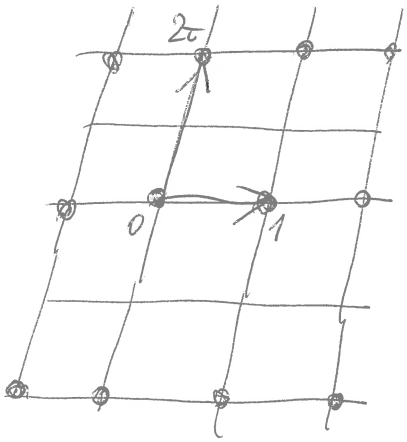
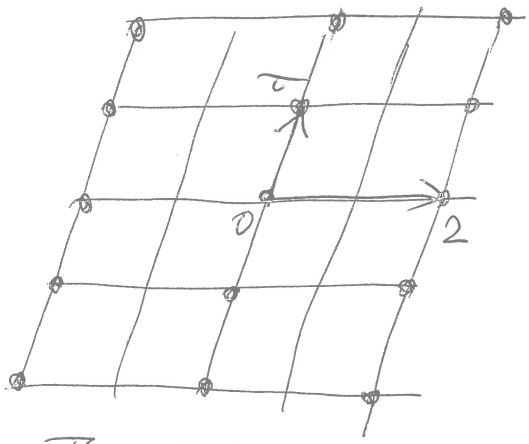
Modular curves $Y_0(N)$, modular polynomials $\Phi_N(X,Y)$

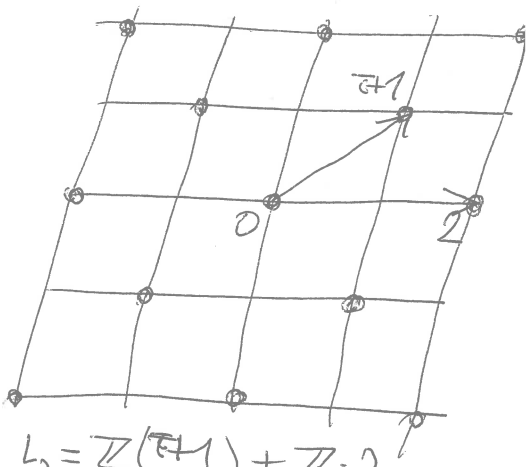
Ex: $L=\mathbb{Z}\tau+\mathbb{Z}$ has 3 sublattices of index 2



$L_0=\mathbb{Z}(2\tau)+\mathbb{Z}\cdot 1$



$L_1=\underbrace{\mathbb{Z}\tau+\mathbb{Z}\cdot 2}_{2\left(\mathbb{Z}\frac{\tau}{2}+\mathbb{Z}\right)}$



$L_2=\underbrace{\mathbb{Z}(\tau+1)+\mathbb{Z}\cdot 2}_{2\left(\mathbb{Z}\frac{\tau+1}{2}+\mathbb{Z}\right)}$

the set $\{j(L_0),\ j(L_1),\ j(L_2)\}=\{j(2\tau),\ j(\frac{\tau}{2}),\ j(\frac{\tau+1}{2})\}$

depends only on $j(L)=j(\tau)$

$\Rightarrow$ the coefficients of the polynomial

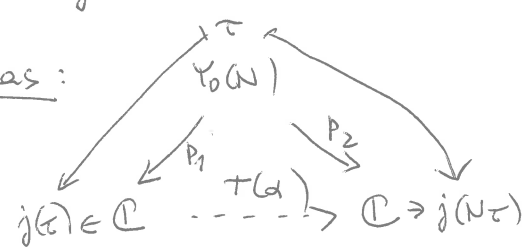
$(X-j(2\tau))(X-j(\frac{\tau}{2}))(X-j(\frac{\tau+1}{2}))$ depend only on $j(\tau)$.

