Hilbert's Irreducibility, Modular Forms, and Computation of Certain Galois Groups (joint with I. Kodrnja)

Modular curves and Galois representations
Zagreb, Croatia, September 18– 22, 2023

Goran Muić

September 22, 2023

Notation

Notation

$SL_2(\mathbb{R})$ is defined by

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ;\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane:

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; \ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az+b}{cz+d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az+b}{cz+d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az+b}{cz+d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

let $N \geq 1$, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ c \equiv 0\ (mod\ N) \right\}$$

Notation

$SL_2(\mathbb{R})$ is defined by

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

$\mathbb{H}$ is the upper half–plane: $Im(z) > 0$
$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ in a well–known way

$$g.z = \frac{az+b}{cz+d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}), \quad z \in \mathbb{H}$$

let $N \geq 1$, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ c \equiv 0\ (mod\ N) \right\}$$

the set of cusps for groups $\Gamma_0(N)$ is $\mathbb{Q} \cup \{\infty\}$

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for $\Gamma_0(N)$ of (integral) even weight $m \geq 0$ if

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for $\Gamma_0(N)$ of (integral) even weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z), \quad \text{for all} \quad z \in \mathbb{H}, \ \gamma \in \Gamma_0(N)$, where

$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for $\Gamma_0(N)$ of (integral) even weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma_0(N)$, where

$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f has a Fourier expansion so called q–**expansion**

$$f(z) = a_0 + a_1 q + a_2 q^2 + \cdots, \quad q = \exp\left(2\pi\sqrt{-1}z\right),$$

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for $\Gamma_0(N)$ of (integral) even weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z), \quad$ for all $\quad z \in \mathbb{H},\ \gamma \in \Gamma_0(N)$, where

$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f has a Fourier expansion so called q**–expansion**

$$f(z) = a_0 + a_1 q + a_2 q^2 + \cdots, \quad q = \exp\left(2\pi\sqrt{-1}z\right),$$

and condition 3. f is a cusp form if $a_0 = 0$

Modular forms of one variable

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for $\Gamma_0(N)$ of (integral) even weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma_0(N)$, where

$$j(\gamma, z) \overset{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f has a Fourier expansion so called q**–expansion**

$$f(z) = a_0 + a_1 q + a_2 q^2 + \cdots, \quad q = \exp(2\pi\sqrt{-1}z),$$

and condition 3. f is a cusp form if $a_0 = 0$

the space of all modular forms $M_m(\Gamma_0(N))$, the space of cuspidal modular forms (or cusp forms) $S_m(\Gamma_0(N))$

a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called modular form for $\Gamma_0(N)$ of (integral) even weight $m \geq 0$ if

1. $f(\gamma.z) = j(\gamma, z)^m f(z)$, for all $z \in \mathbb{H}$, $\gamma \in \Gamma_0(N)$, where

$$j(\gamma, z) \stackrel{def}{=} cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2. f has a Fourier expansion so called q**–expansion**

$$f(z) = a_0 + a_1 q + a_2 q^2 + \cdots , \quad q = \exp\left(2\pi\sqrt{-1}z\right),$$

and condition 3. f is a cusp form if $a_0 = 0$

the space of all modular forms $M_m(\Gamma_0(N))$, the space of cuspidal modular forms (or cusp forms) $S_m(\Gamma_0(N))$ by the Riemann–Roch theorem they are finite dimensional

Modular forms of one variable

Famous example: Ramanujan Δ function is a cusp form for $SL_2(\mathbb{Z}) = \Gamma_0(1)$ of weight 12:

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - \cdots \in S_{12}(\Gamma_0(1))$$

Famous example: Ramanujan Δ function is a cusp form for $SL_2(\mathbb{Z}) = \Gamma_0(1)$ of weight 12:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - \cdots \in S_{12}(\Gamma_0(1))$$

Eisenstein series: $E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \in M_4(\Gamma_0(1))$, $\sigma_3(n) = \sum_{0<d|n} d^3$

Famous example: Ramanujan Δ function is a cusp form for $SL_2(\mathbb{Z}) = \Gamma_0(1)$ of weight 12:

$$\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = q - 24q^2 + 252q^3 - \cdots \in S_{12}(\Gamma_0(1))$$

Eisenstein series: $E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \in M_4(\Gamma_0(1))$, $\sigma_3(n) = \sum_{0<d|n} d^3$

$\Delta(N\cdot), E_4^3(N\cdot) \in M_{12}(\Gamma_0(N)),\ N \geq 1$

Modular forms of one variable

Note: not all interesting cusp forms comes from geometry i.e., not all are coming from $\frac{m}{2}$–holomorphic differentials. For example $\Delta(N\cdot)$.

For us it is important:

Note: not all interesting cusp forms comes from geometry i.e., not all are coming from $\frac{m}{2}$–holomorphic differentials. For example $\Delta(N\cdot)$.

For us it is important:

By Eichler–Shimura theory and explicit determination of certain Eisenstein series, we know that $S_m(\Gamma_0(N))$, and $M_m(\Gamma_0(N))$, for $m \geq 2$ even, have basis consisting of forms with integral q–expansions

Note: not all interesting cusp forms comes from geometry i.e., not all are coming from $\frac{m}{2}$–holomorphic differentials. For example $\Delta(N\cdot)$.

