Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 537–547

On Shafarevich–Tate Sets

Takashi Ono

Let K/k be a finite Galois extension of number fields with the Galois group $g = \mathrm{Gal}(K/k)$. Let g_P be the decomposition group at a prime P in K. Let G be a g-group. For each P in K, we have the restriction map $r_P : H(g,G) \to H(g_P, G)$ of 1-cohomology sets for which $\mathrm{Ker}\ r_P$ makes sense. The *Shafarevich–Tate Set* for $(K/k, G)$ is defined by $Ш(K/k, G) = \cap_P \mathrm{Ker}\, r_P$.

Let X be a smooth curve of genus ≥ 2 over $\mathbb{Q}$. Then $G = \mathrm{Aut}\ X$ is finite by Schwarz theorem and there is a finite Galois extension $K/\mathbb{Q}$ so that G is a finite g-group, $g = \mathrm{Gal}(K/\mathbb{Q})$. The set $Ш(K/k, G)$ becomes finite. As is well-known, the determination of the finite set amounts to an arithmetical refinement of geometrical classification of curves. In this paper, we shall show, among others, that for a hyperelliptic curve $X : y^2 = x^5 - \ell^2 x$, $\ell =$ an odd prime, we have $Ш(K/\mathbb{Q}, G) = 1$ (Hasse principle) if $\ell \equiv 3, 5 \mod 8$, but $\# Ш(K/\mathbb{Q}, G) = 2$ if $\ell \equiv 1, 7 \mod 8$.

There is a way to associate an $S - T$ set $Ш_{\mathbf{H}}(g, G)$ for any group g and a g-group G once we specify a family of subgroups of g (such as the family of decomposition groups g_P when $g = \mathrm{Gal}(K/k)$). E.g., for any finite group G, let $g = G$, acting on itself as inner automorphisms, and let $\mathbf{H}$ be the family of all cyclic subgroups of G. One checks $Ш_{\mathbf{H}}(G, G) = 1$ ("Hasse principle") for some easy groups. Here is an interesting question: *Does the Monster enjoy the Hasse principle?*

§1. $Ш_{\mathbf{H}}(g, G)$.

Let g be a group and G be a (left) g-group. A cocycle is a map $f : g \to G$ such that

$$f(st) = f(s)f(t)^s, \quad s, t \in g.$$

We denote by $Z(g, G)$ the set of all cocycles. Two cocycles f, f' are equivalent, written $f \sim f'$ if there exists an $a \in G$ such that

$$f'(s) = a^{-1} f(s) a^s, \quad s \in g.$$

Received July 29, 1998.

We denote by [f] the class of a cocycle f. The quotient

$$H(g,G) = Z(g,G)/\sim$$

is the cohomology set. $Z(g,G)$ contains a distinguished map 1 defined by $1(s) = 1$ for all $s \in g$. Then a map $f \sim 1$ is said to be a coboundary. Consequently, we have

$$f \text{ is a coboundary} \Leftrightarrow f(s) = a^{-1}a^s \text{ for some } a \in G\ .$$

Now, suppose we are given a family $\mathbf{H}$ of subgroups of g. For each subgroup $h \in \mathbf{H}$, we have the restriction map

$$r_h : H(g,G) \to H(h,G)$$

induced by $f \mapsto f|_h$, $f \in Z(g,G)$. This map sends the distinguished class in $H(g,G)$ to the one in $H(h,G)$. Hence $\operatorname{Ker} r_h$ makes sense. In this situation, we put

$$Ш_{\mathbf{H}}(g,G) = \bigcap_h \operatorname{Ker} r_h,$$

and call this the Shafarevich–Tate set for (g,G) with respect to $\mathbf{H}$. For example, for any finite group G, let $g = G$, acting on itself as inner automorphisms, and let $\mathbf{H} = \mathbf{H}_{\text{cyc}}$ the family of all cyclic subgroups of G. The determination of $Ш_{\text{cyc}}(G) = Ш_{\mathbf{H}}(G,G)$ seems to be an interesting exercise in finite group theory. One verifies that all finite abelian groups, dihedral groups D_{2m} and the quaternion group Q_8 enjoy the Hasse principle $Ш_{\text{cyc}}(G) = 1$.

