Explicit Arithmetic of Modular Curves
Lecture IV: Equations for Modular Curves

Samir Siksek (Warwick/IHÉS/IHP)

20 June 2019

Canonical Map

K	field
X	curve of genus $g \geq 2$
$\Omega(X)$	space of regular differentials on X/K
	this is a K-vector space of dimension g.

Let $\omega_1, \dots, \omega_g$ be a K-basis for $\Omega(X)$.

The **canonical map** is the map

$$\phi : X \to \mathbb{P}^{g-1}, \qquad P \mapsto (\omega_1(P) : \cdots : \omega_g(P)).$$

What does this mean? Let $f \in K(X) \setminus K$. Then every differential ω can be written as $\omega = hdf$ where $h \in K(X)$. So I can write $\omega_i = h_i df$, and then

$$\phi(P) = (h_1(P) : \cdots : h_g(P)).$$

Canonical Map for Genus 2 Curves

Consider a genus 2 curve

$$X \;:\; y^2 = a_6 x^6 + \cdots + a_0, \qquad a_i \in K, \qquad \Delta(f) \neq 0.$$

A basis for $\Omega(X)$ is

$$\omega_1 = \frac{dx}{y}, \qquad \omega_2 = \frac{xdx}{y}.$$

Note that $\omega_2/\omega_1 = x$. Thus

$$\phi : X \to \mathbb{P}^1, \qquad P \mapsto (1 : x(P)).$$

Thus $\phi(X) = \mathbb{P}^1$.

$\therefore$ ϕ is **not** an isomorphism but is 2 to 1.

Canonical Map for Genus 3 Hyperelliptic

$$X \ : \ y^2 = a_8 x^8 + \cdots + a_0, \qquad a_i \in K, \qquad \Delta(f) \neq 0.$$

A basis for $\Omega(X)$ is

$$\omega_1 = \frac{dx}{y}, \qquad \omega_2 = \frac{xdx}{y}, \qquad \omega_3 = \frac{x^2 dx}{y}.$$

$$\phi : X \to \mathbb{P}^2, \qquad \phi(x,y) = (1 : x : x^2).$$

If we choose coordinates $(u_1 : u_2 : u_3)$ for $\mathbb{P}^2$ then the image is the conic

$$\phi(X) = C \ : \ u_1 u_3 = u_2^2 \quad \subset \quad \mathbb{P}^2.$$

$\therefore \quad \phi : X \to \phi(X)$ is **not** an isomorphism but it is 2 to 1.

General Hyperelliptic

A hyperelliptic curve of genus g can be written as

$$X \ : \ y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0, \qquad a_i \in K, \qquad \Delta(f) \neq 0.$$

A basis for $\Omega(X)$ is

$$\frac{dx}{y}, \ \frac{xdx}{y}, \ldots, \ \frac{x^{g-1}dx}{y}.$$

Check that $\phi : X \to \phi(X) \cong \mathbb{P}^1$ is 2 to 1.

Theorem

Let X be a curve of genus ≥ 2.

- *If X is hyperelliptic then $\phi(X) \cong \mathbb{P}^1$ and the canonical map $\phi : X \to \phi(X)$ is 2 to 1.*
- *If X is non-hyperelliptic then $\phi : X \to \mathbb{P}^{g-1}$ is an embedding (so X is isomorphic to $\phi(X)$). Moreover $\phi(X)$ is a curve of degree $2g-2$.*

We focus on those modular curves whose genus is ≥ 2.

Recall the isomorphism

$$S_2(\Gamma_H) \cong \Omega(X_H), \qquad f(q) \mapsto f(q)\frac{dq}{q}.$$

Let $f_1, \ldots, f_g$ be a basis for $S_2(\Gamma_H)$.