For us it is important:

By Eichler–Shimura theory and explicit determination of certain Eisenstein series, we know that $S_m(\Gamma_0(N))$, and $M_m(\Gamma_0(N))$, for $m \geq 2$ even, have basis consisting of forms with integral q–expansions

We let $S_m(\Gamma_0(N))_{\mathbb{Q}}$ be the $\mathbb{Q}$–span of all cusp forms in $S_m(\Gamma_0(N))$

Modular curve $X_0(N)$

Modular curve $X_0(N)$

let $j = E_4^3/\Delta$, then $\mathbb{Q}(j, j(N\cdot))$ has transcendence degree one over $\mathbb{Q}$, the corresponding curve $X_0(N)$ is curve modular curve i.e., the field of rational function is over $\mathbb{Q}$, $\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j(N\cdot))$

Modular curve $X_0(N)$

let $j = E_4^3/\Delta$, then $\mathbb{Q}(j, j(N\cdot))$ has transcendence degree one over $\mathbb{Q}$, the corresponding curve $X_0(N)$ is curve modular curve i.e., the field of rational function is over $\mathbb{Q}$, $\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j(N\cdot))$

for $m \geq 2$ an even integer, let f, g, h be three linearly independent modular forms in $M_m(\Gamma)$ with rational q–expansions,

Modular curve $X_0(N)$

let $j = E_4^3/\Delta$, then $\mathbb{Q}(j, j(N\cdot))$ has transcendence degree one over $\mathbb{Q}$, the corresponding curve $X_0(N)$ is curve modular curve i.e., the field of rational function is over $\mathbb{Q}$, $\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j(N\cdot))$

for $m \geq 2$ an even integer, let f, g, h be three linearly independent modular forms in $M_m(\Gamma)$ with rational q–expansions, define a holomorphic map $X_0(N) \to \mathbb{P}^2$ by

$$z \in \mathbb{H} \longmapsto (f(z) : g(z) : h(z)) \in \mathbb{P}^2$$

Modular curve $X_0(N)$

let $j = E_4^3/\Delta$, then $\mathbb{Q}(j, j(N\cdot))$ has transcendence degree one over $\mathbb{Q}$, the corresponding curve $X_0(N)$ is curve modular curve i.e., the field of rational function is over $\mathbb{Q}$, $\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j(N\cdot))$

for $m \geq 2$ an even integer, let f, g, h be three linearly independent modular forms in $M_m(\Gamma)$ with rational q–expansions, define a holomorphic map $X_0(N) \to \mathbb{P}^2$ by

$$z \in \mathbb{H} \longmapsto (f(z) : g(z) : h(z)) \in \mathbb{P}^2$$

is a regular map between projective varieties, defined over $\mathbb{Q}$.

Modular curve $X_0(N)$

let $j = E_4^3/\Delta$, then $\mathbb{Q}(j, j(N\cdot))$ has transcendence degree one over $\mathbb{Q}$, the corresponding curve $X_0(N)$ is curve modular curve i.e., the field of rational function is over $\mathbb{Q}$, $\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j(N\cdot))$

for $m \geq 2$ an even integer, let f, g, h be three linearly independent modular forms in $M_m(\Gamma)$ with rational q–expansions, define a holomorphic map $X_0(N) \to \mathbb{P}^2$ by

$$z \in \mathbb{H} \longmapsto (f(z) : g(z) : h(z)) \in \mathbb{P}^2$$

is a regular map between projective varieties, defined over $\mathbb{Q}$. the image is an irreducible complex projective curve which we denote by $\mathcal{C}(f, g, h)$ defined over $\mathbb{Q}$

it is easy to check that the map is birational over $\mathbb{C}$ if and only if it is birational over $\mathbb{Q}$.

it is easy to check that the map is birational over $\mathbb{C}$ if and only if it is birational over $\mathbb{Q}$.

In our earlier papers M., *On degrees and birationality of the maps $X_0(N) \to \mathbb{P}^2$ constructed via modular forms,* Monatsh. Math. **Vol. 180, No. 3**, 607–629, (2016), and G. M., I. KODRNJA *On primitive elements of algebraic function fields and models of $X_0(N)$*, The Ramanujan Journal, **55** No. 2 (2021) we study these problems in detail (besides vast literature before) giving several algorithms for birationality

it is easy to check that the map is birational over $\mathbb{C}$ if and only if it is birational over $\mathbb{Q}$.

In our earlier papers M., *On degrees and birationality of the maps $X_0(N) \to \mathbb{P}^2$ constructed via modular forms,* Monatsh. Math. **Vol. 180, No. 3**, 607–629, (2016), and G. M., I. KODRNJA *On primitive elements of algebraic function fields and models of $X_0(N)$*, The Ramanujan Journal, **55** No. 2 (2021) we study these problems in detail (besides vast literature before) giving several algorithms for birationality

We mention the next result

Modular curve $X_0(N)$

Modular curve $X_0(N)$

Theorem

Assume that either $m = 2$ and $X_0(N)$ is not hyperelliptic (implies $g(\Gamma_0(N)) \geq 3$) or $m \geq 4$ is an even integer such that $\dim S_m(\Gamma_0(N)) \geq \max\left(g(\Gamma_0(N)) + 2, 3\right)$. Then, we have the following:

(i) *Let $f_0, \ldots, f_{s-1}$ be a basis of $S_m(\Gamma_0(N))_{\mathbb{Q}}$. Then, $\mathbb{Q}(X_0(N))$ is generated over $\mathbb{Q}$ by the quotients f_i/f_0, $1 \leq i \leq s-1$.*

(ii) *Assume that $f, g \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$. Then, there exists a non-empty Zariski open set $\mathcal{U}_{f,g} \subset S_m(\Gamma_0(N))_{\mathbb{Q}}$ such that $X_0(N)$ is birationally equivalent over $\mathbb{Q}$ to $\mathcal{C}(f,g,h)$ via the map constructed from f, g, h i.e., $\mathbb{Q}\left(g/f, h/f\right) = \mathbb{Q}\left(X_0(N)\right)$ for any $h \in \mathcal{U}_{f,g}$. The elements of set $\mathcal{U}_{f,g}$ are effectively computable from q–expansions of f and g.*

Polynomials

Polynomials

there exists an irreducible over $\mathbb{Z}$ homogeneous polynomial with integral coefficients $P_{f,g,h}$ such that $P_{f,g,h}(f,g,h) = 0$ assuming that $f, g, h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ be linearly independent

Polynomials

there exists an irreducible over $\mathbb{Z}$ homogeneous polynomial with integral coefficients $P_{f,g,h}$ such that $P_{f,g,h}(f,g,h) = 0$ assuming that $f, g, h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ be linearly independent

$P_{f,g,h}$ can be computed in the SAGE software system given q–expansions of the modular forms f, g and h (for reasonably small N)