Abstract version: $\Gamma=\Gamma(1)=\Gamma_0(1)=SL_2(\mathbb{Z})$, $\alpha=\begin{pmatrix}N&0\\0&1\end{pmatrix}$, $\alpha^{-1}\Gamma\alpha\cap\Gamma=\Gamma_0(N)$

the Hecke correspondence defined by $\alpha(\tau)=N\tau$ is

$$\begin{array}{ccccc}
\Gamma_0(N)\tau\in Y_0(N)=(\alpha^{-1}\Gamma\alpha\cap\Gamma)\backslash\mathcal{H} & \xrightarrow{\alpha} & (\Gamma\cap\alpha\Gamma\alpha^{-1})\backslash\mathcal{H}=Y^0(N) & & \\
\downarrow p & \searrow^{p'\circ\alpha} & \downarrow p' & & \\
Y_0(1)= \Gamma\backslash\mathcal{H} & \xrightarrow{T(\alpha)} & \Gamma\backslash\mathcal{H} & = Y_0(1) & \\
j\downarrow 2 & & j\downarrow 2 & & \\
j(\tau)\in\mathbb{C} & & \mathbb{C}\ni j(N\tau) & &
\end{array}$$

Formulas:



$\deg(p_1)=\deg(p_2)=(\Gamma:\overline{\Gamma_0(N)})=N\prod_{p\mid N}(1+\frac{1}{p})$

$\Gamma\begin{pmatrix}N&0\\0&1\end{pmatrix}\Gamma=\coprod\Gamma\beta$

$\{\beta\}=\left\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\middle|\ \begin{array}{l}a,d\geq 1,\ (a,b,d)=1\\ ad=N,\ b\in\mathbb{Z}/d\mathbb{Z}\end{array}\right\}$

$p_2(p_1^{-1}(j(\tau)))=\{j(\frac{a\tau+b}{d})\}=\{j\circ\beta\}$

q-expansion principle for the j-line: $j(\tau) = q^{-1} + \sum_{n\geq 0} c_n q^n$, $c_n \in \mathbb{Z}$

$\mathcal{M}(X_0(1)) = \mathbb{C}(j)$, $\quad \mathcal{M}(X_0(1)) \cap \mathcal{O}(Y_0(1)) = \mathbb{C}[j]$

Prop. If $f = \sum_{n\geq -M} a_n q^n \in$ $\Big)$ then $f = P(j)$, where

P = polynomial whose coefficients are $\mathbb{Z}$-linear combinations of $\{a_n\}$

Pf: $f = a_{-M} j^M + g$, $g = \sum_{n\geq -M+1} b_n q^n$; apply induction.

Polynomial relations between j and $j\circ\beta$ $\quad (\beta \in GL_2(\mathbb{Q})^+)$

the function $(j\circ\beta)(\tau) = j(\beta(\tau)) = j\left(\frac{a\tau+b}{c\tau+d}\right)$ depends only on the class of $\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})\backslash GL_2(\mathbb{Q})^+ / \mathbb{Q}^\times \cdot I =$

$$= \coprod_{m\geq 1} \underbrace{SL_2(\mathbb{Z})}_{\Gamma} \backslash M(m)_{prim}, \qquad M(m)_{prim} = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_2(\mathbb{Z}) \;\middle|\; \begin{array}{l} \det = m \\ (A,B,C,D) = 1 \end{array} \right\}$$

$$SL_2(\mathbb{Z}) \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; \begin{array}{l} a,d \geq 1,\ ad = m \\ (a,b,d) = 1,\ b \in \mathbb{Z}/d\mathbb{Z} \end{array} \right\}$$

Thm. Let $m \geq 1$. (1) $\exists!\ \Phi_m(X,Y) \in \mathbb{Z}[X,Y]$ such that

$\forall \tau \in \mathcal{H} \qquad \prod_{\beta \in \Gamma\backslash M(m)_{prim}} (X - j\circ\beta(\tau)) = \Phi_m(X, j(\tau))$.

