over $\mathbb{Q}$, with $y \notin \mathbb{Q}(t)$. We may assume that y is integral over $\mathbb{Z}[t]$, since if it is not, we may multiply y by a suitable polynomial in $\mathbb{Z}[t]$ so that it is. Since y is integral over $\mathbb{Z}[t]$, then y can be expressed as an algebraic function of t over $\mathbb{R}$, and so has an expansion at infinity:

$$y = y(t) = at^{\frac{n}{e}} + \cdots + b + c\frac{1}{t^{\frac{1}{e}}} + \cdots$$

with $a,b,c,\ldots \in \mathbb{C}$. We choose $t^{\frac{1}{e}}$ to be real. Then, if there are infinitely many values of t tending to infinity in $\mathbb{R}$ such that $y(t)$ is real, then the coefficients $a,b,c,\ldots$ are in fact real. For, if any one of the coefficients were not real, then it would dominate the series to the right of it as t tends to infinity, so there could not be any cancellations, and so $y(t)$ would not be real.

We require the following lemma:

Lemma 3.1.4: Let the function $y(t)$ be m times continuously differentiable in the interval $t_i \leq t \leq t_{i+m}$. Suppose $t_i < t_{i+1} < \ldots < t_{i+m}$, where $t_i,,t_{i+1},\ldots,t_{i+m} \in \mathbb{R}$. Then there exists a τ with $t_i < \tau < t_{i+m}$ such that

$$\frac{y^{(m)}(\tau)}{m!} = \frac{U_m}{V_m}$$

where

$$U_m = \begin{vmatrix} 1 & t_i & {t_i}^2 & \cdots & {t_i}^{m-1} & y(t_i) \\ \vdots & & & & & \vdots \\ 1 & t_{i+m} & {t_{i+m}}^2 & \cdots & {t_{i+m}}^{m-1} & y(t_{i+m}) \end{vmatrix},$$

and V_m is the Vandermonde determinant,

$$V_m = \begin{vmatrix} 1 & t_i & {t_i}^2 & \cdots & {t_i}^{m-1} & {t_i}^m \\ \vdots & & & & & \vdots \\ 1 & t_{i+m} & {t_{i+m}}^2 & \cdots & {t_{i+m}}^{m-1} & {t_{i+m}}^m \end{vmatrix}.$$

Proof: We let

$$F(t) = \begin{vmatrix} 1 & t_i & {t_i}^2 & \cdots & {t_i}^{m-1} & y(t_i) \\ \vdots & & & & & \vdots \\ 1 & t_{i+m} & {t_{i+m}}^2 & \cdots & {t_{i+m}}^{m-1} & y(t_{i+m}) \\ 1 & t & t^2 & \cdots & t^{m-1} & y(t) \end{vmatrix}$$

Then $F(t) = 0$ when $t = t_i, \ldots, t_{i+m-1}$. Then the function

$$G(t) = F(t) - c\,(t - t_i)\,(t - t_{i+1}) \ldots (t - t_{i+m-1})$$

will also vanish at $t = t_{i+m}$, for some constant c. Thus $G(t) = 0$ for $m + 1$ values of t between t_i and t_{i+m}. By Rolle's theorem, there is at least one value of t, $t = \tau$ say, between t_i and t_{i+m} such that $G^{(m)}(\tau) = 0$. But $G^{(m)}(t) = F^{(m)}(t) - m!c$. Thus

$$F^{(m)}(\tau) = m!c\,.$$

Also, $F^{(m)}(\tau) = y^{(m)}(\tau)V_{m-1}$, since $F^{(m)}(\tau)$ has a zero everywhere in the bottom row except for the last term, which is $y^{(m)}(\tau)$. Thus

$$m!c = y^{(m)}(\tau)V_{m-1}$$

But

$$c = \frac{F(t_{i+m})}{(t_{i+m} - t_i) \ldots (t_{i+m} - t_{i+m-1})}$$

and $(t_{i+m} - t_i) \ldots (t_{i+m} - t_{i+m-1})V_{m-1} = V_m$. Since $F(t_{i+m}) = U_m$, we have our result.

We use this to prove

Theorem 3.1.5: Let $y(t)$ be a function of a real variable, with expansion

$$y(t) = at^{\frac{n}{e}} + \cdots + b + c\frac{1}{t^{\frac{1}{e}}} + \cdots$$

where $a, b, c, \ldots, t^{\frac{1}{e}} \in \mathbb{R}$, and converging for all sufficiently large values of t. Assume $y\,(t) \notin \mathbb{R}\,[t]$. Suppose there are infinitely many $t_i \in \mathbb{Z}^+$, with $t_0 < t_1 < \ldots$, such that $y\,(t_i) \in \mathbb{Z}$. Then there exists an $i_0 \in \mathbb{Z}$, $0 < m \in \mathbb{Z}$ and $0 < s \in \mathbb{R}$ such that for all $i > i_0$,

$$t_{i+m} - t_i > {t_i}^s\,.$$

Proof: Let $0 < m \in \mathbb{Z}$ be such that $y^{(m)}(t)$ has no positive powers of $t^{\frac{1}{e}}$, hence

$$y^{(m)}(t) = d\frac{1}{t^s} + \cdots$$

with $d \in \mathbb{R}$. Since $y(t) \notin \mathbb{R}[t]$, $y^{(m)}(t) \neq 0$, so we can assume $d \neq 0$, and $s > 0$. Thus, $y^{(m)}(\tau)$ is small, and $\frac{y^{(m)}(\tau)}{m!}$ is of order τ^{-s}. But

$$\frac{y^{(m)}(\tau)}{m!} = \frac{U_m}{V_m}$$

and V_m is the product of $\frac{m(m+1)}{2}$ differences of the $t_i, \ldots, t_{i+m}$. Thus, for a constant A,

$$(t_{i+m} - t_i)^{\frac{m(m+1)}{2}} > \prod_{i \leq j_1 < j_2 \leq i+m} (t_{j_2} - t_{j_1}) = |V_m| \approx |AU_m \tau^s| .$$

But, $U_m \in \mathbb{Z}$, since the t_i are positive integers, and we know that $t_i < \tau < t_{i+m}$. Thus

$$t_{i+m} - t_i > \sqrt[\frac{m(m+1)}{2}]{|U_m| {t_i}^s}$$

and so

$$t_{i+m} - t_i > {t_i}^{s'}$$

where $s' = \frac{2s}{m(m+1)} > 0$.

We require two corollaries:

Corollary 3.1.6: Let $y(t) = at^{\frac{n}{e}} + \cdots + b + c\frac{1}{t^{\frac{1}{e}}} + \cdots$. Then there exists $\alpha \in \mathbb{R}$ with $0 < \alpha < 1$ such that the number of $t_i \leq B$ for which $y(t_i) \in \mathbb{Z}$ is less than B^α for all B sufficiently large.

Proof: Let $0 < \beta < 1$. Let

N = the number of integers t_i such that $t_i \leq B$,

N_1 = the number of integers t_i such that $t_i \leq B^\beta + 1$,

N_2 = the number of integers t_i such that $B^\beta < t_i < B$.

Write $N_2 = um + m_0$, where $u \geq 0$, and $0 \leq m_0 < m$. By the theorem, $t_{i+m} > t_i + {t_i}^s$. Thus

$$t_{i+um} > t_i + u{t_i}^s .$$

Choosing B large enough, and β small enough that $B \geq t_{i+um}$, and $t_i \geq B^\beta$, we have that $B \geq B^\beta + uB^{\beta s}$ thus $u \leq B^{1-\beta s}$. Thus,

$$N \leq N_1 + N_2 \leq B^\beta + 1 + mB^{1-\beta s} + m_0 ,$$

and so $N \leq B^{\alpha}$ for some $0 < \alpha < 1$.

Corollary 3.1.7: Let U be a Hilbert subset of $\mathbb{Q}$. Then there exists an $\alpha \in \mathbb{R}$, with $0 < \alpha < 1$ such that the number of positive integers $\leq B$ in U is at least

$$B - B^{\alpha}$$

for all B sufficiently large.

Proof: By Lemma 3.1.3, Hilbert subsets of $\mathbb{Q}$ contain a finite intersection of sets

$$U_{t,\mathbf{Z}}(C) = \{t_i \in \mathbb{Z} \,|\, \text{there is no } P \in C(\mathbb{Q}) \text{ such that } t(P) = t_i\}$$

for a finite number of affine plane curves over $\mathbb{Q}$. By the above corollary, there exists as $\alpha \in \mathbb{R}$, $0 < \alpha < 1$, such that the number of $t_i \leq B$ such that $y(t_i) \notin \mathbb{Z}$ is at least $B - B^{\alpha}$. Since $y(t_i)$ is integral over $\mathbb{Z}[t]$, then if $(t_i, y(t_i)) \in C$, with $t_i, y(t_i) \in \mathbb{Q}$, then $y(t_i) \in \mathbb{Z}$ if $t_i \in \mathbb{Z}$. Thus $y(t_i) \notin \mathbb{Z}$ for $t_i \in \mathbb{Z}$ means that $(t_i, y(t_i))$ is not on C. Thus $U_{t,\mathbf{Z}}(C)$, and so U, contains at least $B - B^{\alpha}$ positive integers.

Since $0 < \alpha < 1$, then $B - B^{\alpha} > 1$ for B sufficiently large, and so the Hilbert subsets are non-empty, and so we have that $\mathbb{Q}$ is Hilbertian. Thus we have proved Theorem 3.1.1. Then we have

Theorem 3.1.8: $\mathrm{Gal}(\Phi_n(j(\tau_0), X)/\mathbb{Q}) = PGL_2(\mathbb{Z}_n)$ for infinitely many $j(\tau_0) \in \mathbb{Q}$.