The canonical map is given by

$$\phi : X_H \to \mathbb{P}^{g-1}$$

$$\phi = (f_1(q)\frac{dq}{q} : \cdots : f_g(q)\frac{dq}{q}) = (f_1(q) : \cdots : f_g(q)).$$

Example $X_0(30)$

A basis for $S_2(\Gamma_0(30))$ is

$$f_1 = q - q^4 - q^6 - 2q^7 + q^9 + O(q^{10}),$$
$$f_2 = q^2 - q^4 - q^6 - q^8 + O(q^{10}),$$
$$f_3 = q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + O(q^{10}).$$

$\therefore\ X = X_0(30)$ has genus 3.

By theorem,

- either X is hyperelliptic;
- or $X \cong \phi(X)$ is a curve in $\mathbb{P}^{g-1} = \mathbb{P}^2$ which has degree $2g - 2 = 4$; i.e. $\phi(X)$ is a plane quartic curve.

Which is it?

If X is hyperelliptic then $\phi(X)$ is a conic.

(Note in this case that $f_1(q)dq/q, \ldots, f_3(q)dq/q$ and dx/y, xdx/y, x^2dx/y don't have to be the same basis for $\Omega(X)$. The two bases are related by a linear transformation. So $\phi(X)$ might be a different conic than before.)

$\phi(X) =$ conic iff $\exists a_1, \ldots, a_6$ (not all zero) such that

$$a_1 f_1^2 + a_2 f_2^2 + a_3 f_3^2 + a_4 f_1 f_2 + a_5 f_1 f_3 + a_6 f_2 f_3 = 0.$$

$$\begin{aligned}
f_1^2 &= q^2 - 2q^5 - 2q^7 - 3q^8 + 4q^{10} + O(q^{11}) \\
f_2^2 &= q^4 - 2q^6 - q^8 + O(q^{12}) \\
f_3^2 &= q^6 + 2q^7 - q^8 - 4q^9 - 5q^{10} - 6q^{11} + q^{12} + O(q^{13}) \\
f_1 f_2 &= q^3 - q^5 - q^6 - q^7 - 3q^9 + 2q^{10} + O(q^{11}) \\
f_1 f_3 &= q^4 + q^5 - q^6 - 2q^7 - 3q^8 - 2q^9 - 2q^{10} + O(q^{11}) \\
f_2 f_3 &= q^5 + q^6 - 2q^7 - 2q^8 - 2q^9 - 2q^{10} + 2q^{11} + O(q^{12}).
\end{aligned}$$

$\phi(X) =$ conic iff $\exists a_1, \ldots, a_6$ (not all zero) such that

$$a_1 f_1^2 + a_2 f_2^2 + a_3 f_3^2 + a_4 f_1 f_2 + a_5 f_1 f_3 + a_6 f_2 f_3 = 0.$$

$$\begin{aligned}
f_1^2 &= q^2 - 2q^5 - 2q^7 - 3q^8 + 4q^{10} + O(q^{11})\\
f_2^2 &= q^4 - 2q^6 - q^8 + O(q^{12})\\
f_3^2 &= q^6 + 2q^7 - q^8 - 4q^9 - 5q^{10} - 6q^{11} + q^{12} + O(q^{13})\\
f_1 f_2 &= q^3 - q^5 - q^6 - q^7 - 3q^9 + 2q^{10} + O(q^{11})\\
f_1 f_3 &= q^4 + q^5 - q^6 - 2q^7 - 3q^8 - 2q^9 - 2q^{10} + O(q^{11})\\
f_2 f_3 &= q^5 + q^6 - 2q^7 - 2q^8 - 2q^9 - 2q^{10} + 2q^{11} + O(q^{12}).
\end{aligned}$$