Polynomials

there exists an irreducible over $\mathbb{Z}$ homogeneous polynomial with integral coefficients $P_{f,g,h}$ such that $P_{f,g,h}(f,g,h) = 0$ assuming that $f, g, h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ be linearly independent

$P_{f,g,h}$ can be computed in the SAGE software system given q–expansions of the modular forms f, g and h (for reasonably small N)

$P_{f,g,h}$ is a classical reduced equation of the curve $\mathcal{C}(f,g,h)$

Polynomials

there exists an irreducible over $\mathbb{Z}$ homogeneous polynomial with integral coefficients $P_{f,g,h}$ such that $P_{f,g,h}(f,g,h) = 0$ assuming that $f,g,h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ be linearly independent

$P_{f,g,h}$ can be computed in the SAGE software system given q–expansions of the modular forms f, g and h (for reasonably small N)

$P_{f,g,h}$ is a classical reduced equation of the curve $\mathcal{C}(f,g,h)$

let $Q_{f,g,h}$ be its dehomogenization with respect to the first variable there exists an irreducible over $\mathbb{Z}$ homogeneous polynomial with integral coefficients $P_{f,g,h}$ such that $P_{f,g,h}(f,g,h)=0$ assuming that $f,g,h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ be linearly independent

$P_{f,g,h}$ can be computed in the SAGE software system given q–expansions of the modular forms f, g and h (for reasonably small N)

$P_{f,g,h}$ is a classical reduced equation of the curve $\mathcal{C}(f,g,h)$

let $Q_{f,g,h}$ be its dehomogenization with respect to the first variable

again, we obtain an irreducible over $\mathbb{Z}$ polynomial with integral coefficients, $Q_{f,g,h}(g/f, h/f)=0$ in $\mathbb{Q}\left(X_0(N)\right)$

Polynomials

there exists an irreducible over $\mathbb{Z}$ homogeneous polynomial with integral coefficients $P_{f,g,h}$ such that $P_{f,g,h}(f,g,h) = 0$ assuming that $f, g, h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ be linearly independent

$P_{f,g,h}$ can be computed in the SAGE software system given q–expansions of the modular forms f, g and h (for reasonably small N)

$P_{f,g,h}$ is a classical reduced equation of the curve $\mathcal{C}(f,g,h)$

let $Q_{f,g,h}$ be its dehomogenization with respect to the first variable

again, we obtain an irreducible over $\mathbb{Z}$ polynomial with integral coefficients, $Q_{f,g,h}(g/f, h/f) = 0$ in $\mathbb{Q}(X_0(N))$

the polynomial $Q_{f,g,h}$ depend on both variables since since f, g, h are linearly independent

Polynomials

Polynomials

given f, g, h linearly independent over $\mathbb{Q}$, we construct polynomial $Q_{f,g,h}$ as before

Polynomials

given f, g, h linearly independent over $\mathbb{Q}$, we construct polynomial $Q_{f,g,h}$ as before

observe that (unnormalized) minimal polynomial of $h/f \in \mathbb{Q}(X_0(N))$ over $\mathbb{Q}(g/f)$ is $Q_{f,g,h}(g/f, \cdot)$

Polynomials

given f, g, h linearly independent over $\mathbb{Q}$, we construct polynomial $Q_{f,g,h}$ as before

observe that (unnormalized) minimal polynomial of $h/f \in \mathbb{Q}(X_0(N))$ over $\mathbb{Q}(g/f)$ is $Q_{f,g,h}(g/f, \cdot)$
$\implies \deg Q_{f,g,h}(g/f, \cdot) \leq [\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] =$ the degree of the divisor of zeores of g/f

Polynomials

given f, g, h linearly independent over $\mathbb{Q}$, we construct polynomial $Q_{f,g,h}$ as before

observe that (unnormalized) minimal polynomial of $h/f \in \mathbb{Q}(X_0(N))$ over $\mathbb{Q}(g/f)$ is $Q_{f,g,h}(g/f, \cdot)$
$\implies \deg Q_{f,g,h}(g/f, \cdot) \leq [\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] =$ the degree of the divisor of zeores of g/f

when f, g, h define a birational map, then $\deg Q_{f,g,h}(g/f, \cdot) = [\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$ then various gonality results give lower bound of the degree (Abramovich, Najman, Orlić, ...)

The problem

The problem

let $L_{f,g,h}$ be the splitting field $Q_{f,g,h}(g/f, \cdot)$ containing $\mathbb{Q}(g/f, h/f)$, $G_{f,g,h}$ is the Galois group $Gal(L_{f,g,h}/\mathbb{Q}(g/f))$

The problem

let $L_{f,g,h}$ be the splitting field $Q_{f,g,h}(g/f, \cdot)$ containing $\mathbb{Q}(g/f, h/f)$, $G_{f,g,h}$ is the Galois group $Gal(L_{f,g,h}/\mathbb{Q}(g/f))$

THE GOAL: is to study $L_{f,g,h}$ and $G_{f,g,h}$ for various f, g, h

The problem

let $L_{f,g,h}$ be the splitting field $Q_{f,g,h}(g/f, \cdot)$ containing $\mathbb{Q}(g/f, h/f)$, $G_{f,g,h}$ is the Galois group $Gal(L_{f,g,h}/\mathbb{Q}(g/f))$

THE GOAL: is to study $L_{f,g,h}$ and $G_{f,g,h}$ for various f, g, h

in fact study polynomials $Q_{f,g,h}$ with integral coefficients

The problem

let $L_{f,g,h}$ be the splitting field $Q_{f,g,h}(g/f, \cdot)$ containing $\mathbb{Q}(g/f, h/f)$, $G_{f,g,h}$ is the Galois group $Gal(L_{f,g,h}/\mathbb{Q}(g/f))$

THE GOAL: is to study $L_{f,g,h}$ and $G_{f,g,h}$ for various f, g, h

in fact study polynomials $Q_{f,g,h}$ with integral coefficients

for example, fix f, g and let h vary let $L_{f,g,h}$ be the splitting field $Q_{f,g,h}(g/f, \cdot)$ containing $\mathbb{Q}(g/f, h/f)$, $G_{f,g,h}$ is the Galois group $Gal(L_{f,g,h}/\mathbb{Q}(g/f))$