Proof: We have our extension of $\mathbb{Q}(j(\tau))$, $L = \mathbb{Q}(j(\tau), j_o\alpha_i(\tau)$, $1 \leq i \leq \psi(n))$, which is clearly a finite separable extension of $\mathbb{Q}(j(\tau))$, since the minimum polynomial of the $j_o\alpha_i(\tau)$ is

$$\Phi_n(j(\tau), X) = \prod_{i=1}^{\psi(n)} (X - j_o\alpha_i(\tau))$$

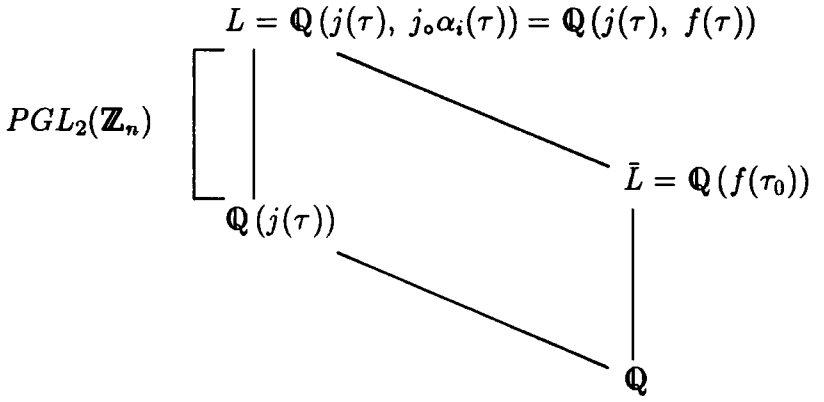
which has no multiple roots since the $j_o\alpha_i(\tau)$ are all distinct. By Galois theory, we know that every finite separable extension is a simple extension, thus we can find an element $f(\tau)$ such that $L = \mathbb{Q}(j(\tau), f(\tau))$. We denote the minimum polynomial of $f(\tau)$ over $\mathbb{Q}(j(\tau))$ by $\phi(j(\tau), X)$, and thus $\phi(j(\tau), X)$ will have degree equal to

$|PGL_2(\mathbb{Z}_n)|$.

We now specialize $j(\tau)$ into the rationals, i.e., choose a $\tau_0 \in \mathbf{H}$ such that $j(\tau_0) \in \mathbb{Q}$. This will give us an extension $\bar{L} = \mathbb{Q}(f(\tau_0))$ over $\mathbb{Q}$ with Galois group a subgroup of $PGL_2(\mathbb{Z}_n)$. Then $f(\tau_0)$ will have a minimum polynomial over $\mathbb{Q}$, denoted by $\bar{\phi}(X)$. But $f(\tau_0)$ is also a root of $\phi(j(\tau_0), X)$, and so by Galois theory again,

$$\bar{\phi}(X) \mid \phi(j(\tau_0), X) \qquad (*)$$

Since $\phi(j(\tau), X)$ is irreducible over $\mathbb{Q}(j(\tau))$, we can apply Hilbert's Irreducibility Theorem to give us that there are infinitely many $j(\tau_0) \in \mathbb{Q}$ such that $\phi(j(\tau_0), X)$ is irreducible over $\mathbb{Q}$. In these cases, by $(*)$, we must have that $\bar{\phi}(X) = \phi(j(\tau_0), X)$, so $|\bar{\phi}(X)| = |PGL_2(\mathbb{Z}_n)|$, and so the Galois group of $\bar{L}$ over $\mathbb{Q}$ is also $PGL_2(\mathbb{Z}_n)$.



Thus we have shown that there are infinitely many rational values of $j(\tau)$ which still give us extensions with Galois group $PGL_2(\mathbb{Z}_n)$.

3.2 Infinitely many primes n for a fixed value of j - an application of the reduction of elliptic curves.

In the previous section we proved that for a fixed n there are infinitely many rational values of j where the Galois group does not collapse. There is an alternative result, namely that for a fixed $j = r \in \mathbb{Q}$, the set of primes p for which the Galois group of $\Phi_p(r, j(\tau/p))$ *does* collapse is finite. We now study this result, and describe the proof, the details of which can be found in Lang, [9]. This result is also proved by Serre in [18].

Let E be an elliptic curve, i.e., a non-singular curve of genus 1, with a rational point taken as an origin. We say that E is **defined over a field** K if the coefficients of the defining equation lie in K. Any elliptic curve defined over K where char $K \neq 2, 3$ can be defined by a Weierstrass equation

$$y^2 = 4x^3 - g_2 x - g_3 \,,$$

where $g_2,\ g_3 \in K$. If $K = \mathbb{C}$, then the map

$$z \mapsto (\wp(z), \wp'(z))$$

parametrises points on E. Let $\Lambda(\omega_1, \omega_2)$ be the lattice defined by the periods ω_1, ω_2 of the Weierstrass $\wp$-function, and let E_K be the set of points (x, y) on E, where $x, y \in K$. Then the map

$$\alpha : \mathbb{C}/\Lambda \longrightarrow E_{\mathbf{C}}$$

is a bijection.

Suppose E is an elliptic curve over K, as above. For each $n \in \mathbb{Z}^+$, we denote by E_n the kernel of the map

$$z \mapsto nz \,,$$

for $z \in E$. Thus E_n is the subgroup of points of order n. If E is defined over $\mathbb{C}$, then since $E_{\mathbf{C}} \cong \mathbb{C}/\Lambda$, we have that

$$E_n \cong \mathbb{Z}_n \otimes \mathbb{Z}_n$$

If E is defined over a field of characteristic zero, then we can embed the field of definition of the curve in $\mathbb{C}$ and obtain the same result.

Now let E be defined over a field K, and let L be a field extension of K. Suppose σ is any automorphism of L. Then, applying σ to the coefficients of the defining equation for E, we obtain a new curve, which we denote by E^σ. Thus, if E is defined by $y^2 = 4x^3 - g_2x - g_3$, then E^σ is defined by $y^2 = 4x^3 - g_2^\sigma x - g_3^\sigma$. Also, if $P = (x, y)$ is a point on E, then $P^\sigma = (x^\sigma, y^\sigma)$ is a point on E^σ.

Let σ be an automorphism of L keeping K fixed, i.e., $\sigma \in \mathrm{Gal}(L/K)$, and so $E^\sigma = E$. Suppose P is a point of finite order on E, so that $nP = 0$ for some positive integer n. Then $nP^\sigma = 0$, so that P^σ is also a point of order n, and so σ permutes the points of order n. Let $P = (x, y)$, and $K(P) = K(x, y)$, so that $K(P)$ is the extension of K obtained by ajoining the coordinates of P. We then define the **field of n-th division points** of E over K, $K(E_n)$, to be the compositum of the fields $K(P)$ for all $P \in E_n$. Since the coordinates of P are taken to be in the algebraic closure of K, denoted by K_a, then we have that the elements of the Galois group of K_a over K are automorphisms of E_n. Thus, for $\mathrm{char}\, K = 0$, $K(E_n)$ is a Galois extension of K. Letting σ be represented by $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with respect to the pair of generators $\{P_1, P_2\}$ for E_n over $\mathbb{Z}_n$, then since

$$\begin{pmatrix} {P_1}^\sigma \\ {P_2}^\sigma \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix},$$

M must be in $GL_2(\mathbb{Z}_n)$, and so we have an injection from $\mathrm{Gal}(K(E_n)/K)$ into $GL_2(\mathbb{Z}_n)$.

To consider the question of when the Galois group is the whole group $GL_2(\mathbb{Z}_n)$, Lang considers a transformation of the Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$ by the translations

$$X = x - \frac{1}{12}, \qquad Y = \frac{y}{2} + \frac{1}{2}\left(x - \frac{1}{12}\right).$$

This transformation gives the equation

$$Y^2 - XY = X^3 - h_2X - h_3,$$

which is known as a **Tate equation**. In the proof of Theorem 2.1.1 we had

$$\wp(z;\tau) = \frac{1}{12} + \frac{q_z}{(1-q_z)^2} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} nq^{nm}({q_z}^n + {q_z}^{-n} - 2),$$

and so

$$\wp'(z;\tau) = \sum_{m\in\mathbb{Z}} \frac{q^m q_z(1+q^m q_z)}{(1-q^m q_z)^3}.$$

Rearranging, and putting $q_z = w$, gives

$$\begin{aligned} x(w) &= \frac{1}{12} + \sum_{m\in\mathbb{Z}} \frac{q^m w}{(1-q^m w)^2} - 2\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}, \\ y(w) &= \sum_{m\in\mathbb{Z}} \frac{q^m w(1+q^m w)}{(1-q^m w)^3}. \end{aligned}$$

Thus

$$\begin{aligned} X(w) &= \sum_{n\in\mathbb{Z}} \frac{q^n w}{(1-q^n w)^2} - 2\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}, \\ Y(w) &= \sum_{n\in\mathbb{Z}} \frac{(q^n w)^2}{(1-q^n w)^3} - \sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}. \end{aligned}$$

The Tate equation defines an elliptic curve, known as a Tate curve, over any field K which is complete under a non-archimedian absolute value, provided that $q \in K$ is such that $0 < |q| < 1$, and $w \in K^*$ is such that $|q| < |w| < |q|^{-1}$. These conditions ensure that the series for $X(w)$ and $Y(w)$ converge absolutely.

Suppose E is such a Tate curve over a suitable field K, as described above, with invariant $j(q)$ for a $q \in K$ such that $0 < |q| < 1$. Let K^* be the multiplicative group of invertible elements in K, and C_q be the infinite cyclic group generated by q in K^*. We then define the **Tate mapping**, ψ, by

$$\begin{aligned} \psi(w) &= (X(w), Y(w)) \quad \text{if} \quad w \notin C_q, \\ \psi(w) &= 0 \quad \text{if} \quad w \in C_q. \end{aligned}$$

This map is a homomorphism from K^* into E_K, with kernel C_q. Let $C_q^{\frac{1}{n}}$ be the subgroup of K^* consisting of elements of K^* whose n-th power is in C_q. Then $C_q^{\frac{1}{n}}$ is generated by a n-th root of unity, ξ_n, and an n-th root of q, $q^{\frac{1}{n}}$ say. Lang then proves, ([9], p.203, Theorem 3):

Theorem 3.2.1: For n prime to char$K$, the Tate mapping defines a Galois isomorphism from $C_q^{\frac{1}{n}}/C_q$ to E_n, and

$$K(E_n) \cong K(\xi_n, q^{\frac{1}{n}}).$$

We shall require one more result, namely for which primes p the subgroup E_p is irreducible as a module over the Galois group. Let E be an elliptic curve defined over K, O the ring of integers of K, O_p the local ring for some prime p of K, and m_p the maximal ideal of O_p. We say that E has **good reduction** at p if E is isomorphic over K to a curve f such that reducing $f \bmod m_p$ gives again a (non-singular) elliptic curve. If the curve is defined by a Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$, with $g_2,\ g_3 \in O_p$, and if p does not divide 2 or 3, then E has good reduction if the discriminant Δ is a unit in O_p. Let $E,\ F$ be elliptic curves over K. Then F is **isogenous** to E if there is a map from E to F with finite kernel. An important result, proved by Serre and Tate, ([16] p.IV-5, Corollary), is;

Theorem 3.2.2: If $E,\ F$ are elliptic curves defined over K, and F is isogenous to E over K, then if E has good reduction at a prime p of K, so does F.

Theorem 3.2.3: Let S be a finite set of primes of K. The set of isomorphism classes of elliptic curves over K having good reduction at all primes of K not in S is finite.