(2) $\Phi_1(X,Y) = X - Y$; $\quad \deg_X \Phi_m(X,Y) = m \prod_{p\mid m} (1 + \frac{1}{p}) = \deg_Y \Phi_m(X,Y)$.

(3) $\Phi_m(X,Y)$ is irreducible in $\mathbb{C}(Y)[X]$.

(4) $\Phi_m(X,Y) = \Phi_m(Y,X)$ if $m > 1$.

(5) If $m \neq n^2$, then $F_m(X) := \Phi_m(X,X)$ has $\deg(F_m) > 1$ and leading coefficient ± 1.

Previous discussion: (P_1, P_2):

$$\begin{array}{ccc} Y_0(N) & \longrightarrow & \{(X,X) \in \mathbb{C}^2 \mid \Phi_N(X,Y) = 0\} \\ \Gamma_0(N)\tau & \longmapsto & (j(\tau), j(N\tau)) \end{array}$$

is surjective, and injective on a complement of finitely many points. In other words, $Y_0(N)$ is a desingularisation of the affine plane curve $\{\Phi_N = 0\}$.

Pf of thm. (1) $\left(j\circ\begin{pmatrix}a&b\\0&d\end{pmatrix}\right)(\tau) = \frac{1}{q^{a/d}\zeta_d^b} + \left(\begin{array}{c}\text{power series in } (q^{a/d}\zeta_d^b) \text{ with}\\ \text{coefficients in } \mathbb{Z}\end{array}\right)$

$ad=m$, $\zeta_d = e^{2\pi i/d}$

$\Rightarrow$ the coefficients of the Fourier expansion in $q^{1/m}$ of each coefficient of $\prod_\beta (X-(j\circ\beta)(\tau))$ lie in $\mathbb{Z}[\zeta_m]$, and are permuted by the action of $\sigma_k \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, $\sigma_k:\zeta_m\longmapsto\zeta_m^k$ (corresponds to $b \pmod d \longmapsto kb \pmod d$) $\Longrightarrow$ q-expansion principle proves (1)

(2) $\deg_X \Phi_m = |\{\beta\gamma\}| = (\Gamma : \Gamma_0(m))$

$\deg_Y \Phi_m = \sum_{\substack{ad=m\\(a,b,d)=1\\b\in\mathbb{Z}/d\mathbb{Z}}} \frac{a}{d} = (-\!\!''\!\!-)$.

(3) Field extensions $\quad M(X_0(1)) \hookrightarrow M(X_0(m)) \hookrightarrow M(X(m))$

G_m = Galois group $SL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm I\}$

G_m acts transitively (on the right) on $\Gamma\backslash M(m)_{prim}$, since $M(m)_{prim} = \Gamma\begin{pmatrix}m&0\\0&1\end{pmatrix}\Gamma$ and $\Gamma\longrightarrow G_m$ is surjective.

(4) Recall $\Phi_m(j(\frac{\tau}{m}), j(\tau)) = 0 \overset{\forall\tau}{\Longrightarrow} \Phi_m(j(\tau), j(m\tau)) = 0$.

But $\forall\tau\in\mathcal{H}$ $\Phi_m(j(m\tau), j(\tau)) = 0 \overset{(3)}{\Longrightarrow} \Phi_m(X,Y) \mid \Phi_m(Y,X)$ in $\mathbb{C}(Y)[X]$

$\overset{(2)}{\Longrightarrow} \Phi_m(X,Y)\cdot(\text{const}) = \Phi_m(Y,X)$, $(\text{const.}) = \pm 1$.

As $m>1$, $j(\tau)$ is not a root of $\Phi_m(X,j) \Longrightarrow (\text{const.}) \neq -1$.

(5) If $m\neq n^2$, then $a\neq d$ and there is no cancellation of the poles in $j(\tau) - (j\circ\begin{pmatrix}a&b\\0&d\end{pmatrix})(\tau) = \frac{1}{q} + \cdots - \frac{1}{q^{a/d}\zeta_d^b} + \cdots$

q-expansion $\Longrightarrow$ the leading coefficient lies in $\mathbb{Z}\cap\{\text{roots of unity}\} = \{\pm 1\}$.