- Coefficient of $q^2 \implies a_1 = 0$.
- Coefficient of $q^3 \implies a_4 = 0$.
- Coefficient of q^4, q^5, q^6 give

$$a_2 + a_5 = 0, \qquad a_5 + a_6 = 0, \qquad -2a_2 + a_3 - a_5 + a_6 = 0$$

There is only one solution (up to scaling) which is

$$a_2 = 1, \quad a_3 = 0, \quad a_5 = -1, \quad a_6 = 1.$$

$$\therefore \quad f_2^2 - f_1 f_3 + f_2 f_3 = 0 + O(q^7).$$

In fact we can check that

$$f_2^2 - f_1 f_3 + f_2 f_3 = 0 + O(q^{100}).$$

Question. Do we know that $f_2^2 - f_1 f_3 + f_2 f_3 = 0$ exactly? **If so** then the image is the conic

$$u_2^2 - u_1 u_3 + u_2 u_3 = 0 \qquad \subset \mathbb{P}^2,$$

and X is hyperelliptic.

In fact we can check that

$$f_2^2 - f_1 f_3 + f_2 f_3 = 0 + O(q^{100})$$

.

Question. Do we know that $f_2^2 - f_1 f_3 + f_2 f_3 = 0$ exactly? **If so** then the image is the conic

$$u_2^2 - u_1 u_3 + u_2 u_3 = 0 \qquad \subset \mathbb{P}^2,$$

and X is hyperelliptic.

Theorem (Sturm)

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of index m. Let $f \in S_k(\Gamma)$ and suppose $\mathrm{ord}_q(f) > km/12$. Then $f = 0$.

Theorem (Sturm)

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of index m. Let $f \in S_k(\Gamma)$ and suppose $\mathrm{ord}_q(f) > km/12$. Then $f = 0$.

Let $f = f_2^2 - f_1 f_3 + f_2 f_3$.

f_1, f_2, f_3 are cusp forms for $\Gamma_0(30)$ of weight 2.

$\therefore$ f is a cusp form for $\Gamma_0(30)$ of weight $k = 4$.

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p).$$

$$N = 30 \implies m = 30(1 + 1/2)(1 + 1/3)(1 + 1/5) = 72 \implies \frac{km}{12} = 36.$$

Since $\mathrm{ord}_q(f) \geq 100$ we know from Sturm that $f = 0$.

$\therefore$ $X_0(30)$ is hyperelliptic.

$X_0(45)$

Repeat $X_0(45)$. A basis for $S_2(\Gamma_0(45))$ is

$$g_1 = q - q^4 + O(q^{10}),$$
$$g_2 = q^2 - q^5 - 3q^8 + O(q^{10}),$$
$$g_3 = q^3 - q^6 - q^9 + O(q^{10}).$$

$\therefore$ $X_0(45)$ has genus 3. **Is it hyperelliptic?** i.e. **Is the canonical image a conic**? Again we look for $a_1, \ldots, a_6$ such that

$$a_1 g_1^2 + a_2 g_2^2 + a_3 g_3^2 + a_4 g_1 g_2 + a_5 g_1 g_3 + a_6 g_2 g_3 = 0.$$

By solving the resulting system of linear equations from the coefficients of $q^2, \ldots, q^{10}$ we find that all the $a_i = 0$.

$\therefore$ image is not a conic.

$\therefore$ $X_0(45)$ is **not** hyperelliptic, and the image is a plane quartic.

Write down an equation for this plane quartic!

- Look at all 10 monomials of degree 4 in g_1, g_2, g_3.
- Want a linear combination which is 0.
- By solving the system resulting from the coefficients of q^j up to q^{20} we find a unique solution (up to scaling).

This unique solution gives us our degree 4 model:

$$X_0(45) \; : \; x_0^3 x_2 - x_0^2 x_1^2 + x_0 x_1 x_2^2 - x_1^3 x_2 - 5x_2^4 \qquad \subset \mathbb{P}^2.$$

Did we need to check up to the Sturm bound? Not this time!

- Already proved that $X_0(45)$ is not hyperelliptic.
- So we know that the canonical image is a quartic.
- We solved for this quartic and found only one solution.
- So that must be the correct quartic.