Theorem 3.2.2 implies

Corollary 3.2.4: Let E be an elliptic curve over K. Then there are only a finite number of non-isomorphic curves which are isogenous to E over K.

Let E be an elliptic curve over K isomorphic to $\mathbb{C}/\Lambda$. Then the endomorphisms of E, End(E), are given by $\{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$. E is said to have have **complex multiplication** if the ring of endomorphisms is bigger than $\mathbb{Z}$.

Lemma 3.2.5: Suppose E is an elliptic curve over K, with no complex multiplication, i.e., End(E) $\cong \mathbb{Z}$, and suppose $F,\ G$ are elliptic curves isogenous to E over K. Choose isogenies $X : F \to E,\ Y : G \to E$ with cyclic kernels. If these kernels are not isomorphic, then F and G are not isomorphic over K.

Proof: Let the kernels of the isogenies X, Y have order f, g respectively, and suppose that F and G are isomorphic, so let $Z : F \to G$ be an isomorphism. Then there will be an isogeny $X' : E \to F$, with cyclic kernel f, and so the composition $X'ZY$ gives an isogeny from $E \to E$, with kernel $\frac{\mathbb{Z}}{f\mathbb{Z}} \otimes \frac{\mathbb{Z}}{g\mathbb{Z}}$. However, $\mathrm{End}(E) = \mathbb{Z}$, so this isogeny must be multiplication by an integer e, and hence the kernel must be of the form $\frac{\mathbb{Z}}{e\mathbb{Z}} \otimes \frac{\mathbb{Z}}{e\mathbb{Z}}$. Thus f and g divide e, and $e^2 = fg$, giving $e = f = g$, contradicting the fact that X, Y have non-isomorphic cyclic kernels.

Suppose E is an elliptic curve over K without complex multiplication, and E_p is the subgroup of points of order p. Let $G = \mathrm{Gal}(K_a/K)$. Then W is said to be a **G-subspace** of E_p if $gW \subseteq W$ for all $g \in G$. Then E_p is **G-irreducible** if it has no proper G-subspaces. Now we have

Theorem 3.2.6: E_p is G-irreducible for almost all primes p.

Proof: Suppose E_p is reducible, and so must have a one-dimensional G-subspace, W_p, which is cyclic of order p. Then E/W_p is an elliptic curve, which is isogenous to E over K. By the above lemma, curves E/W_p are non-isomorphic for different values of p. By Corollary 3.2.4, there are only a finite number of elliptic curves E/W_p, therefore E_p is reducible for only finitely many p.

Now we can get to our main result. Suppose E is an elliptic curve over a field K, with invariant $j = j(q)$ which is not integral at some prime p of K. Thus E has no complex multiplication. We define the completion K_p of K by

$$K_p = \mathbb{Q}_p \otimes K\,,$$

where $\mathbb{Q}_p$ is the field of p-adic numbers. Let $\mathbf{F}_l$ denote the field $\mathbb{Z}/l\mathbb{Z}$.

Theorem 3.2.7: Let E be an elliptic curve with non integral j invariant over a number field K, and $q = \pi^e u$, where u is a unit in K_p, and e is the order of q at (π). Then the Galois group of $K(E_l)$ over K is $GL_2(\mathbf{F}_l)$ for all primes l satisfying

(i) l does not divide e,

(ii) l is such that there is no curve isogenous to E where the degree of the isogeny is equal to l,

(iii) l does not divide the absolute discriminant of the field K.

Proof: We look at the local extension, $K_p(E_l)$ over K_p, and show that this contains $SL_2(\mathbf{F}_l)$ for almost all primes l, so that the global extension, $K(E_l)$ over K, also contains $SL_2(\mathbf{F}_l)$ for almost all l, since

$$\mathrm{Gal}\,(K_p(E_l)/K_p) \subseteq \mathrm{Gal}\,(K(E_l/K)\,.$$

Let G =Gal $(K(E_l)/K)$, G' =Gal $(K_p(E_l)/K_p)$, and so G' acts on E_l. Now, $q = \pi^e u$, and we know that

$$j = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n\,,$$

where $c_n \in \mathbf{Z}$. Thus we have that $q \in K$ with $0 < |q| < 1$. Also, to find e, we simply take the power of p which exactly divides the denominator of j. By Theorem 3.2.1 we have that E_l is Galois isomorphic to $C_q^{\frac{1}{n}}/C_q$ and that $K_p(E_l) \cong K_p(\xi_l,\, q^{\frac{1}{l}})$. Now, for all l not dividing e, there is an automorphism, σ, of $K_p(\xi_l,\, q^{\frac{1}{l}})$ over K_p such that

$$\begin{aligned} \sigma\xi_l &= \xi_l\,, \\ \sigma q^{\frac{1}{l}} &= \xi_l q^{\frac{1}{l}}\,, \end{aligned}$$

and this automorphism may be represented by the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

with respect to the basis $\{\xi_l, q^{\frac{1}{l}}\}$. Thus G', and hence G, contains the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ with respect to $\{\xi_l, q^{\frac{1}{l}}\}$. However, we know that E_l is G-irreducible for almost all l, by Theorem 3.2.6, and so for an l where E_l is G-irreducible there must be an element, δ say, of G such that $\delta\xi_l \notin \{\xi_l\}$, otherwise E_l would have a proper G-subspace. Thus $\delta\xi_l = \xi_n{}^r\, q^{s/l}$ where $s \not\equiv 0 \,(\mathrm{mod}\, l)$. Let $\delta\xi_l = \nu$. Then

$$\begin{aligned} \delta\sigma\delta^{-1}\nu &= \delta\sigma\xi_l \\ &= \delta\xi_l \\ &= \nu\,. \end{aligned}$$

Thus $\sigma' = \delta\sigma\delta^{-1}$ leaves ν fixed. We choose the basis $\{\xi_l, \nu\}$, and so with respect to this basis σ and σ' are represented by the matrices $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ and

$C = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$, with $b, c \neq 0$ since σ and σ' are non-trivial automorphisms. Then $B^x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $C^y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ for $bx \equiv cy \equiv 1 \,(\mathrm{mod}\, l)$. But these two matrices generate $SL_2(\mathbf{Z})$, and hence generate $SL_2(\mathbf{F}_l)$, and so G contains a copy of $SL_2(\mathbf{F}_l)$.

Also, $K(E_l) \cong K(\xi_l, q^{\frac{1}{l}})$, so that $K(E_l)$ contains the l-th roots of unity. For all l such that $l \not| \Delta(K)$ we have that $|K(\xi_l) : K| = l - 1$, and so G contains a copy of $(\mathbf{F}_l)^*$. Since $GL_2(\mathbf{F}_l) = SL_2(\mathbf{F}_l) \,.\, (\mathbf{F}_l)^*$, where $SL_2(\mathbf{F}_l) \cap (\mathbf{F}_l)^* = \{1\}$, then we have our result.

We now take $K = \mathbb{Q}$, and so condition (iii) is satisfied for all l. Let $E(j)$ be an elliptic curve defined over $\mathbb{Q}$, having invariant j, and described by $Y^2 = 4X^3 - aX - b$. Choose an l which also satisfies conditions (i) and (ii). Then $\mathrm{Gal}(\mathbb{Q}(E_l)/\mathbb{Q}) = GL_2(\mathbf{F}_l)$, by Theorem 3.2.7. Now let $\tilde{E}$ be an elliptic curve defined over $\mathbb{Q}(j)$, which we choose to be described by

$$Y^2 = 4X^3 - a\lambda(j)X - b\lambda(j)\,.$$

We require that when we choose $j = r \in \mathbb{Q}$, then $\tilde{E} = E(j)$. But

$$\lambda(j) = \frac{27b^2 j}{a^3(j - 12^3)}$$

gives $\lambda(j) = 1$ for $j = r \in \mathbb{Q}$, as required.

We recall from Chapter 2 that $F_n = \mathbb{Q}(j, f_a)$ for the Fricke functions f_a, and now take $n = l$. Since the f_a are functions of $\wp$ multiplied by a rational function of g_2 and g_3, where g_2, g_3 are rational functions in j, then we have that $F_l = \mathbb{Q}(j, f_a) = \mathbb{Q}(j, X(\tilde{E}_l))$. Thus $\mathbb{Q}(j, \tilde{E}_l)$ is an extension of F_l, and we know that $\mathrm{Gal}(F_l/\mathbb{Q}(j)) = GL_2(\mathbf{F}_l)/\{\pm 1\}$. But $\mathbb{Q}(j)$ has char 0, and so $\mathrm{Gal}\,(\mathbb{Q}(j, \tilde{E}_l)/\mathbb{Q}(j)) \subseteq GL_2(\mathbf{F}_l)$, as shown earlier in this section. Let $H = \mathrm{Gal}(\mathbb{Q}(j, \tilde{E}_l)/\mathbb{Q}(j))$. Then we must have that $H \cong GL_2(\mathbf{F}_l)$ or $H \cong GL_2(\mathbf{F}_l)/\{\pm 1\}$. But $GL_2(\mathbf{F}_l)/\{\pm 1\}$ is not a subgroup of $GL_2(\mathbf{F}_l)$, and so we have that $\mathrm{Gal}(\mathbb{Q}(j, \tilde{E}_l)/\mathbb{Q}(j)) = GL_2(\mathbf{F}_l)$.

We already have that $L = \mathbb{Q}(j, j_\circ\alpha_i(\tau))$. We let $H = \mathbb{Q}(E(j)_l)$, $R = \mathbb{Q}[j]$, $S = \mathbb{Q}[j, j_\circ\alpha_i(\tau)]$, $A = \mathbb{Q}[E(j)_l]$ and $T = SA$. We let $r \in \mathbb{Q}\backslash\mathbb{Z}$, and choose $t \in \mathbf{H}$ such that $j(t) = r$. We then let $R_{(r)} = \{x/y \,|\, x, y \in R, (j - r) \not| y\}$, so $R_{(r)}$

is a P.I.D. Let $S_{(r)} = SR_{(r)}$ etc, and $S|_t = \{f(t) \mid f \in S\}$ etc. We know that $\mathrm{Gal}(H/\mathbb{Q}(j)) = GL_2(\mathbf{F}_l)$ and $\mathrm{Gal}(L/\mathbb{Q}(j)) = PGL_2(\mathbf{F}_l)$. Choose an l such that $A|_t$ has Galois group $GL_2(\mathbf{F}_l)$ over $\mathbb{Q}$.

Lemma 3.2.8: $T_{(r)}$ is a free $R_{(r)}$-module of rank $|GL_2(\mathbf{F}_l)|$, and $S_{(r)}$ is a free $R_{(r)}$-module of rank $|PGL_2(\mathbf{F}_l)|$.