Cor. $\forall\,\beta\in GL_2(\mathbb{Q})^+$ $\quad j\circ\beta$ is integral over j.

Kronecker's congruence. $\forall$ prime p $\quad \boxed{\Phi_p(X,Y) \equiv (X-Y^p)(X^p-Y) \pmod p}$.

Pf. $\{\beta\} = \left\{ \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \quad b \in \mathbb{Z}/p\mathbb{Z} \right\}$

the following congruences hold in $\mathbb{Z}[\zeta_p]((q^{1/p}))$:

$$j\circ p = j(p\tau) = \sum c_n q^{pn} \equiv \left(\sum c_n q^n\right)^p = j^p \pmod p$$

$$j\circ\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} = j\left(\frac{\tau+b}{p}\right) = \sum c_n (q^{1/p})^n \zeta_p^{bn} \equiv \sum c_n (q^{1/p})^n \pmod{(1-\zeta_p)}$$

$$\Rightarrow \Phi_p(X,j) \equiv (X-j^p)\underbrace{\left(X - \sum c_n (q^{1/p})^n\right)^p}_{\equiv X^p - j} \pmod{(1-\zeta_p)}$$

$\Phi_p(X,j) \in \mathbb{Z}[X,j]$

q-expansion principle $\Rightarrow$ $\Phi_p(X,Y) \equiv (X-Y^p)(X^p-Y) \pmod{(1-\zeta_p)\mathbb{Z}[X,Y]}$

$\Rightarrow$ idem mod $p\,\mathbb{Z}[X,Y]$

Exercise. If $p \nmid m$ (p prime), then $\Phi_{pm}(X,Y) \equiv \Phi_m(X,Y^p)\,\Phi_m(X^p,Y) \pmod p$

"Eichler – Shimura congruence"

Relation to supersingular elliptic curves

Recall: an elliptic curve E over a field k of $\mathrm{char}(k) = p \neq 0$ is **supersingular** (SS) if $E[F] = [p] = 0$.

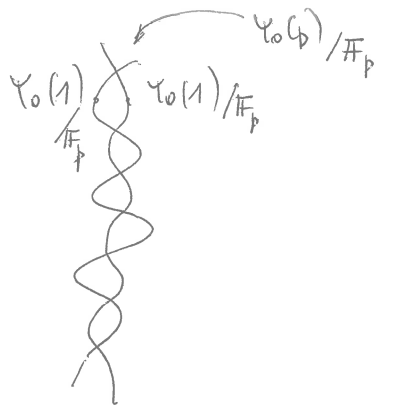
Numerology: $\quad \left|\{\text{SS elliptic curves over } \overline{\mathbb{F}_p}\}/\text{Isom}\right| = \underbrace{1 + \dim S_2(\Gamma_0(p))}_{\dim M_2(\Gamma_0(p))}$

$= 1 + \text{genus}(X_0(p))$

Explanation: "$Y_0(p)$ over $\mathbb{F}_p$" is, essentially, given by the equation

$$\Phi_p(X,Y) \equiv 0 \pmod p \iff \underbrace{(X-Y^p)(X^p-Y) \equiv 0 \pmod p}$$

two affine lines over $\mathbb{F}_p$ glued together via the Frobenius map (the intersection points are the SS j-invariants)



Complex multiplication

Φ_m and isogenies: if $L \subset \mathbb{C}$ is a lattice and $L' \subset L$ a primitive sublattice of index m, then $\lambda : \mathbb{C}/L' \xrightarrow{pr} \mathbb{C}/L$ is an isogeny with $\ker(\lambda) = L/L' \simeq \mathbb{Z}/m\mathbb{Z}$.