THE GOAL: is to study $L_{f,g,h}$ and $G_{f,g,h}$ for various f, g, h

in fact study polynomials $Q_{f,g,h}$ with integral coefficients

for example, fix f, g and let h vary

then, using the trivial estimate $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] \leq l_{m,N} \stackrel{def}{=} \dim S_m(\Gamma_0(N)) + g(\Gamma_0(N)) - 1 - \epsilon_m$, $\epsilon_2 = 1$ and $\epsilon_m = 0$ for $m \geq 4$, we see that up to an isomorphism of groups we can have only finitely many groups $G_{f,g,h}$ up to an isomorphism when we let h vary over $S_m(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$

The problem

Definition

Keep f, g fixed. Let $\mathcal{G} = \mathcal{G}_{f,g}$ be the set consisting of all representatives of groups $G_{f,g,h}$, $h \in S_m(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$ up to isomorphism. For $G \in \mathcal{G}$, let Ξ_G be the set of all $h \in S_m(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$ such that $G_h \simeq G$. We denote by Ξ'_G the set of all $h \in \Xi_G$ such that the degree of $Q_{f,g,h}(g/f, \cdot)$ is $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$ i.e., the map given by f, g, h is birational over $\mathbb{Q}$ ($\iff \mathbb{Q}(g/f, h/f) = \mathbb{Q}(X_0(N))$).

The problem

Definition

Keep f, g fixed. Let $\mathcal{G} = \mathcal{G}_{f,g}$ be the set consisting of all representatives of groups $G_{f,g,h}$, $h \in S_m(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$ up to isomorphism. For $G \in \mathcal{G}$, let Ξ_G be the set of all $h \in S_m(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$ such that $G_h \simeq G$. We denote by Ξ'_G the set of all $h \in \Xi_G$ such that the degree of $Q_{f,g,h}(g/f, \cdot)$ is $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$ i.e., the map given by f, g, h is birational over $\mathbb{Q}$ ($\iff \mathbb{Q}(g/f, h/f) = \mathbb{Q}(X_0(N))$).

to deal with the sets Ξ_G and Ξ'_G we use Hilbert's irreducibility

Hilbert's irreducibilty

Hilbert's irreducibilty

Serre: a subset $A \subset \mathbb{Z}$ thin if the number of elements in the intersection of A with a segment $[-n, n]$ is $O(n^{1/2})$ as $n \longrightarrow \infty$.

Serre: a subset $A \subset \mathbb{Z}$ thin if the number of elements in the intersection of A with a segment $[-n, n]$ is $O(n^{1/2})$ as $n \longrightarrow \infty$.

For $\lambda \in \mathbb{Z}$, we let $L_{f,g,h,\lambda}$ be the splitting field of $Q_{f,g,h}(\lambda, \cdot)$, and $G_{f,g,h,\lambda} \overset{def}{=} Gal(L_{h,\lambda}/\mathbb{Q})$.

Serre: a subset $A \subset \mathbb{Z}$ thin if the number of elements in the intersection of A with a segment $[-n, n]$ is $O(n^{1/2})$ as $n \longrightarrow \infty$.

For $\lambda \in \mathbb{Z}$, we let $L_{f,g,h,\lambda}$ be the splitting field of $Q_{f,g,h}(\lambda, \cdot)$, and $G_{f,g,h,\lambda} \overset{def}{=} Gal(L_{h,\lambda}/\mathbb{Q})$.

Hilbert's irreducibility $\Longrightarrow$ There exists a thin subset $A_{f,g,h} \subset \mathbb{Z}$ such that $G_{f,g,h}$ is isomorphic to $G_{f,g,h,\lambda}$, for $\lambda \in \mathbb{Z} - A_{f,g,h}$

Hilbert's irreducibilty

Serre: a subset $A \subset \mathbb{Z}$ thin if the number of elements in the intersection of A with a segment $[-n, n]$ is $O(n^{1/2})$ as $n \longrightarrow \infty$.

For $\lambda \in \mathbb{Z}$, we let $L_{f,g,h,\lambda}$ be the splitting field of $Q_{f,g,h}(\lambda, \cdot)$, and $G_{f,g,h,\lambda} \stackrel{def}{=} Gal(L_{h,\lambda}/\mathbb{Q})$.

Hilbert's irreducibility $\implies$ There exists a thin subset $A_{f,g,h} \subset \mathbb{Z}$ such that $G_{f,g,h}$ is isomorphic to $G_{f,g,h,\lambda}$, for $\lambda \in \mathbb{Z} - A_{f,g,h}$

but for our applications polynomail $Q_{f,g,h}$ needs to be transformed a little bit in a standard fashion

Serre: a subset $A \subset \mathbb{Z}$ thin if the number of elements in the intersection of A with a segment $[-n, n]$ is $O(n^{1/2})$ as $n \longrightarrow \infty$.

For $\lambda \in \mathbb{Z}$, we let $L_{f,g,h,\lambda}$ be the splitting field of $Q_{f,g,h}(\lambda, \cdot)$, and $G_{f,g,h,\lambda} \overset{def}{=} Gal(L_{h,\lambda}/\mathbb{Q})$.

Hilbert's irreducibility $\implies$ There exists a thin subset $A_{f,g,h} \subset \mathbb{Z}$ such that $G_{f,g,h}$ is isomorphic to $G_{f,g,h,\lambda}$, for $\lambda \in \mathbb{Z} - A_{f,g,h}$

but for our applications polynomail $Q_{f,g,h}$ needs to be transformed a little bit in a standard fashion

write $Q_{f,g,h}(\lambda, T) = \sum_{i=1}^{n} a_i(\lambda) T^i \in \mathbb{Z}[\lambda, T]$, λ, T variables

Hilbert's irreducibilty

Serre: a subset $A \subset \mathbb{Z}$ thin if the number of elements in the intersection of A with a segment $[-n, n]$ is $O(n^{1/2})$ as $n \longrightarrow \infty$.