Proof: We prove the lemma first for $T_{(r)}$. We have that $T_{(r)} = R_{(r)}[E(j)_l, j_\circ\alpha_i(\tau)]$. Let β be any one of the $E(j)_l$, $j_\circ\alpha_i(\tau)$, and let

$$a_0\beta^n + a_1\beta^{n-1} + \ldots = 0$$

be a primitive minimum polynomial of β over $R_{(r)}$. If this polynomial cannot be made monic, then a_0 is not a unit in $R_{(r)}$, i.e., a_0 is divisible by $(j-r)^n$ for some $0 < n \in \mathbb{Z}$, and $(j-r)$ does not divide some a_i, say a_r. Then $a_r/a_0 \to \infty$ as $\tau \to t$. But a_r/a_0 is a symmetric function of the conjugates of β, and we know that none of these conjugates go to ∞ at $\tau = t$, and so we must have that β is integral over $R_{(r)}$. Then $T_{(r)}$ is a finitely generated torsion-free $R_{(r)}$-module. Since $R_{(r)}$ is a principal ideal domain, then we have that $T_{(r)}$ is a free $R_{(r)}$-module (see [14], p.22, Corollary 2), of finite rank s, say, i.e., there exist $x_1, \ldots x_s \in T_{(r)}$ such that for all $v \in T_{(r)}$, v can be uniquely expressed as $v = \sum_i r_i x_i$ for $r_i \in R_{(r)}$.

Now $T_{(r)} = SAR_{(r)}$, so $A \subseteq T_{(r)}\,\mathbb{Q}(j) \subseteq H$. But $\mathbb{Q}(j) \subseteq T_{(r)}\,\mathbb{Q}(j) \subseteq H$, and since any integral domain finite dimensional over a field is a field, then $T_{(r)}\,\mathbb{Q}(j)$ is a field. Since H is the field of quotients of A, we must have that $T_{(r)}\,\mathbb{Q}(j) = H$. Thus an element h of H can be uniquely written as $h = \sum q_i x_i$ where $q \in \mathbb{Q}(j)$, and so the x_i span H over $\mathbb{Q}(j)$. If $q_i \in \mathbb{Q}(j)$, then there exists $0 \leq n \in \mathbb{Z}$ such that $(j-r)^n q_i \in R_{(r)}$, and so if $\sum q_i x_i = 0$ then $\sum (j-r)^n q_i x_i = 0$ also. But the x_i are linearly independent over $R_{(r)}$, and so $(j-r)^n q_i = 0$, and hence the x_i are linearly independent over $\mathbb{Q}(j)$. Thus $\{x_1, \ldots, x_s\}$ is a basis for H over $\mathbb{Q}(j)$, and so $s = |H : \mathbb{Q}(j)| = |GL_2(\mathbf{F}_l)|$. This proves the lemma for $T_{(r)}$.

The proof for $S_{(r)}$ is achieved by replacing $T_{(r)}$ by $S_{(r)}$, i.e., by showing in the same way that $S_{(r)}$ is a free $R_{(r)}$-module, with rank equal to the dimension of $S_{(r)}\,\mathbb{Q}(j) = L$ over $\mathbb{Q}(j)$, i.e., $|PGL_2(\mathbf{F}_l)|$.

Corollary 3.2.9: (i) $T_{(r)}|_t = T|_t = A|_t$,
(ii) $|PGL_2(\mathbf{F}_l)| \geq \dim_{\mathbb{Q}}(S|_t)$,
(iii) The kernel of the evaluation map $T_{(r)} \mapsto T_{(r)}|_t$ is $(j-r)_{T_{(r)}}$,
(iv) For each $g \in PGL_2(\mathbf{F}_l)$ there is an automorphism g_t of $S|_t$ defined by $f(t)^{g_t} = f^g(t)$.

Proof: (i) Clearly $T_{(r)}|_t \supseteq T|_t \supseteq A|_t$. But by the lemma we know that an element v of $T_{(r)}$ can be written as $v = \sum r_i x_i$ with $r_i \in R_{(r)}$, thus $w \in T_{(r)}|_t$ can be written as $w = \sum r_i(t) x_i(t)$ with $r_i(t) \in R_{(r)}|_t = \mathbb{Q}$. Thus

$$|GL_2(\mathbf{F}_l)| \geq \dim_{\mathbb{Q}}(T_{(r)}|_t) \geq \dim_{\mathbb{Q}}(T|_t) \geq \dim_{\mathbb{Q}}(A|_t) = |GL_2(\mathbf{F}_l)|,$$

and so all these dimensions are equal, giving us (i).
(ii) As for (i), with $S_{(r)}|_t \supseteq S|_t$, and so $|PGL_2(\mathbf{F}_l)| \geq \dim_{\mathbb{Q}}(S_{(r)}|_t) \geq \dim_{\mathbb{Q}}(S|_t)$.
(iii) The kernel I of this map certainly contains $(j-r)$. Now, the dimension of $T_{(r)}/(j-r)$ over $R_{(r)}/(j-r)$ is equal to $|GL_2(\mathbf{F}_l)|$, by the lemma. But $R_{(r)}/(j-r) = \mathbb{Q}$, and the dimension of $T_{(r)}|_t$ over $\mathbb{Q}$ is also $|GL_2(\mathbf{F}_l)|$ by (i). Thus I cannot be bigger, and so $I = (j-r)_{T_{(r)}}$.
(iv) Let $J = (j-r)_{T_{(r)}} \cap S$. Then J is the kernel of the evaluation map restricted to S, and is stable under the action of g. So $S|_t = S/J$ has the given automorphism.

Theorem 3.2.10: If $\mathrm{Gal}\,(A|_t/\mathbb{Q}) \cong GL_2(\mathbf{F}_l)$, then $\mathrm{Gal}\,(S|_t/\mathbb{Q}) \cong PGL_2(\mathbf{F}_l)$.

Proof: By part (iv) of the corollary there is a homomorphism $\phi : PGL_2(\mathbf{F}_l) \to \mathrm{Aut}(S|_t)$. The action of g_t is determined by its action on the $j \circ \alpha_i$, and so the images of ϕ permute the $j \circ \alpha_i$. Now the $j \circ \alpha_i$ remain distinct when evaluated at $\tau = t$: Suppose $j \circ \alpha_i(t) = j \circ \alpha_j(t)$ for some $i \neq j$. Thus, $A(t) = A'(t)$ where A, A' are of the form in Theorem 1.3.1, and so $t = A^{-1}A'(t)$. Then $t = \dfrac{at+b}{ct+d}$ with $a, b, c, d \in \mathbb{Z}$, and so $t \in \mathbf{H}$ is imaginary quadratic, and so, by Theorem 1.3.6, $j(t)$ is an algebraic integer. But $j(t) = r \in \mathbb{Q} \backslash \mathbb{Z}$, so we must have that the $j \circ \alpha_i(t)$ are all distinct. Thus ϕ is injective. Also, by part (ii) of the corollary

$$|PGL_2(\mathbf{F}_l)| \geq \dim_{\mathbb{Q}}(S|_t) \geq |\mathrm{Gal}\,(S|_t/\mathbb{Q})|,$$

and so ϕ is also surjective. This completes the proof.

We now give some specific examples of elliptic curves E with non-integral j-invariants, and show for which primes l the Galois group of $\mathbb{Q}(E_l)$ over $\mathbb{Q}$ is $GL_2(\mathbf{F}_l)$, and so $\mathrm{Gal}(j_\circ\alpha_i(t)/\mathbb{Q}) = PGL_2(\mathbf{F}_l)$, where $j(t) = r \in \mathbb{Q}\backslash\mathbb{Z}$ is the invariant of E. We know this holds for primes l satisfying all conditions of Theorem 3.2.7. We use Table 1 given in [2] to find our examples.

Example 3.2.9: The curve

$$y^2 + y = x^3 - x\,.$$

From Table 1, [2], the conductor, $N = 37$, $\Delta = 37$, $j = \dfrac{2^{12}3^3}{37}$. Thus $e = 1$, and so we do not have to eliminate any primes l by condition (i) of Theorem 3.2.7. Also, from Table 1, the curve is not isogenous to any other curves, so by (ii) we do not have to eliminate any l either. Thus $\mathrm{Gal}(\mathbb{Q}(E_l)/\mathbb{Q}) = GL_2(\mathbf{F}_l)$ *for all primes* l, and so $\mathrm{Gal}(\Phi_l(\dfrac{2^{12}.3^3}{37}, X)/\mathbb{Q}) = PGL_2(\mathbf{F}_l)$ *for all* l.

Example 3.2.10: The curve

$$y^2 + xy + y = x^3 + x^2 - 3x + 1\,.$$

We have $N = 50 = 2^2.5$, $\Delta = -2^2.5^2$, $j = -\dfrac{5.29^3}{2^5}$. Thus $e = 5$, so we must eliminate $l = 5$, by condition (i) of Theorem 3.2.7. Also, the curve is isogenous to the two curves

$$\begin{aligned} y^2 + xy + y &= x^3 + x^2 + 22x - 9\,, \\ y^2 + xy + y &= x^3 + x^2 - 13x - 219, \end{aligned}$$

and the degrees of the isogenies are 3,5 respectively. Thus $\mathrm{Gal}(\mathbb{Q}(E_l)/\mathbb{Q}) = GL_2(\mathbf{F}_l)$ *for all primes* $l \neq 3, 5$, and so $\mathrm{Gal}(\Phi_l(\dfrac{-5.29^3}{2^5}, X)/\mathbb{Q}) = PGL_2(\mathbf{F}_l)$ *for all* $l \neq 3, 5$.

CHAPTER 4

The two – valued Modular Equation

4.1 The two-valued Modular Equation

The modular polynomial, $\Phi_n(j(\tau),\ j(n\tau))$ has extremely large coefficients, with Φ_3 already having a coefficient 22 digits long. In this chapter we study a paper by Cohn, [3], which is based on work by Fricke, [4], and gives a two-valued modular equation with much smaller coefficients. We are then able to give specific examples of equations whose roots generate extensions over $\mathbb{Q}$ with Galois groups $PGL_2(\mathbb{Z}_{13})$ and $PGL_2(\mathbb{Z}_{11})$.

We know that $j(z)$ is invariant under the modular group, Γ. The function $j(z/n)$ is invariant under a subgroup of Γ, $\Gamma^0(n)$, where

$$\Gamma^0(n) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma \;\middle|\; \beta \equiv 0 \,(\mathrm{mod}\, n) \right\}.$$

Then $G = \mathbf{H}/\Gamma^0(n)$ is a Riemann surface, with genus g, say. We now consider the Atkin-Lehner involution,

$$z \mapsto W(z) = \frac{-n}{z},$$

and extend the group $\Gamma^0(n)$ to $\Gamma^0(n)^*$, where

$$\Gamma^0(n)^* = \Gamma^0(n) + W\Gamma^0(n),$$

an extension of degree 2. Now $G^* = \mathbf{H}/\Gamma^0(n)^*$ is a Riemann surface of genus g^*, say, where in fact $g^* \leq g$, and G is a double covering over G^*, i.e. one orbit of G^* gives two orbits of G.