Example 1. We shall find a pair (g,G) which fails to have Hasse principle with respect to $\mathbf{H} = \mathbf{H}_{\text{cyc}}$. So let

$$\begin{aligned} g &= \langle \sigma, \tau;\ \sigma^2 = \tau^2 = 1, \quad \tau\sigma = \sigma\tau \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\ G &= \langle a;\ a^8 = 1 \rangle \cong \mathbb{Z}/8\mathbb{Z}\ , \end{aligned}$$

with the action

$$a^\sigma = a^{-1}, \quad a^\tau = a^5.$$

Note that we have

$$\mathbf{H} = \mathbf{H}_{\text{cyc}} = \{1, \langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle\}.$$

Let $[f]$ be an element of $Ш_{\mathbf{H}}(g,G) \subset H(g,G)$. Since each cyclic subgroup $\langle s \rangle$, $s \in g$, belongs to $\mathbf{H}$, we have $f(s) = a(s)^{-1}a(s)^s$, $a(s) \in G$; so, on replacing f by a cocycle equivalent to it using $a(\sigma)$, we may assume that

$$f(\sigma)=1, \quad f(\tau)=x^{-1}x^{\tau}, \quad x=a^{i}, \quad 0\le i\le 7.$$

Then, we find

$$f(\tau)=x^{-1}x^{\tau}=\begin{cases} 1, & i: \text{ even },\\ a^4, & i: \text{ odd }. \end{cases} \tag{1.1}$$

If i is even, then obviously $f=1$; if i is odd, then we have $f \not\sim 1$. In fact, if not, there should be $y\in G$ such that $1=f(\sigma)=y^{-1}y^{\sigma}$ and $f(\tau)=y^{-1}y^{\tau}$, with $y=a^{j}$ for some j. The first equality implies that $a^{2j}=1$; hence j must be even. Then we have $a^4=f(\tau)=y^{-1}y^{\tau}=a^{-j}a^{5j}=a^{4j}=1$, a contradiction.

Conversely, one can easily construct a cocycle f which takes values shown in (1.1) at the generators σ,τ of g. So we found that

$$\#Ш_{\mathbf{H}}(g,G)=2 \tag{1.2}$$

with a single nontrivial class $[f]$ given by $f(\sigma)=1$, $f(\tau)=a^4$.

§2. $Ш(K/k,G)$.

Let K/k be a finite Galois extension of number fields and g be the Galois group: $g=\mathrm{Gal}(K/k)$. For a (finite or infinite) prime P in K, denote by g_P the decomposition group of P for K/k:

$$g_P=\{s\in g;\ P^s=P\}.$$

Let

$$\mathbf{H}=\mathbf{H}_{\mathrm{dec}}=\{g_P; P \text{ primes in } K\}.$$

For a g-group G, we can speak of the Shafarevich–Tate set $Ш_{\mathbf{H}}(g,G)$ in §1. Since the Galois group and the family $\mathbf{H}=\mathbf{H}_{\mathrm{dec}}$ are determined by the given Galois extension K/k, we can set

$$Ш(K/k,G)=Ш_{\mathbf{H}}(g,G). \tag{2.1}$$

There are two extreme cases where we get the Hasse principle $Ш(K/k,G)=1$ without effort. First of all, let us call K/k *trivial* if $g=g_P$, i.e., if $g\in\mathbf{H}_{\mathrm{dec}}$. In this case, we have $Ш(K/k,G)=1$, trivially, for any g-group G. For example, every cyclic extension K/k is trivial by Chebotarev theorem. A counterexample for a noncyclic abelian extension will be given in the next example. Secondly, if g acts trivially, then $Z(g,G) = \mathrm{Hom}(g,G)$ and $Z(g_P,G) = \mathrm{Hom}(g_P,G)$ for all P; hence, again by Chebotarev, we have $Ш(K/k,G) = 1$.