For $\lambda \in \mathbb{Z}$, we let $L_{f,g,h,\lambda}$ be the splitting field of $Q_{f,g,h}(\lambda, \cdot)$, and $G_{f,g,h,\lambda} \stackrel{def}{=} Gal(L_{h,\lambda}/\mathbb{Q})$.

Hilbert's irreducibility $\implies$ There exists a thin subset $A_{f,g,h} \subset \mathbb{Z}$ such that $G_{f,g,h}$ is isomorphic to $G_{f,g,h,\lambda}$, for $\lambda \in \mathbb{Z} - A_{f,g,h}$

but for our applications polynomail $Q_{f,g,h}$ needs to be transformed a little bit in a standard fashion

write $Q_{f,g,h}(\lambda, T) = \sum_{i=1}^{n} a_i(\lambda) T^i \in \mathbb{Z}[\lambda, T]$, λ, T variables

$$\widetilde{Q}_{f,g,h}(\lambda, T) \stackrel{def}{=} a_n(\lambda)^{n-1} Q(\lambda, T/a_n(\lambda)) =$$
$$T^n + a_{n-1}(\lambda) T^{n-1} + \sum_{i=1}^{n-2} a_n(\lambda)^{n-1-i} a_i(\lambda) T^i$$

Application of Hilbert's irreducibilty

Application of Hilbert's irreducibilty

the following theorem is useful for explicit computations

Application of Hilbert's irreducibilty

the following theorem is useful for explicit computations
we regard $G_{f,g,h}$ a subgroup of symmteric group of n letters

Application of Hilbert's irreducibilty

the following theorem is useful for explicit computations
we regard $G_{f,g,h}$ a subgroup of symmteric group of n letters

using Hilbert's irreducibility and famous theorem of Frobenius (latter generalized by Chebotarev)

Theorem

$G_{f,g,h}$ contains a permutation with a cycle pattern $n_1, n_2, \ldots, n_t$ if and only if there exists a prime number p and $r \in \{0, 1, \ldots, p-1\}$ such that $\widetilde{Q}_{f,g,h}(r, T) =$ $T^n + a_{n-1}(r)T^{n-1} + \sum_{i=1}^{n-2} a_n(r)^{n-1-i} a_i(r) T^i \pmod{p}$ can be decomposed into a product of different irreducible factors of degrees $n_1, n_2, \ldots, n_t$.

Some general results (part 1)

Theorem

Let $m \geq 2$ be an even integer such that $\dim S_m(\Gamma_0(N))_{\mathbb{Q}} \geq 3$*. Then, there exists a thin subset $A_{m,N} \subset \mathbb{Z}$, and triples of linearly independent forms $f_i, g_i, h_i \in S_m(\Gamma_0(N))_{\mathbb{Q}}$, $1 \leq i \leq k$, such that for any $f, g, h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ which are linearly independent, there exists i such that $G_{f,g,h} \simeq G_{f_i,g_i,h_i,\lambda}$, $\lambda \in \mathbb{Z} - A_{m,N}$.*

Some general results (part 2)

Theorem

Assume that either $m = 2$ *and* $X_0(N)$ *is not hyperelliptic (implies* $g(\Gamma_0(N)) \geq 3$*) or* $m \geq 4$ *is an even integer such that* $\dim S_m(\Gamma_0(N)) \geq \max\left(g(\Gamma_0(N)) + 2, 3\right)$*. Assume that* $f, g \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ *are linearly independent. Then, there exists a subgroup* G *of the symmetric group of* $l_{m,N}$*–letters such that* Ξ'_G *is Zariski dense in* $S_m(\Gamma_0(N))_{\mathbb{Q}}$*.*

The Case of Non–Hyperelliptic Modular Curves

The Case of Non–Hyperelliptic Modular Curves

by Ogg $X_0(N)$ is non–hyperelliptic for
$N \in \{34, 38, 42, 43, 44, 45, 51 - 58, 60 - 70\}$ or $N \geq 72$
$\Longrightarrow g(\Gamma_0(N)) \geq 3$

The Case of Non–Hyperelliptic Modular Curves

by Ogg $X_0(N)$ is non–hyperelliptic for
$N \in \{34, 38, 42, 43, 44, 45, 51 - 58, 60 - 70\}$ or $N \geq 72$
$\implies g(\Gamma_0(N)) \geq 3$

Theorem

Maintaining above assumptions, we select f and g in $S_2(\Gamma_0(N))_{\mathbb{Q}}$ with largest possible orders of vanishing at $\mathfrak{a}_\infty$ (a point in $X_0(N)$ that corresponds to a cusp ∞), $\nu_\infty(f) < \nu_\infty(g)$. Then, $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] \leq g(\Gamma_0(N))$. Consequently, for $h \in S_2(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$, $G_{f,g,h}$ can be embedded as a subgroup of the symmetric group of $g(\Gamma_0(N))$–letters $S_{g(\Gamma_0(N))}$ (non–uniquely). Moreover, there exists a subgroup G of $S_{g(\Gamma_0(N))}$ such that Ξ'_G is Zariski dense in $S_2(\Gamma_0(N))_{\mathbb{Q}}$.

Some comments on the theorem

Some comments on the theorem

$$\dim S_2(\Gamma_0(N)_{\mathbb{Q}} = g(\Gamma_0(N))$$

Some comments on the theorem

$\dim S_2(\Gamma_0(N)_{\mathbb{Q}} = g(\Gamma_0(N))$

we obtain a bound $\#G \leq g(\Gamma_0(N))!$ on the size of every possible Galois group $G \in \mathcal{G}_{f,g}$

$\dim S_2(\Gamma_0(N)_{\mathbb{Q}} = g(\Gamma_0(N))$

we obtain a bound $\#G \leq g(\Gamma_0(N))!$ on the size of every possible Galois group $G \in \mathcal{G}_{f,g}$

Now, we give some examples of explicit computations

The case $N = 63$

The case $N = 63$

Consider three basis elements of 5–dimensional space $S_2(\Gamma_0(63))$ having highest order of zero at ∞:

$$
\begin{aligned}
f &\stackrel{def}{=} q^4 + q^7 - 4q^{10} + 2q^{13} - 2q^{16} - 4q^{19} + 5q^{22} + \cdots , \\
g &\stackrel{def}{=} 2q^5 - q^8 - 3q^{11} - q^{14} + 2q^{17} + q^{23} + \cdots , \\
h &\stackrel{def}{=} q^3 - q^6 + q^9 - q^{12} - 2q^{15} - q^{18} - q^{21} + 3q^{24} + \cdots .
\end{aligned}
$$