The Riemann surfaces of genus 0 are essentially Riemann spheres, so there is a bijection from the surface to $\mathbb{C} \cup \{\infty\}$. We only consider cases where $g^* = 0$, i.e.,

where there is a bijection t from G^* to $\mathbb{C} \cup \{\infty\}$, so t is a function on the upper half plane which is modular for $\Gamma^0(n)^*$. Then the field K of meromorphic functions of G is an extension of degree 2 over the field K^* of meromorphic functions of G^*, and $K^* = \mathbb{C}(t)$, since $g^* = 0$. Thus $K = \mathbb{C}(t, s)$ where $s^2 \in K$, and we can take s^2 to be a squarefree polynomial in t, i.e., $s^2 = f(t)$. Then the degree of $f(t)$ must be $2g + 2$, in order that G has genus g. Then, the two orbits of G corresponding to one orbit of G^* are given by $(t, \pm s)$. Now,

$$j(z/n) = j(\alpha(z/n)) = j(-n/z) = j(W(z)),$$

where $\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \Gamma$. Since $j(z)$ is a function of $t(z), s(z)$, then there exists a function $F_n(t, s)$ such that

$$j(z) = F_n(t, s), \tag{4.1.1a}$$

$$j(z/n) = F_n(t, -s). \tag{4.1.1b}$$

If we put

$$N_n(t) = j(z)j(z/n), \tag{4.1.2a}$$

$$D_n(t, s) = j(z) - j(z/n), \tag{4.1.2b}$$

$$S_n(t) = (D_n{}^2(t, s) + 4N_n(t))^{1/2}, \tag{4.1.2c}$$

then we have an equation in t with coefficients in j, which we call the **two valued modular equation**, given by

$$j^2 - S_n(t)\, j + N_n(t) = 0. \tag{4.1.3}$$

Since t is modular for $\Gamma^0(n)^*$, then it is modular for $\Gamma(n)$, and so must have Fourier expansion in powers of $q^{\frac{1}{n}}$. Then, since two points in the fundamental domain are inequivalent under $\Gamma^0(n)$ for their imaginary parts sufficiently large, then t must have a Fourier expansion of the form $a_0\, q^{\frac{-1}{n}} + a_1 + \cdots$ or $b_0 + b_1\, q^{\frac{1}{n}} + \cdots$. We choose t such that $t(i\infty) = \infty$, and so take the first expansion, choosing $a_0 = 1$, $a_1 = -C$. Then we have

$$j(z) = t^n + nCt^{n-1} + \mathrm{O}(t^{n-2}), \tag{4.1.4a}$$

$$j(z/n) = t + C + \mathrm{O}(1/t). \tag{4.1.4b}$$

This choice for t is not unique since there may be a translation in t.

Functions $N_n(t)$ and $D_n(t,s)$ for suitable choices of t, s are given in the appendix to [3].

We first consider a case where $g = 0$. We change variables from t, s to x, y so that $(t,s) \leftrightarrow (t,-s)$ is given instead by $x \leftrightarrow y$: Since $g = 0$, we can choose $s^2 = t^2 - 4B^2$ for some constant B. We then define $w = \dfrac{s}{t+2B}$, so that $w^2 = \dfrac{(t-2B)}{(t+2B)}$. Then we choose

$$x = \frac{(1-w)}{(1+w)}, \tag{4.1.5a}$$

$$xy = 1\,. \tag{4.1.5b}$$

Thus we have that

$$\begin{aligned} j(z) &= G_n(x)\,, \\ j(z/n) &= G_n(y)\,. \end{aligned}$$

Since $t \approx B/x$ as $z \to \infty$, we can choose $x\,(i\infty) = 0$, so that $j(z), j(z/n)$ satisfy the asymptotic conditions (4.1.4a,b). We require that x is a modular function for $\Gamma^0(n)$ which preserves the symmetry of $(t,s) \leftrightarrow (t,-s)$. Since $\eta(z)$ satisfies $\eta(-1/z) = (-iz)^{\frac{1}{2}}\eta(z)$, then for the cases where $(n-1)\,\Big|\,24$ we can take x to be

$$x = x\,(z) = \left(\frac{\eta\,(z)\,n^{\frac{1}{4}}}{\eta\,(z/n)}\right)^{\frac{24}{(n-1)}}\,. \tag{4.1.6}$$

The fact that this is modular for $\Gamma^0(n)$ will be proved in Corollary 4.1.8. It also preserves the symmetry of $(t,s) \leftrightarrow (t,-s)$ since

$$\begin{aligned} y = x\,(-n/z) &= \left(\frac{\eta\,(-n/z)\,n^{\frac{1}{4}}}{\eta\,(-1/z)}\right)^{\frac{24}{(n-1)}}\,, \\ &= \left(\frac{(-iz/n)^{\frac{1}{2}}\eta\,(z/n)\,n^{\frac{1}{4}}}{(-iz)^{\frac{1}{2}}\eta\,(z)}\right)^{\frac{24}{(n-1)}}\,, \\ &= \left(\frac{\eta\,(z/n)}{\eta\,(z)\,n^{\frac{1}{4}}}\right)^{\frac{24}{(n-1)}}\,, \\ &= \frac{1}{x\,(z)}\,, \end{aligned}$$

and $(t,s) \leftrightarrow (t,-s)$ gives $w \leftrightarrow -w$, and so $x \leftrightarrow y$. Then, from the q-expansions we find that

$$B = n^{\frac{6}{(n-1)}}, \qquad C = \frac{24}{(n-1)}.$$

We require the following lemma:

Lemma 4.1.7: $x(z) = n^{\frac{6}{(n-1)}} \left(\frac{\eta(z)}{\eta(z/n)}\right)^{\frac{24}{(n-1)}}$ is a modular function for

$$\Gamma_0^0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; b \equiv c \equiv 0 \pmod{n} \right\},$$

for all $(n-1) \mid 24$.

Proof: Let $A = \begin{pmatrix} a & bn \\ cn & d \end{pmatrix} \in \Gamma_0^0(n)$. We require the following property of $\eta(\tau)$:

$$\eta\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \epsilon\,(\gamma\tau+\delta)^{\frac{1}{2}}\eta(\tau),$$

for $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$ and where $\epsilon^{24} = 1$. An explicit formula for ϵ is given by Dedekind's functional equation, as found in [1], p.52, Theorem 3.4. Let $v = \frac{24}{(n-1)}$. Then we have that

$$\begin{aligned}
x(A(z)) &= n^{\frac{v}{4}} \left(\frac{\eta(\frac{az+bn}{cnz+d})}{\eta(\frac{az+bn}{n(cnz+d)})}\right)^v \\
&= n^{\frac{v}{4}} \left(\frac{\eta(\frac{az+bn}{cnz+d})}{\eta(\frac{a(z/n)+b}{n^2c(z/n)+d})}\right)^v \\
&= n^{\frac{v}{4}} \left(\frac{\epsilon_1}{\epsilon_2}\right)^v \left(\frac{cnz+d}{n^2c(z/n)+d}\right)^{\frac{v}{2}} \left(\frac{\eta(z)}{\eta(z/n)}\right)^v \\
&= n^{\frac{v}{4}} \left(\frac{\epsilon_1}{\epsilon_2}\right)^v \left(\frac{\eta(z)}{\eta(z/n)}\right)^v
\end{aligned}$$

where $\epsilon_1^{24} = \epsilon_2^{24} = 1$. We must now show that $(\epsilon_1/\epsilon_2)^v = 1$. We examine the cases $n = 2, 3$ and 4 separately. For $n = 2$ we have that $v = 24$, and so clearly $(\epsilon_1/\epsilon_2)^v = 1$. For $n \geq 3$ we look at the functional equation for ϵ and find that

$$\begin{aligned}
\left(\frac{\epsilon_1}{\epsilon_2}\right)^v &= \exp\left\{\pi i v \left(\frac{a+d}{12cn} - \frac{a+d}{12cn^2} - \sum \begin{array}{c}\text{terms with } cn^2 \text{or } (cn^2)^2 \\ \text{in their denominators}\end{array}\right)\right\} \\
&= \exp\left\{\frac{2\pi i(a+d)}{cn^2} - \pi i v \sum\right\} \qquad (*)
\end{aligned}$$

Thus, for $n = 3$, we have

$$\left(\frac{\epsilon_1}{\epsilon_2}\right)^{12} = \exp\left\{\frac{2\pi i(a+d)}{9c} - \pi i v \sum\right\},$$

and so, for 2 not dividing c, we must have that $(\epsilon_1/\epsilon_2)^{12} = 1$. We must show that all matrices in $\Gamma_0^0(3)$ can be generated by matrices of the form $\begin{pmatrix} a & 3b \\ 3c & d \end{pmatrix}$ where 2 does not divide c. Let $B = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$, so B is of the required form, and let $X = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ be a general matrix in $\Gamma_0^0(3)$. Then $BX = \begin{pmatrix} p & q \\ r+3p & s+3q \end{pmatrix}$. Now, if 2 does not divide r, then X is already of the required form. So suppose that 2 divides r. Then 2 does not divide p, otherwise 2 would divide $\det X = 1$. Thus 2 does not divide $r + 3p$, and so $BX = Y$, say is of the required form. Thus $X = B^{-1}Y$ is generated by matrices of the required form, and so $x(z)$ is modular for $\Gamma_0^0(3)$.

For $n = 4$ we have

$$\left(\frac{\epsilon_1}{\epsilon_2}\right)^{8} = \exp\left\{\frac{2\pi i(a+d)}{16c} - \pi i v \sum\right\},$$

and so for 3 not dividing c, then $(\epsilon_1/\epsilon_2)^8 = 1$. The matrices of the form $\begin{pmatrix} a & 4b \\ 4c & d \end{pmatrix}$, where 3 does not divide c, can be shown to generate $\Gamma_0^0(4)$ by exactly the same method as above.