Return to $X_0(30)$

Know this is hyperelliptic and so has a model

$$y^2 = h(x), \qquad h = a_8 x^8 + \cdots + a_0.$$

The model is **not** unique. If (u, v) is any point on this model, we then we can change the model to move this point to infinity:

$$x' = \frac{1}{x - u}, \qquad y' = \frac{y}{(x - u)^4}.$$

The new model has the form

$$y'^2 = v^2 x'^8 + \cdots .$$

If $v = 0$ (i.e. the original point was a Weierstrass point) then we would end up with $y'^2 =$ degree 7 but otherwise it is $y'^2 =$ degree 8.

Now the infinity cusp c_∞ is a point on $X_0(30)$. Let's move c_∞ to infinity on the hyperelliptic model. **Question: Do we obtain a degree 7 model or a degree 8 model?**

Exercise.

(i) Let

$$X \ : \ y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0$$

be a curve of genus g where $a_{2g+2} \neq 0$. Let ∞_+ be one of the two points at infinity. Show that

$$\operatorname{ord}_{\infty_+}\left(\frac{dx}{y}\right) = g-1, \quad \operatorname{ord}_{\infty_+}\left(\frac{xdx}{y}\right) = g-2, \ldots,$$

(ii) Let

$$X \ : \ y^2 = a_{2g+1}x^{2g+1} + \cdots + a_0$$

be a curve of genus g (here necessarily $a_{2g+1} \neq 0$ otherwise the genus would be smaller than g). Let ∞ be the unique point at infinity. Show that

$$\operatorname{ord}_{\infty}\left(\frac{dx}{y}\right) = 2(g-1), \quad \operatorname{ord}_{\infty}\left(\frac{xdx}{y}\right) = 2(g-2), \ldots,$$

Recall that basis for $S_2(\Gamma_0(30))$ is

$$
\begin{aligned}
f_1 &= q - q^4 - q^6 - 2q^7 + q^9 + O(q^{10}),\\
f_2 &= q^2 - q^4 - q^6 - q^8 + O(q^{10}),\\
f_3 &= q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + O(q^{10}).
\end{aligned}
$$

$$
\mathrm{ord}_{c_\infty}\left(f_1(q)\frac{dq}{q}\right) = 0, \quad \mathrm{ord}_{c_\infty}\left(f_2(q)\frac{dq}{q}\right) = 1, \quad \mathrm{ord}_{c_\infty}\left(f_3(q)\frac{dq}{q}\right) = 2.
$$

$$
\therefore \quad \mathrm{ord}_{c_\infty}(\omega) \le 2, \qquad \forall \omega \in \Omega(X) \setminus \{0\}.
$$

But if $c_\infty = \infty$ on $y^2 =$ degree 7 model, then there is some ω with $\mathrm{ord}_{c_\infty}(\omega) = 4$.

$\therefore$ When we move c_∞ to ∞ we get a $y^2 =$ degree 8 model.

$$X \ : \ y^2 = a_8 x^8 + a_7 x^7 + \cdots + a_0, \qquad a_8 \neq 0, \qquad c_\infty = \infty_+.$$

$$\mathrm{ord}_{c_\infty}\left(f_1(q)\frac{dq}{q}\right) = 0, \quad \mathrm{ord}_{c_\infty}\left(f_2(q)\frac{dq}{q}\right) = 1, \quad \mathrm{ord}_{c_\infty}\left(f_3(q)\frac{dq}{q}\right) = 2.$$

$$\mathrm{ord}_{\infty_+}\left(\frac{dx}{y}\right) = 2, \qquad \mathrm{ord}_{\infty_+}\left(x\frac{dx}{y}\right) = 1, \qquad \mathrm{ord}_{\infty_+}\left(x^2\frac{dx}{y}\right) = 0.$$

From the valutions

$$\begin{aligned} \frac{dx}{y} &= \alpha_3 \cdot f_3(q)\frac{dq}{q}, \\ \frac{xdx}{y} &= \beta_2 \frac{f_2(q)dq}{q} + \beta_3 \frac{f_3(q)dq}{q}, \\ \frac{x^2dx}{y} &= \gamma_1 \frac{f_1(q)dq}{q} + \gamma_2 \frac{f_2(q)dq}{q} + \gamma_3 \frac{f_3(q)dq}{q}, \end{aligned}$$

where α_3, β_2 and $\gamma_1 \neq 0$.