Cor. $\{ (j(L), j(L')) \mid \mathbb{C}/L' \xrightarrow{\lambda} \mathbb{C}/L$ isogeny, $\ker(\lambda) \simeq \mathbb{Z}/m\mathbb{Z} \}$

$= \{ (Y, X) \in \mathbb{C}^2 \mid \Phi_m(X, Y) = 0 \}$

Recall: $\mathrm{End}(\mathbb{C}/L) = \{$holomorphic maps $\lambda : \mathbb{C}/L \to \mathbb{C}/L$, $\lambda(0) = 0\}$

$= \{ z \mapsto \alpha z \mid \alpha \in \mathbb{C}, \alpha L \subset L \}$

Prop. $(\tau \in \mathbb{C} \setminus \mathbb{R})$

$$\mathrm{End}(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})) = \begin{cases} \mathbb{Z} & \text{if } A\tau^2 + B\tau + C \neq 0 \text{ if } A, B, C \in \mathbb{Z},\ A \neq 0 \\ \mathbb{Z}A\tau + \mathbb{Z} & \text{if } A\tau^2 + B\tau + C = 0,\ A, B, C \in \mathbb{Z} \\ & (A, B, C) = 1 \end{cases}$$

$\left((A\tau)^2 + B(A\tau) + AC = 0 \right)$

Pf. Exercise.

Above: $D = B^2 - 4AC < 0$, $D \equiv 0, 1 \pmod 4$

$\mathcal{O} = \mathbb{Z}A\tau + \mathbb{Z} = \mathbb{Z}\left[\frac{D + \sqrt{D}}{2}\right] = \mathbb{Z}\frac{D+\sqrt{D}}{2} + \mathbb{Z}$ the quadratic ring of discriminant D $\left(\mathcal{O} = \mathcal{O}_D = \right.$

$K = \mathbb{Q}(\sqrt{D})$ imaginary quadratic field, discriminant d_K,

$D = d_K f^2$, $f \geq 1$ the conductor of $\mathcal{O} = \mathcal{O}_D$

$\mathcal{O} = \mathcal{O}_D = \mathbb{Z} + f\mathcal{O}_K$ ($\mathcal{O}_K$ = the ring of integers of K)

Prop. $\exists$ bijection $\quad L \longleftrightarrow I$

$$\mathbb{C}^\times \backslash \{ L \subset \mathbb{C} \text{ lattice} \mid \mathrm{End}(\mathbb{C}/L) = \mathcal{O}_D \} \longleftrightarrow K^\times \backslash \{ \underbrace{\text{invertible fractional } \mathcal{O}_D\text{-ideals}}_{I \subset K} \}$$

$\mathrm{Pic}(\mathcal{O}_D)$ (finite) abelian group

Pf. Exercise.

Rmks. (1) $D = d_K \iff \mathcal{O}_D = \mathcal{O}_K \iff \mathcal{O}_D$ is a Dedekind ring

(2) Exact sequence

$$\frac{\mathcal{O}_K^\times}{\mathbb{Z}^\times} \longrightarrow \frac{(\mathcal{O}_K/f\mathcal{O}_K)^\times}{(\mathbb{Z}/f\mathbb{Z})^\times} \longrightarrow \mathrm{Pic}(\mathcal{O}_D) \longrightarrow \underbrace{\mathrm{Pic}(\mathcal{O}_K)}_{cl_K} \longrightarrow 1$$

Terminology: $L \subset \mathbb{C}$ lattice (resp. $\mathbb{C}/L$) has **complex multiplication** if $\mathrm{End}(\mathbb{C}/L) \neq \mathbb{Z}$. As above, $\mathrm{End}(\mathbb{C}/L) = \mathcal{O}_D$, $D = d_K f^2$, $K = \mathbb{Q}(\sqrt{D})$ imaginary quadratic field, $L = \alpha(\mathbb{Z}\tau + \mathbb{Z})$ for some $\alpha \in \mathbb{C}^\times$ and $\tau \in K \cap \mathfrak{H}$.