For the cases where $n \geq 5$, by looking at $(*)$ we see that $(\epsilon_1/\epsilon_2)^v = 1$ whenever $(cn, 6) = 1$, and so we must show that these matrices generate $\Gamma_0^0(n)$: The matrix $C = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \in \Gamma_0^0(n)$ satisfies the requirement that $(n, 6) = 1$, and $C^h = \begin{pmatrix} 1 & 0 \\ hn & 1 \end{pmatrix}$. Let $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a general matrix in $\Gamma_0^0(n)$, i.e., $b \equiv c \equiv 0 \pmod{n}$. Then a, c are not both divisible by 2 or by 3, since $\det X = 1$. We have

$$C^{\pm h}X = \begin{pmatrix} a & b \\ c \pm hna & d \pm hnb \end{pmatrix}.$$

We need to show that one of $C^{\pm h}X$ is of the required form, i.e., one of $(c \pm hna, 6) = 1$. There are 4 cases:

(i) $2 \nmid c, 3 \nmid c$. Then X is already of the required form.

(ii) $2 \mid c, 3 \nmid c$. Take $h = 1$. Then $2 \nmid a$, and so $2 \nmid c \pm na$. Also, if $3 \mid c + na$, then $a \equiv -c \pmod{3}$, and so $c - na \equiv c - a \equiv 2c \equiv -c \not\equiv 0 \pmod{3}$. Thus $3 \nmid c - na$, and

so $B^{-1}X$ is of the required form.

(iii) $2 \mid c, 3 \mid c$. Then $2 \nmid a, 3 \nmid a$, and so $2 \nmid c \pm na, 3 \nmid c \pm na$.

(iv) $2 \nmid c, 3 \mid c$. Then $3 \nmid a$. Take $h = 2$. Then $2 \nmid c \pm 2na$, and $3 \nmid c \pm 2na$.

Thus, in each case, X can be generated by matrices of the required form, and so $x(z)$ is modular for $\Gamma_0^0(n)$. This proves the lemma.

Corollary 4.1.8: For all $(n-1) \mid 24$, $x(z)$ is a modular function for $\Gamma^0(n)$.

Proof: Let $\begin{pmatrix} a & bn \\ c & d \end{pmatrix} \in \Gamma^0(n)$, and so $(a,n) = 1$, since $\det X = 1$. Now the matrix $C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ leaves $x(z)$ fixed, since in $(*)$ given in the proof of the lemma, we replace cn^2 by n, so we can see that we always have $(\epsilon_1/\epsilon_2)^v = 1$. Then

$$C^x X = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} a & bn \\ c & d \end{pmatrix} = \begin{pmatrix} a & bn \\ c+ax & d+bnx \end{pmatrix} = Y, \text{say}.$$

Since $(a,n) = 1$, we can solve $xa \equiv c \pmod{n}$, and so $Y \in \Gamma_0^0(n)$. Thus $X = C^{-x}Y$ leaves $x(z)$ fixed, and so $x(z)$ is modular for $\Gamma^0(n)$.

We thus consider the case $n = 13$, i.e., $B = \sqrt{13}$ and $s^2 = t^2 - 52$. We need to show that the extension generated by t and s is the same extension as the extension L as defined in chapter 2, and then we are able to give an equation whose roots give an extension over $\mathbb{Q}$ with Galois group $PGL_2(\mathbb{Z}_{13})$. First we have, from the appendix to [3], that

$$\begin{aligned} N_{13} &= (t+5)^2(t^4+254t^3+5077t^2+34092t+75492)^4, \\ D_{13} &= (t-3)(t+2)(t+4)(t+5)(t+6)(t+7)(t+9)(t^2-52)^{\frac{1}{2}} \\ &\qquad (t^2-27)(t^2-t-38)(t^2+6t-3), \end{aligned}$$

and so, from (4.1.2a,b) we can evaluate $j(z), j(z/13)$ and show that they lie in $\mathbb{Q}(j,t,s)$. Thus we have that

$$L = \overline{\mathbb{Q}(j(z), j(z/13))} \subseteq \overline{\mathbb{Q}(j,t,s)}.$$

Now we are able to show that

Theorem 4.1.9: $\mathrm{Gal}\left(\overline{\mathbb{Q}(j,t,s)}/\mathbb{Q}(j)\right) = PGL_2(\mathbb{Z}_{13})$.

Proof: We need to show that $t, s \in L$, to get our result. We look at x, where from (4.1.6) we have that

$$x = \left(\frac{\eta^2(z)}{\eta^2(z/13)}\right)\sqrt{13}.$$

From Lemma 4.1.7, x is a modular function for $\Gamma_0^0(n)$, and is thus modular for $\Gamma(n)$. Now, $\eta(z), \eta(z/13)$ have integer coefficients in their expansions in powers of q and $q^{\frac{1}{13}}$ respectively. We also have that $\sqrt{13} \in L$, since fixing F_{13} by $\frac{\lambda I}{\{\pm 1\}}$ gives us L. Thus fixing the subgroup $\mathbb{Q}(\xi_{13})$ of F_{13} by $\frac{\lambda I}{\{\pm 1\}}$ must give us the group $L \cap \mathbb{Q}(\xi_{13})$. We know that $\mathrm{Gal}\left(\mathbb{Q}(\xi_{13})/\mathbb{Q}\right) = (\mathbf{F}_{13})^*$, and $\mathrm{Gal}\left(\mathbb{Q}(\xi_{13})/L \cap \mathbb{Q}(\xi_{13})\right) = (\mathbf{F}_{13}^*)^2$, since the determinant of a matrix in $\frac{\lambda I}{\{\pm 1\}}$ is a square. Thus $L \cap \mathbb{Q}(\xi_{13})$ is a quadratic extension of $\mathbb{Q}$ which is ramified only at 13, and so must be $\mathbb{Q}(\sqrt{13})$, since $13 \equiv 1 \pmod 4$. Thus $\sqrt{13} \in L$, and hence $\sqrt{13} \in F_n$, so we get that $x \in F_n$.

We show that x is fixed by the action of the scalar matrices, $\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$, where $k \in (\mathbb{Z}_{13})^*$. Now,

$$\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}^2 \begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix},$$

where $\begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \in GL_2(\mathbb{Z}_{13})$, $\begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix} \in SL_2(\mathbb{Z}_{13})$. We already know how $\begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}$ acts, from chapter 2:

$$\sigma_k : \xi_{13} \longrightarrow \xi_{13}{}^l, \qquad \text{where } kl \equiv 1 \pmod{13}.$$

Since $\eta(z), \eta(z/13) \in \mathbb{Z}[q], \mathbb{Z}[q^{\frac{1}{13}}]$ respectively, then x is fixed under σ_k. Thus it remains to show how $\begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix}$ acts on x. First we choose m such that $km \equiv 1 \pmod{13^2}$, i.e., $km - 13^2 a = 1$ for some integer a. Thus the matrix $V = \begin{pmatrix} k & 13a \\ 13 & m \end{pmatrix} \in SL_2(\mathbb{Z})$ is mapped to $\begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix}$ under $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}_{13})$. But $V \in \Gamma_0^0(13)$, and so by Lemma 4.1.7, it leaves x fixed. Thus x is fixed under the scalar matrices, and so lies inside the extension $L = \overline{\mathbb{Q}(j(z), j(z/13))}$. Thus

$$\mathbb{Q}(j,x) \subseteq \overline{\mathbb{Q}(j(z), j(z/13))} \subseteq \overline{\mathbb{Q}(j,t,s)}.$$

But from (4.1.5a) we find that

$$t = \frac{B(1+x^2)}{x},$$

and then

$$s = \left(\frac{B(1+x^2)}{x} + 2B\right)\left(\frac{1-x}{1+x}\right),$$

thus $s, t \in \mathbb{Q}(j,x)$, and so we have that

$$\mathbb{Q}(j) \subseteq \mathbb{Q}(j,s,t) \subseteq \overline{\mathbb{Q}(j(z),j(z/13))} \subseteq \overline{\mathbb{Q}(j,t,s)}.$$

But $\overline{\mathbb{Q}(j(z),j(z/13))}$ is a normal extension of $\mathbb{Q}(j)$, and so we have that $\overline{\mathbb{Q}(j(z),j(z/13))} = \overline{\mathbb{Q}(j,t,s)}$. Thus

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{Q}(j,t,s)}/\mathbb{Q}(j)) &= \mathrm{Gal}(\overline{\mathbb{Q}(j(z),j(z/13))}/\mathbb{Q}(j(z))), \\ &= PGL_2(\mathbb{Z}_{13}). \end{aligned}$$

We now show that we can dispense with s;

Theorem 4.1.10: $\mathrm{Gal}(\overline{\mathbb{Q}(j,t,s)}/\mathbb{Q}(j)) = \mathrm{Gal}(\overline{\mathbb{Q}(j,t)}/\mathbb{Q}(j))$.

Proof: We have that $\mathbb{Q}(j,t,s)$ is an extension of degree 2 over $\mathbb{Q}(j,t)$. Thus the Galois group of $\overline{\mathbb{Q}(j,t,s)}$ over $\overline{\mathbb{Q}(j,t)}$ is an elementary abelian group, N say, of order 2^r. Now, $\dfrac{PGL_2(\mathbb{Z}_{13})}{PSL_2(\mathbb{Z}_{13})} \cong C_2$, and $PSL_2(\mathbb{Z}_{13})$ is a simple, normal subgroup of $PGL_2(\mathbb{Z}_{13})$. Thus we have a composition series

$$\{1\} \lhd PSL_2(\mathbb{Z}_{13}) \lhd PGL_2(\mathbb{Z}_{13}).$$

Now, since $\overline{\mathbb{Q}(j,t)}$ is normal over $\mathbb{Q}(j)$, then N is a normal subgroup of $PGL_2(\mathbb{Z}_{13})$, and so we get

$$\{1\} \lhd N \lhd PGL_2(\mathbb{Z}_{13}),$$

and so by the Jordan-Holder Theorem, we must have that $N = C_2$ or $N = PSL_2(\mathbb{Z}_{13})$. But $|N| = 2^r$, and so $r = 1$ and $N = C_2$. We conclude by showing that $PGL_2(\mathbb{Z}_{13})$ has no normal subgroup of order 2, for any such subgroup must be contained in the centre of $PGL_2(\mathbb{Z}_{13})$, which we will show is trivial: We need to find which $a \in PGL_2(\mathbb{Z}_{13})$ satisfy

$$g^{-1}ag = \lambda a$$

for all $g \in PGL_2(\mathbb{Z}_{13})$, and where $\lambda \in (\mathbb{Z}_{13})^*$. Taking $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ respectively gives us that a is of the form $\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}$. But $PGL_2(\mathbb{Z}_{13}) = \dfrac{GL_2(\mathbb{Z}_{13})}{\{\lambda I\}}$,

and so $a = I$, as required. Thus $PGL_2(\mathbb{Z}_{13})$ has no normal subgroup of order 2, and hence $\mathrm{Gal}(\overline{\mathbb{Q}(j,t)}/\mathbb{Q}(j)) = PGL_2(\mathbb{Z}_{13})$.