$$X \ : \ y^2 = a_8x^8 + a_7x^7 + \cdots + a_0, \qquad a_8 \neq 0, \qquad c_\infty = \infty_+.$$

$$\frac{dx}{y} = \alpha_3 \cdot f_3(q)\frac{dq}{q},$$
$$\frac{xdx}{y} = \beta_2\frac{f_2(q)dq}{q} + \beta_3\frac{f_3(q)dq}{q},$$
$$\frac{x^2dx}{y} = \gamma_1\frac{f_1(q)dq}{q} + \gamma_2\frac{f_2(q)dq}{q} + \gamma_3\frac{f_3(q)dq}{q},$$

The change of hyperelliptic model

$$x \mapsto rx, \qquad y \mapsto sy$$

preserve points at infinity but has the effect

$$\frac{dx}{y} \mapsto (r/s)\frac{dx}{y}, \qquad \frac{xdx}{y} \mapsto (r^2/s)\frac{xdx}{y}, \qquad \dots$$

Thus we can make $\alpha_3 = 1$ and $\beta_2 = 1$.

$$X \;:\; y^2 = a_8x^8 + a_7x^7 + \cdots + a_0, \qquad a_8 \neq 0, \qquad c_\infty = \infty_+.$$

$$\frac{dx}{y} = f_3(q)\frac{dq}{q},$$
$$\frac{xdx}{y} = \frac{f_2(q)dq}{q} + \beta_3\frac{f_3(q)dq}{q},$$
$$\frac{x^2dx}{y} = \gamma_1\frac{f_1(q)dq}{q} + \gamma_2\frac{f_2(q)dq}{q} + \gamma_3\frac{f_3(q)dq}{q},$$

The change of model

$$x \mapsto x + t, \qquad y \mapsto y.$$

preserves the points at infinity and has the effect

$$\frac{dx}{y} \mapsto \frac{dx}{y}, \qquad \frac{xdx}{y} \mapsto \frac{xdx}{y} + t\frac{dx}{y}.$$

So we can suppose $\beta_3 = 0$. i.e.

$$\frac{dx}{y} = f_3(q)\frac{dq}{q}, \qquad \frac{xdx}{y} = f_2(q)\frac{dq}{q}.$$

$$X \ : \ y^2 = a_8 x^8 + a_7 x^7 + \cdots + a_0, \qquad a_8 \neq 0, \qquad c_\infty = \infty_+.$$

$$\frac{dx}{y} = f_3(q)\frac{dq}{q}, \qquad \frac{xdx}{y} = f_2(q)\frac{dq}{q}.$$

$$x = f_2(q)/f_3(q) = \frac{1}{q} - 1 + q - q^2 + 2q^3 - 2q^4 + 2q^5 - 3q^6 + 5q^7 - 5q^8 + 5q^9 + \cdots .$$

$$y = \frac{dx}{dq} \cdot \frac{q}{f_3(q)} = -\frac{1}{q^4} + \frac{1}{q^3} - \frac{1}{q^2} - \frac{1}{q} + 5 - 15q + 29q^2 - 60q^3 + 118q^4 - 210q^5 + 346q^6 - 573q^7 + 929q^8 - 1454q^9 + \cdots .$$

By comparing the coefficients of q^{-8} on both sides we see that $a_8 = 1$.