Prop. $L \subset \mathbb{C}$ has complex multiplication

$\Updownarrow$

$\exists\ m \neq n^2 \quad \Phi_m(j(L), j(L)) = 0.$ ($\Rightarrow j(L)$ is an algebraic integer)

Pf. If L has complex multiplication, $\mathrm{End}(\mathbb{C}/L) = \mathcal{O} \neq \mathbb{Z}$, $L = \alpha I$, $\alpha \in \mathbb{C}^\times$, $I \subset \mathcal{O}$ invertible ideal. there exists $\beta \in \mathcal{O}$ primitive such that $m = N_{K/\mathbb{Q}}(\beta) \neq n^2 \Rightarrow \beta I \subset I$ primitive sublattice of index $m \Rightarrow \Phi_m(\underbrace{j(\beta L)}_{j(L)}, j(L)) = 0$

Converse: if $m \neq n^2$, $\Phi_m(j(L), j(L)) = 0 \Rightarrow \exists$ isogeny $\mathbb{C}/L \xrightarrow{\lambda} \mathbb{C}/L$ with $\ker(\lambda) \simeq \mathbb{Z}/m\mathbb{Z} \Rightarrow \mathrm{End}(\mathbb{C}/L) \neq \mathbb{Z}$.

Fact. $\forall m > 1 \quad \Phi_m(X, X) = (\text{const}) \prod_{D<0} \prod_{I \in \mathrm{Pic}(\mathcal{O}_D)} (X - j(I))^{r(\mathcal{O}_D, m)}$

$r(\mathcal{O}_D, m) = \left| \{ \alpha \in \mathcal{O}_D \mid \alpha \text{ primitive}, N_{K/\mathbb{Q}}(\alpha) = m \} / \mathcal{O}_D^\times \right|$

Cor. $\forall m > 1 \quad \deg \Phi_m(X, X) = \sum_{D<0} r(\mathcal{O}_D, m) \, |\mathrm{Pic}(\mathcal{O}_D)|$

Ring class fields of K

K = imaginary quadratic field, $\mathcal{O}_K \subset K$ ring of integers
d_K = discriminant

Thm. If $D = d_K f^2$, $\mathcal{O}_D = \mathbb{Z} + f\mathcal{O}_K$ $(f \geq 1)$, $I \subset K$ invertible fractional $\mathcal{O}_D$-ideal, p prime such that $(p, f) = 1$ and p splits in $K/\mathbb{Q}$ $(\Leftrightarrow p\mathcal{O}_D = \mathfrak{P}\overline{\mathfrak{P}}$, $\mathfrak{P}, \overline{\mathfrak{P}} \subset I$ invertible ideals)

then: $j(I)^p \equiv j(\overline{\mathfrak{P}} I) \pmod{\mathfrak{P}\mathcal{O}_L}$, for any number field $L \supset K(j(I), j(\overline{\mathfrak{P}} I))$

Rmk: Kronecker's congruence $\Rightarrow$ $j(\mathfrak{P}I)$, $j(\overline{\mathfrak{P}}I)$ are roots of $\Phi_p(X, j(I))$ and $\Phi_p(X, j(I)) \equiv (X^p - j(I))(X - j(I)^p) \pmod{p\mathcal{O}_L}$

Class field theory $\Rightarrow$ $K(j(I))/K$ is a Galois extension with abelian Galois group and the Artin map

$$\left(\frac{K(j(I))/K}{\cdot}\right) : \mathrm{Pic}(\mathcal{O}_D) \xrightarrow{\sim} \mathrm{Gal}(K(j(I))/K)$$

is an isomorphism $\quad [I] \longmapsto \left(j(I) \longmapsto j(I^{-1}I)\right)$

---

the extension $K(j(I))/K$ depends only on $\mathcal{O} = \mathrm{End}(\mathbb{C}/I)$; it is called the **ring class field of $\mathcal{O}$**, denoted by $K[\mathcal{O}]$