The case $N = 63$

Consider three basis elements of 5–dimensional space $S_2(\Gamma_0(63))$ having highest order of zero at ∞:

$$f \overset{def}{=} q^4 + q^7 - 4q^{10} + 2q^{13} - 2q^{16} - 4q^{19} + 5q^{22} + \cdots,$$

$$g \overset{def}{=} 2q^5 - q^8 - 3q^{11} - q^{14} + 2q^{17} + q^{23} + \cdots,$$

$$h \overset{def}{=} q^3 - q^6 + q^9 - q^{12} - 2q^{15} - q^{18} - q^{21} + 3q^{24} + \cdots.$$

Proposition

Maintaining above assumptions, we have $G_{f,g,h} \simeq S(5)$, $h \in \Xi'_{S(5)}$, $\mathbb{Q}(g/f, h/f) = \mathbb{Q}(X_0(63))$.

The case $N = 63$

The case $N = 63$

the polynomial $P_{f,g,h}$ is determined by
$-2h^4f^2 - hf^5 + h^5g + 2h^2f^3g + h^3fg^2 - f^4g^2 + 3hf^2g^3 - 3h^2g^4 = 0$
(computed in SAGE)

The case $N = 63$

the polynomial $P_{f,g,h}$ is determined by
$-2h^4f^2 - hf^5 + h^5g + 2h^2f^3g + h^3fg^2 - f^4g^2 + 3hf^2g^3 - 3h^2g^4 = 0$
(computed in SAGE)

$Q_{f,g,h}(\lambda, T) =$
$\lambda T^5 - 2T^4 + \lambda^2 T^3 + \left(2\lambda - 3\lambda^4\right) T^2 + \left(3\lambda^3 - 1\right) T - \lambda^2$

The case $N = 63$

the polynomial $P_{f,g,h}$ is determined by
$-2h^4f^2 - hf^5 + h^5g + 2h^2f^3g + h^3fg^2 - f^4g^2 + 3hf^2g^3 - 3h^2g^4 = 0$
(computed in SAGE)

$$Q_{f,g,h}(\lambda, T) = \lambda T^5 - 2T^4 + \lambda^2 T^3 + \left(2\lambda - 3\lambda^4\right) T^2 + \left(3\lambda^3 - 1\right) T - \lambda^2$$

$$\widetilde{Q}_{f,g,h}(\lambda, T) = T^5 - 2T^4 + \lambda^3 T^3 + \left(2\lambda - 3\lambda^4\right) \lambda^2 T^2 + \left(3\lambda^3 - 1\right) \lambda^3 T - \lambda^6$$

The case $N = 63$

the polynomial $P_{f,g,h}$ is determined by
$-2h^4f^2 - hf^5 + h^5g + 2h^2f^3g + h^3fg^2 - f^4g^2 + 3hf^2g^3 - 3h^2g^4 = 0$
(computed in SAGE)

$Q_{f,g,h}(\lambda, T) =$
$\lambda T^5 - 2T^4 + \lambda^2 T^3 + \left(2\lambda - 3\lambda^4\right) T^2 + \left(3\lambda^3 - 1\right) T - \lambda^2$

$\widetilde{Q}_{f,g,h}(\lambda, T) =$
$T^5 - 2T^4 + \lambda^3 T^3 + \left(2\lambda - 3\lambda^4\right) \lambda^2 T^2 + \left(3\lambda^3 - 1\right) \lambda^3 T - \lambda^6$

For $\lambda \equiv -1 \pmod 3$, reducing $\equiv \pmod 3$, the polynomial $\widetilde{Q}_{f,g,h}(\lambda, T)$ becomes $T^5 + T^4 - T^3 + T^2 + T + 1$ which is irreducible over $\mathbb{Z}/3\mathbb{Z}$

The case $N = 63$

the polynomial $P_{f,g,h}$ is determined by
$-2h^4f^2 - hf^5 + h^5g + 2h^2f^3g + h^3fg^2 - f^4g^2 + 3hf^2g^3 - 3h^2g^4 = 0$
(computed in SAGE)

$Q_{f,g,h}(\lambda, T) =$
$\lambda T^5 - 2T^4 + \lambda^2T^3 + \left(2\lambda - 3\lambda^4\right)T^2 + \left(3\lambda^3 - 1\right)T - \lambda^2$

$\widetilde{Q}_{f,g,h}(\lambda, T) =$
$T^5 - 2T^4 + \lambda^3T^3 + \left(2\lambda - 3\lambda^4\right)\lambda^2T^2 + \left(3\lambda^3 - 1\right)\lambda^3T - \lambda^6$

For $\lambda \equiv -1 \pmod 3$, reducing $\equiv \pmod 3$, the polynomial $\widetilde{Q}_{f,g,h}(\lambda, T)$ becomes $T^5 + T^4 - T^3 + T^2 + T + 1$ which is irreducible over $\mathbb{Z}/3\mathbb{Z} \implies G_{f,g,h}$ contains a 5–cycle

The case $N = 63$

The case $N = 63$

for $\lambda \equiv -1 \pmod 7$, the polynomial $\widetilde{Q}_{f,g,h}(\lambda, T)$ becomes a product of two irreducible polynomials

$$T^5 - 2T^4 - T^3 + 2T^2 + 3T - 1 = \left(T^2 - T + 3\right) \cdot \left(T^3 - T^2 + 4T + 2\right).$$

The case $N = 63$

for $\lambda \equiv -1 \pmod 7$, the polynomial $\widetilde{Q}_{f,g,h}(\lambda, T)$ becomes a product of two irreducible polynomials

$$T^5 - 2T^4 - T^3 + 2T^2 + 3T - 1 = \left(T^2 - T + 3\right) \cdot \left(T^3 - T^2 + 4T + 2\right).$$

This shows that the Galois group $G_{f,g,h}$ contains a permutation which is a product of commuting 2–cycle and 3–cycle. Its cube is a transposition.