$$X \; : \; y^2 = x^8 + a_7 x^7 + \cdots + a_0, \qquad\qquad c_\infty = \infty_+.$$

$$x = \frac{1}{q} - 1 + q - q^2 + 2q^3 - 2q^4 + 2q^5 - 3q^6 + 5q^7 - 5q^8 + 5q^9 + \cdots .$$

$$y^2 - x^8 = \frac{6}{q^7} - \frac{33}{q^6} + \cdots$$

so $a_7 = 6$. Also

$$y^2 - x^8 - 6x^7 = \frac{9}{q^6} - \frac{48}{q^5} + \cdots$$

so $a_6 = 9$. Continuing in this fashion we arrive at

$$y^2 - x^8 - 6x^7 - 9x^6 - 6x^5 + 4x^4 + 6x^3 - 9x^2 + 6x - 1 = O(q^{100}).$$

Therefore, a model for $X_0(30)$ is

$$X_0(30) \; : \; y^2 \; = \; x^8 + 6x^7 + 9x^6 + 6x^5 - 4x^4 - 6x^3 + 9x^2 - 6x + 1.$$

The Modular Curve X_H

$H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$

- An isomorphism $\alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ a **level N structure on E**.
- A level N-structure is same as choice of basis for $E[N]$: $P = \alpha^{-1}(e_1)$, $Q = \alpha^{-1}(e_2)$ where $e_1 = (1,0)$, $e_2 = (0,1)$.
- We call pairs (E_1, α_1) and (E_2, α_2) H-**isomorphic**, and write

$$(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$$

  if there is an isom $\phi : E_1 \to E_2$ and an element $h \in H$ such that

$$\alpha_1 \;=\; h \circ \alpha_2 \circ \phi \qquad \text{(think of } h \in H \text{ as } h : (\mathbb{Z}/N\mathbb{Z})^2 \cong (\mathbb{Z}/N\mathbb{Z})^2\text{).}$$

Suppose $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$. Then there is a modular curve X_H defined over $\mathrm{Spec}(\mathbb{Z}[1/N])$ such that ...

K be a perfect field, $\mathrm{char}(K) = 0$, or $\mathrm{char}(K) \nmid N$.

- A point $Q \in Y_H(\overline{K})$ represents class $[(E, \alpha)]_H$ where $E/\overline{K}$, α a mod N level structure;
- we identify $Q = [(E, \alpha)]_H$.

Lemma

Let $Q = [(E, \alpha)]_H \in Y_H(\overline{K})$. Let $E'/\overline{K}$ be an elliptic curve that is isomorphic to E. Then there is some isomorphism $\alpha' : E'[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ such that $Q = [(E', \alpha')]_H$.

i.e. I can replace E by any isomorphic E' and obtain the same point $Q \in Y_H$ provided I suitably choose the mod N level structure on E'.

Galois action and rationality

$$G_K \text{ acts on pairs } (E,\alpha) \qquad (E,\alpha)^\sigma := (E^\sigma, \alpha\circ\sigma^{-1}).$$

Action is compatible with action of G_K on $Y_H(\overline{K})$:

$$Q = [(E,\alpha)]_H \implies Q^\sigma = [(E^\sigma, \alpha\circ\sigma^{-1})]_H.$$

Lemma

Let $Q \in Y_H(\overline{K})$. Then $Q \in Y_H(K)$ iff $Q = [(E,\alpha)]_H$ for some E/K, $\alpha : E[N] \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^2$ such that for all $\sigma \in G_K$, there is an $\phi_\sigma \in \mathrm{Aut}_{\overline{K}}(E)$ and $h_\sigma \in H$ satisfying

$$\alpha = h_\sigma \circ \alpha \circ \sigma^{-1} \circ \phi_\sigma. \tag{1}$$

The case $-I \notin H$

Theorem

Suppose $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ *and* $-I \in H$.

(i) *Every* $Q \in Y_H(K)$ *is supported on some* E/K *(i.e.* $\exists E/K$ *and* $\alpha : E[N] \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^2$ *such that* $Q = [(E, \alpha)]_H$.

(ii) *If* $Q \in Y_H(K)$ *and* $j(Q) \neq 0$, 1728, *then* $Q = [(E, \alpha)]_H$ *such that* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation). Conversely, if there is* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation) then* $[(E, \alpha)] \in Y_H(K)$ *for a suitable* α.