The complex conjugation c sends $\mathfrak{P}$ to $\overline{\mathfrak{P}}$ and

$$[\mathfrak{P}\overline{\mathfrak{P}}] = [1] \in \mathrm{Pic}(\mathcal{O}_D)$$

$\Rightarrow$ $\mathbb{Q} \subset K \underbrace{\subset K[\mathcal{O}]}_{\mathrm{Pic}(\mathcal{O}_D)}$ Galois extension

$\mathrm{Gal}(K[\mathcal{O}]/\mathbb{Q}) = \mathrm{Pic}(\mathcal{O}_D) \rtimes \langle 1, c \rangle$, $\quad c[I]c^{-1} = [I^{-1}]$

generalised dihedral group

$J_0(N) = J(X_0(N))$

We know: $\Omega^1(X_0(N)) \left(\simeq S_2(\Gamma_0(N))\right) = \bigoplus \mathbb{C}\cdot\omega_f$

$i\infty \in X_0(N)$ base point $\qquad \bigoplus \mathbb{C}\cdot f(\tau) \qquad \omega_f = (2\pi i) f(\tau) d\tau$

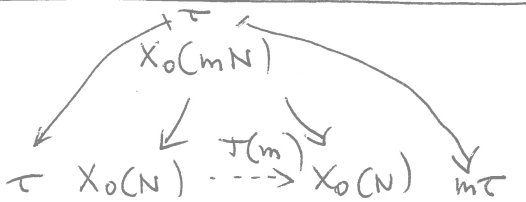
Abel–Jacobi map: $\tau \longmapsto \left\{\left(\int_{i\infty}^{\tau} \omega_f\right)_f\right\} /$ periods

$\left\{ \left(\int_\gamma \omega_f \right),\ \gamma \in H_1(X_0(N), \mathbb{Z}) \right\}$

Decompositions according to Hecke operators

Atkin–Lehner: $S_2(\Gamma_0(N)) = \bigoplus_{M|N} \bigoplus_{d|\frac{N}{M}} S_2(\Gamma_0(M))_{new} \Big|_2 \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$

Easy part of the Hecke algebra: $\mathbb{T}^{(N)} = \mathbb{Z}\left[\{T(m)\} \mid (m,N)=1\right]$



acts on $H_1(X_0(N), \mathbb{Z})$

$\Omega^1(X_0(N)) \simeq S_2(\Gamma_0(N))$

covariant action = contravariant action

$T(m)\,T(m') = T(m')\,T(m)$ (false for $X_1(N)$)

action on $\Omega^1(X_0(N))$: hermitian $\Rightarrow$ simultaneously diagonalisable

rational structure $H_1(X_0(N), \mathbb{Q})$ of $\Omega^1(X_0(N))^*$ is $\mathbb{T}^{(N)}$-stable

Decompositions: $\mathbb{T}^{(N)}_{\mathbb{Q},new} = \prod K_\alpha \qquad [K_\alpha : \mathbb{Q}] < \infty$

$T(m) \longleftrightarrow (T(m)_\alpha)$ $\qquad K_\alpha$ totally real

$(m,N)=1$

$\forall\, \sigma : K_\alpha \hookrightarrow \mathbb{R} \qquad \exists!$ normalised eigenform ${}^\sigma f_\alpha \in S_2(\Gamma_0(N))_{new}$