The case $N = 63$

for $\lambda \equiv -1 \pmod 7$, the polynomial $\widetilde{Q}_{f,g,h}(\lambda, T)$ becomes a product of two irreducible polynomials

$$T^5 - 2T^4 - T^3 + 2T^2 + 3T - 1 = \left(T^2 - T + 3\right) \cdot \left(T^3 - T^2 + 4T + 2\right).$$

This shows that the Galois group $G_{f,g,h}$ contains a permutation which is a product of commuting 2–cycle and 3–cycle. Its cube is a transposition.

$$\implies G_{f,g,h} = S(5)$$

The case $N = 72$

The case $N = 72$

We have $g(\Gamma_0(72)) = 5$. Using SAGE, the basis of 5–dimensional space $S_2(\Gamma_0(72))$ is given by

The case $N = 72$

We have $g(\Gamma_0(72)) = 5$. Using SAGE, the basis of 5–dimensional space $S_2(\Gamma_0(72))$ is given by

$$f \overset{def}{=} f_0 \overset{def}{=} q^5 - 2q^{11} - q^{17} + 4q^{23} - 3q^{29} + \cdots ,$$
$$g \overset{def}{=} f_1 \overset{def}{=} q^7 - q^{13} - 3q^{19} + q^{25} + 3q^{31} + 4q^{37} + \cdots ,$$
$$f_2 \overset{def}{=} q^3 - q^9 - 2q^{15} + q^{27} + 4q^{33} - 2q^{39} + \cdots ,$$
$$f_3 \overset{def}{=} q^2 - 4q^{14} + 2q^{26} + 8q^{38} + \cdots ,$$
$$f_4 \overset{def}{=} q - 2q^{13} - 4q^{19} - q^{25} + 8q^{31} + 6q^{37} + \cdots .$$

The case $N = 72$

The case $N = 72$

Proposition

Let $h = f_3$. Then, we have that $G_{f,g,h} \simeq D(4)$ a dihedral group of order $2 \cdot 4 = 8$. Next, $h \in \Xi'_{D(4)}$. Moreover,
$\mathbb{Q}(g/f, h/f) = \mathbb{Q}(X_0(72))$,
$[\mathbb{Q}(X_0(72)) : \mathbb{Q}(g/f)] = 4 < g(\Gamma_0(72)) = 5$. *Moreover, the Galois group of the extension $\mathbb{Q}(X_0(72)) \subset L_{f,g,h}$ is generated by a transposition in $D(4)$.*

The case $N = 72$

Proposition

Let $h = f_3$. Then, we have that $G_{f,g,h} \simeq D(4)$ a dihedral group of order $2 \cdot 4 = 8$. Next, $h \in \Xi'_{D(4)}$. Moreover,
$\mathbb{Q}(g/f, h/f) = \mathbb{Q}(X_0(72))$,
$[\mathbb{Q}(X_0(72)) : \mathbb{Q}(g/f)] = 4 < g(\Gamma_0(72)) = 5$. *Moreover, the Galois group of the extension $\mathbb{Q}(X_0(72)) \subset L_{f,g,h}$ is generated by a transposition in $D(4)$.*

Proposition

Let $h = f_3 + f_4$. Then, $h \in \Xi'_{D(4)}$ and we have $G_{f,g,h} \simeq S(4)$. Moreover, $\mathbb{Q}(g/f, h/f) = \mathbb{Q}(X_0(72))$.

Proposition

Maintaining above assumptions, let $h = f_2$*. Then, we have* $G_{f,g,h} \simeq \mathbb{Z}/2\mathbb{Z}$*. Next,* $h \in \Xi_{\mathbb{Z}/2\mathbb{Z}}$ *but* $\Xi'_{\mathbb{Z}/2\mathbb{Z}} = \emptyset$*.*

MGMA routine

MGMA routine

The Galois groups of polynomials $\widetilde{Q}(\lambda, \cdot)$ over $\mathbb{Q}(\lambda)$ can also be computed using MAGMA system and a routine *GaloisGroup* due to Fiecker

The Case of Hyperelliptic Modular Curves

by

Ogg, $X_0(N)$ is a hyperelliptic curve if and only if N belongs to the set $\{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$.

by
Ogg, $X_0(N)$ is a hyperelliptic curve if and only if N belongs to the set $\{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$.

select $f, g \in S_2(\Gamma_0(N))_{\mathbb{Q}}$ such that their orders at ∞ satisfy that $\nu_\infty(g)$ is largest possible, and $\nu_\infty(f) = \nu_\infty(g) - 1$. The existence of f and g is easy to check using SAGE system.

The Case of Hyperelliptic Modular Curves

by
Ogg, $X_0(N)$ is a hyperelliptic curve if and only if N belongs to the set $\{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$.

select $f, g \in S_2(\Gamma_0(N))_{\mathbb{Q}}$ such that their orders at ∞ satisfy that $\nu_\infty(g)$ is largest possible, and $\nu_\infty(f) = \nu_\infty(g) - 1$. The existence of f and g is easy to check using SAGE system.