(iii) *If* $Q \in Y_H(K)$ *and* $j(Q) \neq 0$, 1728, *and* $Q = [(E, \alpha)]_H$ *as above, then* $Q = [(E', \alpha')]$ *for any quadratic twist* E'/K *defined over* K, *and for suitable* α'.

Theorem

Suppose $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ *and* $-I \in H$.

(ii) *If* $Q \in Y_H(K)$ *and* $j(Q) \neq 0$, 1728, *then* $Q = [(E, \alpha)]_H$ *such that* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation). Conversely, if there is* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation) then* $[(E, \alpha)] \in Y_H(K)$ *for a suitable* α.

Some details for (ii). Note that $j(Q) = j(E)$. As this $\neq 0$, 1728, the automorphism group $\mathrm{Aut}(E) = \{1, -1\}$. Thus $\phi_\sigma = \pm 1$ and in particular commutes with all other maps. But

$$\alpha = h_\sigma \circ \alpha \circ \sigma^{-1} \circ \phi_\sigma \implies \alpha \circ \sigma = (\phi_\sigma h_\sigma) \circ \alpha.$$

This can be rewritten as

$$\overline{\rho}_{E,N}(\sigma) = \phi_\sigma h_\sigma$$

once we have taken $\alpha^{-1}(1, 0)$, $\alpha^{-1}(0, 1)$ as basis for $E[N]$. Note that $\phi_\sigma h_\sigma = \pm h_\sigma \in H$. Thus $\overline{\rho}_{E,N}(G_K) \subseteq H$ as required.

The case $-I \notin H$

Theorem

Suppose $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ *and* $-I \notin H$.

(i) *Every* $Q \in Y_H(K)$ *is supported on some* E/K *(i.e.* $\exists E/K$ *and* $\alpha : E[N] \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^2$ *such that* $Q = [(E,\alpha)]_H$.

(ii) *If* $Q \in Y_H(K)$ *and* $j(Q) \neq 0, 1728$, *then* $Q = [(E,\alpha)]_H$ *such that* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation). Conversely, if there is* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation) then* $[(E,\alpha)] \in Y_H(K)$ *for a suitable* α.

(iii) *If* $Q \in Y_H(K)$ *and* $j(Q) \neq 0, 1728$, *and* $Q = [(E,\alpha)]_H$ *as above, then* E *is unique.*

Theorem

Suppose $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ *and* $-I \notin H$.

(ii) *If* $Q \in Y_H(K)$ *and* $j(Q) \neq 0$, 1728, *then* $Q = [(E, \alpha)]_H$ *such that* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation). Conversely, if there is* E *is defined over* K *and* $\overline{\rho}_{E,N}(G_K) \subset H$ *(up to conjugation) then* $[(E, \alpha)] \in Y_H(K)$ *for a suitable* α.

(iii) *If* $Q \in Y_H(K)$ *and* $j(Q) \neq 0$, 1728, *and* $Q = [(E, \alpha)]_H$ *as above, then* E *is unique.*

Some details. As before $\phi_\sigma \in \{\pm 1\}$ and $\overline{\rho}_{E,N}(\sigma) = \phi_\sigma h_\sigma$.
The map $\psi : \sigma \mapsto \phi_\sigma$ is a quadratic character.

If ψ is trivial then $\overline{\rho}_{E,N}(G_K) \subset H$. Otherwise ψ is a quadratic character, and by Galois theory its kernel fixes a quadratic extension $K(\sqrt{d})$ of K.

Now $\overline{\rho}_{E_d,N} = \psi \cdot \overline{\rho}_{E,N}$, and thus $\overline{\rho}_{E_d,N}(\sigma) = h_\sigma \in H$.

Replacing E by E_d and adjusting the level structure α gives $Q = [(E, \alpha)]_H$ with E defined over K and $\overline{\rho}_{E,N}(G_K) \subset H$.