We are now able to give our specific example. Using the equations for N_{13}, D_{13} to give S_{13}, by (4.1.2c), we find our 2-valued modular equation, (4.1.3). We choose a rational value of j so that 13 satisfies conditions conditions (i) and (ii) of Theorem 3.2.7. Thus we choose the curve

$$y^2 = x^3 - x^2 + x\,,$$

which has $j = 2^{11}/3$, giving us the equation

Example 4.1.11:

$$\begin{aligned} f_{13}(2^{11}/3,t) \;=\; & \frac{1}{9}(9\,t^{14} + 804\,t^{13} + 1788072\,t^{12} + 236043288\,t^{11} \\ & +12246025350\,t^{10} + 352217211216\,t^9 + 6451265464020\,t^8 \\ & +80606750638440\,t^7 + 711610221772905\,t^6 \\ & +4501773356745132\,t^5 + 20346314325794652\,t^4 \\ & +64281217622417952\,t^3 + 135086706336372336\,t^2 \\ & +169866024492553920\,t + 96801145628029504)\,, \end{aligned}$$

which has Galois group $PGL_2(\mathbb{Z}_{13})$ over $\mathbb{Q}$.

We now consider the case $b = 11$, of genus 1, following the work of Fricke, [4]. Fricke uses two theta-functions to derive his equations. The first is described by

$$y(\omega_1,\omega_2) = \frac{2\pi}{\omega_2}\sum_{\mu,\nu} q^{2(a\mu^2+b\mu\nu+c\nu^2)}\,, \tag{4.1.12}$$

for $q = e^{\pi i\tau}$, $(\mu,\nu) \in \mathbb{Z}^2$, and $(a,b,c) = ax^2 + bxy + cy^2$ a positive quadratic form of discriminant = -11. Then, as shown in [12],p VI-22, Theorem 20, $y(\omega_1,\omega_2)$ satisfies the following relation;

$$y(\alpha\omega_1 + \beta\omega_2, \gamma\omega_1 + \delta\omega_2) = \left(\frac{\alpha}{11}\right) y(\omega_1,\omega_2)\,, \tag{4.1.13}$$

for $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(11) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma \;\middle|\; \gamma \equiv 0 \,(\mathrm{mod}\, 11) \right\}$, and where $\left(\frac{\alpha}{11}\right)$ is the Legendre symbol. The other theta-function Fricke uses is

(4.1.14) $$z(\omega_1,\omega_2)=\frac{2\pi i}{\omega_2}\sum_{\mu,\nu}(-1)^{\nu}q^{a\mu^2+b\mu\nu+c\nu^2}\,,$$

taken over all odd integers μ, and all integers ν. According to Fricke, the product

$$z(\omega_1,\omega_2)\sqrt{\Delta(\omega_1,\omega_2)}$$

also satisfies the relation (4.1.13). By substituting the quadratic form (1,1,3), which is of discriminant $b^2-4ac=-11$, into (4.1.12), (4.1.14) we obtain

$$\begin{aligned} y(\omega_1,\omega_2) &= \frac{2\pi i}{\omega_2}(1+2q^2+4q^6+2q^8+4q^{10}\cdots) \\ z(\omega_1,\omega_2) &= \frac{2\pi i}{\omega_2}(q-q^3-q^5+q^{11}+q^{13}-q^{23}\cdots) \end{aligned}$$

respectively. These are both homogeneous functions of weight 1, i.e.,

$$y(\lambda\omega_1,\lambda\omega_2)=\frac{1}{\lambda}y(\omega_1,\omega_2)\,,$$

and similarly for $z(\omega_1,\omega_2)$. Fricke then considers the transformation W which sends

$$\tau\longmapsto\tau'=\frac{-1}{11\tau}\,,$$

and chooses W such that

$$\omega_1'=\frac{i\omega_2}{\sqrt{11}},\qquad \omega_2'=-i\sqrt{11}\omega_1\,,$$

i.e.,

$$W=\begin{pmatrix} 0 & \frac{i}{\sqrt{11}} \\ -i\sqrt{11} & 0 \end{pmatrix}.$$

Under this transformation the modular forms g_2, g_3 and Δ are transformed to g_2', g_3' and Δ'. Then $(g_2'-g_2)^2$ is a modular form of weight 8 with respect to $\Gamma_0(11)$, which Fricke asserts can be expressed as

$$(g_2'-g_2)^2=ay^8+by^6z^2+cy^4z^4+dy^2z^6+ez^8\,.$$

The first few terms of the q-expansions are sufficient to give that

$$(g_2'-g_2)^2=100y^2(y^6-20y^4z^2+56y^2z^4-44z^6)\,.$$

Thus we put $g\,(\omega_1,\omega_2)=\dfrac{g_2'-g_2}{10}$, which has q-expansion

$$g\,(\omega_1,\omega_2)=\left(\frac{2\pi i}{\omega_2}\right)^4(1-2q^2-18q^4-56q^6-146q^8-252q^{10}\cdots)\,,$$

a modular form of weight 4 for the subgroup $\Gamma_0(11)$. Fricke then defines his s and t by

$$t(\tau) = \left(\frac{y(\omega_1,\omega_2)}{z(\omega_1,\omega_2)}\right)^2, \qquad s(\tau) = \left(\frac{g(\omega_1,\omega_2)}{z(\omega_1,\omega_2)}\right).$$

As before, we must show that t and s lie inside L. From the expansions for y, z and g, we can see that $t, s \in \mathbb{Q}((q))$, and thus $\in F_n$. It remains to show that t, s are fixed under the action of the scalar matrices.

We let $K = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$. Then $K \in \Gamma_0(11)$, and so

$$K(y(\omega_1,\omega_2)) = \left(\frac{k}{11}\right) y(\omega_1,\omega_2),$$

$$K(z(\omega_1,\omega_2)\sqrt{\Delta(\omega_1,\omega_2)}) = \left(\frac{k}{11}\right) z(\omega_1,\omega_2)\sqrt{\Delta(\omega_1,\omega_2)}.$$

But $\sqrt{\Delta(\omega_1,\omega_2)} = (2\pi)^{12}\eta^{12}(\omega_1,\omega_2)$, and $K(\eta^{12}(\omega_1,\omega_2)) = \eta^{12}(\omega_1,\omega_2)$, and so

$$K(z(\omega_1,\omega_2)) = \left(\frac{k}{11}\right) z(\omega_1,\omega_2),$$

Thus

$$K(t(\tau)) = t(\tau).$$

Also, since g is modular for $\Gamma_0(11)$, we have that

$$K(g(\omega_1,\omega_2)) = g(\omega_1,\omega_2),$$

giving

$$K(s(\tau)) = \frac{g(\omega_1,\omega_2)}{\left(\frac{k}{11}\right)^4 z(\omega_1,\omega_2)^4},$$

and since the Legendre symbol is equal to ± 1,

$$K(s(\tau)) = s(\tau).$$

Thus $t, s \in L$, and so, as before, we have that

$$\overline{\mathbb{Q}(j,t,s)} = \overline{\mathbb{Q}(j(z), j(z/11))},$$

i.e.,

$$\mathrm{Gal}(\overline{\mathbb{Q}(j,t,s)}/\mathbb{Q}) = PGL_2(\mathbb{Z}_{11}).$$

We construct our two-valued modular equation $f(j,t)$ for $b = 11$ using $S_{11}(t)$, $N_{11}(t)$, as given in [3]. We note that we have

$$j(z) = \frac{S_{11}(t) + D_{11}(t)}{2}, \qquad j(z/11) = \frac{S_{11}(t) - D_{11}(t)}{2},$$

where

$$D_{11}(t) = (t^4 - 20t^3 + 56t^2 - 44t)^{\frac{1}{2}} \times \text{monic polynomial in } t \text{ of degree } 9\,.$$

Writing

$$(t^4 - 20t^3 + 56t^2 - 44t)^{\frac{1}{2}} = t^2 - 10t - 22 - \frac{242}{t} - \frac{2662}{t^2} - \frac{31944}{t^3} - \cdots,$$

we find that $j(z)$, $j(z/11)$ satisfy the asymptotic conditions (4.1.4a,b), with $C = -6$.

The same curve as before, $y^2 = x^3 - x^2 + x$, with $j = 2^{11}/3$ has 11 satisfying the conditions (i) and (ii) of Theorem 3.2.7, and gives the equation

Example 4.1.15:

$$\begin{aligned} f_{11}(2^{11}/3, t) \;=\; & \frac{1}{9}(9t^{12} - 96t^{11} + 1755072t^{10} + 87793728t^9 - 109114368t^8 \\ & -2241355776t^7 + 10223026176t^6 - 20789919744t^5 \\ & +28214427648t^4 - 35589193728t^3 + 41108373504t^2 \\ & -30828134400t + 10070523904)\,, \end{aligned}$$

having Galois group $PGL_2(\mathbb{Z}_{11})$ over $\mathbb{Q}$.

4.2 The size of the discriminant

From examples 4.1.11, 4.1.15 we are able to see how much smaller the coefficients of the 2-valued modular equation $f_n(j,t)$ are than those of the standard modular equation $\Phi_n(j,t)$. Indeed, Φ_3 has a coefficient 22 digits long, whereas the largest coefficients of f_{11} and f_{13} have 11 and 18 digits respectively.

We now investigate the discriminant of the modular equation and find in the cases we look at that it is divisible by many squares of primes. We find out whether these primes ramify, or that we simply do not have the full ring of integers. We do this work for the modular equation of level 2. From [4] we have that

$$\begin{aligned}\Phi_2(j,x) = x^3 + &\left(2^4.3.31j - j^2 - 2^4.3^4.5^3\right)x^2 + \left(2^4.3.31j^2 + 3^4.5^3.4027j + 2^8.3^7.5^6\right)x \\ &+ \left(j^3 - 2^4.3^4.5^3j^2 + 2^8.3^7.5^6j - 2^{12}.3^9.5^9\right),\end{aligned}$$

which has discriminant

$$d = d(j) = 2^2j^2(j + 3^3.5^3)^2(j^2 + 3^3.5^2.283j - 5^3.97499)^2(j - 1728).$$

We want to choose a rational value r of j such that $\mathrm{Gal}\,(\Phi_2(r,x)/\mathbb{Q}) = PGL_2(\mathbb{Z}_2)$. Now, $PGL_2(\mathbb{Z}_2) \cong S_3$, and since $\Phi_2(r,x)$ is a cubic, it has Galois group a subgroup of S_3. Thus we only need to show that 2 and 3 divide the order of the Galois group. Now

$$\begin{aligned} 2 \;\Big|\; |\mathrm{Gal}\,(r,x)/\mathbb{Q})| &\;\Leftrightarrow\; d(r) \neq \text{square}, \\ 3 \;\Big|\; |\mathrm{Gal}\,(r,x)/\mathbb{Q})| &\;\Leftrightarrow\; \Phi_2 \text{ is irreducible over } \mathbb{Q}. \end{aligned}$$

Choosing $j = 2$ gives $d < 0$, therefore $d \neq$ square. Also,

$$\Phi_2(2,x) \equiv x^3 + 2x^2 + 2x + 3 \pmod 5,$$

and since $0, \pm 1, \pm 2$ are not roots of $x^3 + 2x^2 + 2x + 3$, $\Phi_2(2,x)$ is irreducible, and hence $\mathrm{Gal}\,(\Phi_2(2,x)/\mathbb{Q}) = PGL_2(\mathbb{Z}_2)$.