Theorem

Assume that $X_0(N)$ is a hyperelliptic curve, and $f, g \in S_2(\Gamma_0(N))_{\mathbb{Q}}$ as above. Then, we have the following:

(i) *The extension $\mathbb{Q}(g/f) \subset \mathbb{Q}(X_0(N))$ has the degree two, and therefore the Galois group is $\mathbb{Z}/2\mathbb{Z}$.*

(ii) *For all even integers $m \geq 4$ there exists a non-empty Zariski open set $\mathcal{U}_m \subset S_m(\Gamma_0(N))_{\mathbb{Q}}$ such that $L_{f^{\frac{m}{2}}, gf^{\frac{m}{2}-1}, h} = \mathbb{Q}(X_0(N)) = \mathbb{Q}\left(g/f, h/f^{m/2}\right)$, $h \in \mathcal{U}_m$.*

An example to the theorem

An example to the theorem

Let $N = 30$. Then, $g(\Gamma_0(30)) = 3$. Using SAGE we find the following base of $S_2(\Gamma_0(30))$:

$$f_0 = q - q^4 - q^6 - 2q^7 + q^9 + q^{10} + \cdots$$
$$f_1 = q^2 - q^4 - q^6 - q^8 + q^{10} + \cdots$$
$$f_2 = q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + q^{10} + \cdots$$

An example to the theorem

Let $N = 30$. Then, $g(\Gamma_0(30)) = 3$. Using SAGE we find the following base of $S_2(\Gamma_0(30))$:

$$f_0 = q - q^4 - q^6 - 2q^7 + q^9 + q^{10} + \cdots$$
$$f_1 = q^2 - q^4 - q^6 - q^8 + q^{10} + \cdots$$
$$f_2 = q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + q^{10} + \cdots$$

We let $f = f_1$ and $g = f_2$. Now, we have that

$$f^2 = q^4 - 2q^6 - q^8 + 5q^{12} + \cdots$$
$$fg = q^5 + q^6 - 2q^7 - 2q^8 - 2q^9 - 2q^{10} + 2q^{11} + 3q^{12} \cdots$$

are elements of $S_4(\Gamma_0(30))$. By listing the basis of $S_4(\Gamma_0(30))$ using SAGE, we construct a new base as follows: $F = F_0 = f^2$, $G = F_1 = fg$, $F_i = q^{i-1} + \ldots$, $2 \leq i \leq 4$, $F_i = q^{i+1} + \ldots$, $5 \leq i \leq 14$.

An example to the theorem

An example to the theorem

Applying the Trial method (from our Ramanujan paper), we may let $h = F_3 \in \mathcal{U}_m$. The corresponding polynomial $Q_{f^2,fg,h}(\lambda, T)$ is given by

$$225\lambda^6\left(1-\lambda-\lambda^2+\lambda^3\right)T^2-\lambda^3\big(237-370\lambda+319\lambda^2+341\lambda^3$$
$$-310\lambda^4-101\lambda^5+400\lambda^6-10\lambda^7-64\lambda^8+32\lambda^9\big)T+12-44\lambda-85\lambda^2$$
$$+153\lambda^3+1073\lambda^4+1375\lambda^5-420\lambda^6-660\lambda^7-30\lambda^8+162\lambda^9-26\lambda^{10}$$
$$-118\lambda^{11}+84\lambda^{12}+20\lambda^{13}+12\lambda^{14}-4\lambda^{15}$$

Applying the Trial method (from our Ramanujan paper), we may let $h = F_3 \in \mathcal{U}_m$. The corresponding polynomial $Q_{f^2, fg, h}(\lambda, T)$ is given by

$$225\lambda^6 \left(1-\lambda-\lambda^2+\lambda^3\right) T^2 - \lambda^3\big(237 - 370\lambda + 319\lambda^2 + 341\lambda^3 - 310\lambda^4 - 101\lambda^5 + 400\lambda^6 - 10\lambda^7 - 64\lambda^8 + 32\lambda^9\big)\, T + 12 - 44\lambda - 85\lambda^2 + 153\lambda^3 + 1073\lambda^4 + 1375\lambda^5 - 420\lambda^6 - 660\lambda^7 - 30\lambda^8 + 162\lambda^9 - 26\lambda^{10} - 118\lambda^{11} + 84\lambda^{12} + 20\lambda^{13} + 12\lambda^{14} - 4\lambda^{15}$$

observe that we have obtained a quadratic polynomial in T as it should be

An example to the theorem

We easily see that $\widetilde{Q}_{f^2,fg,h}(\lambda, T)$ is given by

$$T^2 - \lambda^3\big(237 - 370\lambda + 319\lambda^2 + 341\lambda^3 - 310\lambda^4 - 101\lambda^5 + 400\lambda^6 - 10\lambda^7$$
$$- 64\lambda^8 + 32\lambda^9\big)\,T + 225\lambda^6\left(1 - \lambda - \lambda^2 + \lambda^3\right)\cdot\big(12 - 44\lambda - 85\lambda^2$$
$$+ 153\lambda^3 + 1073\lambda^4 + 1375\lambda^5 - 420\lambda^6 - 660\lambda^7 - 30\lambda^8 + 162\lambda^9 - 26\lambda^{10}$$
$$- 118\lambda^{11} + 84\lambda^{12} + 20\lambda^{13} + 12\lambda^{14} - 4\lambda^{15}\big).$$

An example to the theorem

We easily see that $\widetilde{Q}_{f^2,fg,h}(\lambda, T)$ is given by

$$T^2 - \lambda^3(237 - 370\lambda + 319\lambda^2 + 341\lambda^3 - 310\lambda^4 - 101\lambda^5 + 400\lambda^6 - 10\lambda^7$$
$$- 64\lambda^8 + 32\lambda^9)\, T + 225\lambda^6\left(1 - \lambda - \lambda^2 + \lambda^3\right) \cdot \left(12 - 44\lambda - 85\lambda^2\right.$$
$$+ 153\lambda^3 + 1073\lambda^4 + 1375\lambda^5 - 420\lambda^6 - 660\lambda^7 - 30\lambda^8 + 162\lambda^9 - 26\lambda^{10}$$
$$\left.- 118\lambda^{11} + 84\lambda^{12} + 20\lambda^{13} + 12\lambda^{14} - 4\lambda^{15}\right).$$

We let $\lambda \in \mathbb{Z} - A_{f^2,fg,h}$ and reduce that polynomial (mod 5) $\Longrightarrow$ $T^2 - \lambda^3(2 - \lambda^2 + \lambda^3 - \lambda^5 + \lambda^8 + 2\lambda^9)\, T$. Letting $\lambda \equiv 1 \pmod 5$ we obtain $T^2 - T = T(T-1)$. Considering $G_{f^2,fg,h,\lambda}$ as a subgroup of the symmetric group $S(2)$, we see that it contains a transposition. Hence, $G_{f^2,fg,H,\lambda} = S(2)$. This recovers the Galois group by using Hilbert's irreducibility.

Thank you!