$\forall (m,N)=1 \qquad T(m)\,{}^\sigma f_\alpha = \sigma(T(m)_\alpha)\,{}^\sigma f_\alpha$

$$S_2(\Gamma_0(N))_{new} = \bigoplus_\alpha \bigoplus_{\sigma : K_\alpha \hookrightarrow \mathbb{R}} \mathbb{C}\cdot {}^\sigma f_\alpha \qquad (V_\alpha)$$

$$H_1(X_0(N), \mathbb{Q})_{new} = \bigoplus_\alpha H_\alpha$$

$\dim_{\mathbb{Q}} = 2[K_\alpha : \mathbb{Q}]$

Galois orbits of Hecke eigenvalues

$\Rightarrow \quad \Omega^1(X_0(N)) = \bigoplus_\beta V_\beta^{m_\beta}$

$H_1(X_0(N), \mathbb{Q}) = \bigoplus_\beta H_\beta^{m_\beta}$

$m_\beta = 1$ on the new part

$m_\beta = \sigma_1(N/M)$ on $\bigoplus_d S_2(\Gamma_0(M))_{new} \Big|_2 \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow \quad J(X_0(N)) \xrightarrow[\text{Ker}]{\text{finite}} \bigoplus_\beta \left(\underbrace{(V_\beta^*)^{\mathbb{R}}}_{\mathbb{C}^{d_\beta}} / H_{\beta,\mathbb{Z}} \right)^{m_\beta}$ (*)

$H_{\beta,\mathbb{Z}}$: lattice

$d_\beta = [K_\beta : \mathbb{Q}]$ ← totally real

abelian variety with real multiplication by $\mathcal{O}_{K_\beta}$.

Modularity of elliptic curves over $\mathbb{Q}$:

E elliptic curve over $\mathbb{Q}$

$N =$ conductor of E

$\Downarrow$

$E(\mathbb{C})$ occurs in the decomposition (*)

Abel–Jacobi map : (base point $i\infty$)

$$\begin{array}{ccccc} X_0(N) & \xrightarrow{\quad} & J(X_0(N)) & \xrightarrow{\quad} & E(\mathbb{C}) = \mathbb{C}/L \\ \Psi & & \Psi & & \\ \tau & \longmapsto & \left(\omega \longmapsto \int_{i\infty}^{\tau} \omega \ (\text{mod periods})\right) & & \end{array}$$

α

$\alpha^*(dz) = c \cdot (2\pi i) f(\tau) d\tau$ (ω_f)

$f(\tau) \in S_2(\Gamma_0(N))$

$\forall \gamma \in \Gamma_0(N)$

$$\left\{ c \int_{\tau_0}^{\gamma(\tau_0)} \omega_f \;\middle|\; \gamma \in \Gamma_0(N) \right\} \subset L$$ sublattice

---

Fact : if α exists over $\mathbb{C}$ $\Rightarrow$ it exists over $\mathbb{Q}$.

Cor. If $E_1 \xrightarrow{\lambda} E_2$ is an isogeny of elliptic curves with $\text{End}(E_1) = \mathcal{O}_{D_1}$, $\text{End}(E_2) = \mathcal{O}_{D_2}$, $D_j = d_K f_j^2$, $\mathbb{Q}(\sqrt{D_1}) = K = \mathbb{Q}(\sqrt{D_2})$

and $\text{Ker}(\lambda) = \mathbb{Z}/N\mathbb{Z}$

$\Downarrow$

CM point $(j(E_1), j(E_2)) \in Y_0(N)$ (ring class field of $\mathcal{O}$)

$\mathcal{O} := \mathcal{O}_{d_K \text{lcm}(f_1, f_2)^2}$

$\downarrow \alpha$ $\qquad$ $\downarrow$

CM pt $\in E(K_{\mathcal{O}})$

Ex. $N = 37$ $\qquad g(X_0(37)) = 2$

$X_0(37)$ is hyperelliptic, but its hyperelliptic involution $\neq$ the Fricke involution W_{37}.

$J_0(37) \longrightarrow E_1 \times E_2$ elliptic curves

$\ker($ — " — $) \simeq \mathbb{Z}/2\mathbb{Z}$

$S_2(\Gamma_0(37)) = \mathbb{C}f_1 \oplus \mathbb{C}f_2$ $\qquad f_j(\tau) = \sum_{n \geq 1} a_j(n) q^n$ $\quad q = e^{2\pi i \tau}$