Now,

$$d = -2^5.11^2.29^2.211^2.307^2.863.19759^2.$$

Let θ be a root of $\Phi_2(2,x)$ and put $K = \mathbb{Q}[\theta]$, $R = \text{int}\, K$. Then we have that

$$d = \Delta_K(\mathbb{Z}[\theta]) = |R : \mathbb{Z}[\theta]|^2 \Delta(R).$$

Clearly, if $|R : \mathbb{Z}[\theta]| > 1$, then $\mathbb{Z}[\theta]$ is not the full ring of integers. We require the following theorem:

Theorem 4.2.1: If $p^2||d$, $p > 3$, and p does not divide $|R : \mathbb{Z}[\theta]|$, and if $b \in \mathbb{Z}$ is such that $3b \equiv a \pmod{p}$, where a is the coefficient of x^2 in $\Phi_2(r,x)$ for some $r \in \mathbb{Z}$, then $g(x) = \Phi_2(r, x-b)$ is such that $g(x) \equiv x^3 \pmod{p}$ and p^2 does not divide $g(0)$.

Proof: We have that $(p)_R = p_1^{e_1} \cdots p_s^{e_s}$, where $\sum e_i f_i = n = 3$, for the ramification indices e_i and the residue degrees f_i where $0 \leq e_i, f_i \in \mathbb{Z}$. Thus each $e_i \leq 3$. If p does not divide e_i for any i, p is said to be tamely ramified, and $N(p_1)^{e_1-1} \cdots N(p_s)^{e_s-1} || \Delta(R)$. In this case, if $p^t || \Delta(R)$, then $t = \sum_i (e_i - 1)$. We have $p > 3$, and thus p does not divide e_i for any i. We also have that $p^2 || \Delta(R)$, i.e., $\sum(e_i - 1) = 2$. Thus we must have that $(p)_R = P^3$. Since p does not divide $|R : \mathbb{Z}[\theta]|$, we may apply Dedekind's Theorem. Then,

$$\Phi_2(r,x) \equiv (x+b)^3 \pmod{p},$$

so $g(x) \equiv x^3 \pmod{p}$. Let $\phi = \theta + b$. Then $g(\phi) = g(\theta + b) = \Phi_2(\theta) = 0$, and so ϕ is a root of $g \pmod{p}$. Also, from Dedekind's Theorem, $P = (p, \theta + b) = (p, \phi)$. Suppose $p^2 | g(0)$. Now, $g(0) = -N(\phi)$, and hence $P^2 | (\phi)$. Then we have that $P^2 | (p) + (\phi) = P$, giving a contradiction, hence our result.

We use Theorem 4.2.1 to show that we do not have the full ring of integers. We have that $d = -2^5.11^2.29^2.211^2.307^2.863.19759^2$, and the coefficient of x^2 in $\Phi_2(2,x)$ is $a = -159028$. We check for $p = 11$; $b = -53013$ is a solution to $3b \equiv a \pmod{11}$, and thus we put

$$g(x) = \Phi_2(2, x + 53013) = x^3 + 11x^2 + 399584481x + 12692331156599.$$

Since 11 does not divide 12692331156599, we must have that $11 \Big| |R : \mathbb{Z}[\theta]|$. Checking the other primes in the same way we find that $p \Big| |R : \mathbb{Z}[\theta]|$ for all primes p such that $p^2 || d$. Thus we have many primes whose squares divide the discriminant which do not ramify. It should thus be possible to generate the extension by adding the

root of a polynomial whose discriminant is divisible by fewer squares of redundant primes, and therefore has smaller coefficients.

We thus look at the discriminant of the 2-valued modular equation. From [3] we have that

$$N_2 = (t+272)^3, \qquad D_2 = (t+47)\,(t^2-128^2)^{\frac{1}{2}},$$

giving $S_2 = t^2 + 49t - 6656$. Substituting S_2, N_2 into (4.1.3) gives

$$f_2(j,t) = t^3 + (816-j)t^2 + (221952 - 49j)t + (j^2 + 6656j + 20123648),$$

with discriminant

$$d^* = 2^2.j^2.(j+3^2.5^2)^2.(j-1728).$$

Thus $d^* \mid d$, and so d^* is is divisible by fewer squares of primes than d. We see that

$$\frac{d}{d^*} = (j^2 + 3^3.5^2.283j - 5^3.97499)^2,$$

and in fact this corresponds to a value of $j(\tau)$ for $\tau = \dfrac{\pm 1 + \sqrt{-15}}{2}$. Now d and d^* are divisible by the differences of conjugates of $j(\tau/n)$ and t respectively. For d we have that $j(V(\tau)) = j(V'(\tau))$, where V, V' are primitive matrices of determinant n, only if $n(V')^{-1}AV(\tau) = \tau$ for some $A \in \Gamma$, i.e., only if τ is fixed under a transformation of determinant n^2. For d^*, since t is modular for $\Gamma_0(n)^*$, then $t\,(V(\tau)) = t\,(\tau)$ for $V \in$ transversal of $\Gamma/\Gamma^0(n)$ if and only if $V(\tau) = U(\tau)$ for some $U \in \Gamma^0(n)^*$, i.e., $U \in \Gamma^0(n)$ or $U \in W\Gamma^0(n)$. For $U \in \Gamma^0(n)$ we must have that τ is fixed under a transformation of determinant 1, i.e., τ must be equivalent to i or ϱ, where $\varrho = e^{\frac{2\pi i}{3}}$. If $U \in W\Gamma^0(n)$, then τ must be fixed under a transformation of determinant n. Since these are stronger conditions, it explains why $d^* | d$.

Suppose τ is fixed under a transformation of determinant m, i.e., $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \tau$ for $ad - bc = m$. Then

$$\tau = \frac{-(d-a)^2 \pm \sqrt{(a+d)^2 - 4m}}{2c}.$$

For d, by the above, we have $m = 4$, so the possible complex square roots are $\sqrt{-16} = 4i$, $\sqrt{-15}$, $\sqrt{-12} = 2i\sqrt{3}$, and $\sqrt{-7}$. But $j(\varrho) = 0$ for $\varrho = e^{\frac{2\pi i}{3}}$, $j(i) = 1728$ and $j((-1+\sqrt{-7})/2) = 3^3.5^3$, so we must have that $j^2 + 3^3.5^2.283j - 5^3.97499 = 0$

corresponds to a value of $j(\tau)$ for $\tau \in \mathbb{Q}(\sqrt{-15})$, and in fact $\tau = \dfrac{\pm 1 + \sqrt{-15}}{2}$.

For d^* we have that $m = 2$, by the above, and so the only possible complex square roots are $\sqrt{-8} = 2\sqrt{-2}$, $\sqrt{-7}$ and $\sqrt{-4} = 2i$. We must in fact expect to exclude the value $\sqrt{-n}$ since this is a fixed point of W, and so the only values of $j(\tau)$ which may appear in the discriminant are for $\tau = i$, ϱ and $(-1 + \sqrt{-7})/2$.

Since, for $g = 0$, we have that $\mathbb{Q}(j, j(\tau/n)) = \mathbb{Q}(s,t) = \mathbb{Q}(x)$, where x is modular for $\Gamma^0(n)$, then τ is fixed under a transformation of determinant 1. Thus the only values of $j(\tau)$ which may appear in the discriminant are for $\tau = i$ and ϱ, giving an extension generated by the roots of an equation with even smaller coefficients.

REFERENCES

1. APOSTOL, T.M., *Modular Functions and Dirichlet series in Number Theory*, Springer-Verlag, New York, 1976.

2. BIRCH, B.J. and KUYK, W., *Modular Functions of one Variable IV*, Lecture Notes in Mathematics, vol.476, Springer-Verlag, 1975.

3. COHN, H., Fricke's Two-valued Modular Equations, *Mathematics of Computation*, vol.51, no.184, 1988, pp.787-807.

4. FRICKE, R., *Lehrbruch der Algebra III*, Braunschweig, 1928.

5. GUNNING, R., *Lectures on Modular Forms*, Princetown University Press, 1962.

6. HARTLEY, B., and HAWKES, T.O., *Rings, Modules and Linear Algebra*, Chapmann and Hall, 1970.

7. HARTSHORNE, R., *Algebraic Geometry*, Springer-Verlag, New York, 1977.

8. KNOPP, M.I., *Modular Functions in Analytic Number Theory*, Markham, 1970.

9. LANG, S.,*Elliptic Functions*, Addison Wesley, 1973.

10. LANG, S., *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

11. MACBEATH, A.M., Extensions of the Rationals with Galois group $\mathrm{PGL}(2, \mathbb{Z}_n)$, *Bulletin London Math. Soc.*, 1, 1969, pp.332-338.

12. OGG, A., *Modular Forms and Dirichlet series*, Benjamin, New York, 1969.

13. RANKIN, R., *Modular Forms and Functions*, Cambridge, 1977.

14. SAMUEL, P., *Algebraic Theory of Numbers*, Hermann, Paris, 1970.

15. SCHOENEBERG, B., *Elliptic Modular Functions*, Springer-Verlag, New York, 1974.

16. SERRE, J-P., *Abelian l-adic Representations*, Benjamin, New York, 1968.

17. SERRE, J-P., *A Course in Arithmetic*, Springer-Verlag, New York, 1973.

18. SERRE, J-P., Propriétés galoisennes des points d'ordre fini des courbes elliptiques, *Inventiones Math.*, vol.5, 1972, pp.259-331.

19. SHIMURA, G., *Introduction to the Arithmetic Theory of Automorphic Functions*, Princetown University Press, 1971.

20. VELU, J., Isogénies entre courbes elliptiques, *Comptes Rendues Acad. Sci. Paris*, vol.273A-B, 1971, pp.A238-A241.

21. YUI, N., Explicit form of the modular equaion, *J. Reine Angew. Math.*, vol.299/300, 1978, pp.185-200.