The following important relation follows also from Chebotarev theorem.

$$\mathbf{H}_{\mathrm{cyc}} \subset \mathbf{H}_{\mathrm{dec}}\ . \tag{2.2}$$

Let us call K/k *locally cyclic* if g_P is cyclic for all primes P. Since $\#g_P \leq 2$ for primes at infinity, we have only to check the finite primes. For example, if K/k is unramified then K/k is locally cyclic. In view of (2.2), we have

$$\mathbf{H}_{\mathrm{cyc}} = \mathbf{H}_{\mathrm{dec}} \Leftrightarrow K/k \text{ is locally cyclic.} \tag{2.3}$$

Therefore in such a case an arithmetical problem of determining $Ш(K/k,G)$ is reduced to an algebraic problem of $Ш_{\mathbf{H}}(g,G)$ with $g = \mathrm{Gal}(K/k)$ and $\mathbf{H} = \mathbf{H}_{\mathrm{cyc}}$. The following example discusses these matters.

Example 2. Let ℓ be an odd prime and ζ be a primitive 8th root of unity. Let $k = \mathbb{Q}(\sqrt{\ell})$, $K = k(\zeta) = \mathbb{Q}(i, \sqrt{2}, \sqrt{\ell})$. The extension K/k is Galois with

$$g = \mathrm{Gal}(K/k) = \langle \sigma, \tau;\ \sigma^2 = \tau^2 = 1, \quad \tau\sigma = \sigma\tau \rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Let $G = \langle \zeta \rangle \subset K^\times$. The group g acts on G by the Galois action: $\zeta^\sigma = \zeta^{-1} = \bar{\zeta}$, $\zeta^\tau = \zeta^5$. Hence the g-group (g,G) is exactly the one in Example 1. Since $g = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the only subgroup of g which is not cyclic is g itself. Hence

$$\begin{aligned} &K/k \text{ is locally cyclic } \Leftrightarrow \mathbf{H}_{\mathrm{cyc}} = \mathbf{H}_{\mathrm{dec}} \Leftrightarrow g \notin \mathbf{H}_{\mathrm{dec}} \\ &\quad \Leftrightarrow g \neq g_P \text{ for all } P \Leftrightarrow K/k \text{ is nontrivial.} \end{aligned} \tag{2.4}$$

From (1.2), (2.3), (2.4), we find

$$K/k \text{ is nontrivial } \Leftrightarrow \#Ш(K/k,G) = 2. \tag{2.5}$$

Now a criterion for the nontriviality of K/k can be obtained by the Kummer theory (cf. [2], Satz 119 and [5],(2.7) Theorem):

(2.6)

$$K/k \text{ is nontrivial } \Leftrightarrow \begin{array}{l} \ell \equiv 3 \mod 4 \text{ and } x^2 \equiv \ell \mod 4(1-\zeta) \\ \text{has a solution in } \mathbb{Z}[\zeta]. \end{array}$$

In particular, if $\ell \equiv 7 \mod 8$, the congruence has a solution $x = i$; so, from (2.5) and (2.6), we have

$$\#Ш(K/k,G) = 2 \quad \text{for} \quad \ell \equiv 7 \mod 8. \tag{2.7}$$

In terms of ordinary Galois cohomology, we have an isomorphism

(2.8) $k^\times/(k^\times)^8 \cong H^1(k,G)$, (similarly for k_p for each p).

The Shafarevich–Tate group of G (in Galois cohomology) is

(2.9) $Ш(k,G) \overset{\text{def}}{=} \operatorname{Ker}(H^1(k,G) \to \Pi_p H^1(k_p,G))$.

It can be shown that there is a natural bijection

(2.10) $$Ш(k,G) \cong Ш(K/k,G)$$

where the set on the right hand side is the one in (2.1). In view of (2.7)–(2.10), we find that, when $\ell \equiv 7 \mod 8$, the Hasse principle for the equation

$$x^8 = a, \quad a \in k = \mathbb{Q}(\sqrt{\ell})$$

does not hold for some a. (In fact, one can take $a = 16$, as pointed out by Prof. Wada.) Instead of K/k, consider the absolute cyclotomic field $F = \mathbb{Q}(\zeta)$ whose Galois group is the same as that for K/k. Since 2 is totally ramified in F, the extension $F/\mathbb{Q}$ is trivial; hence, unlike (2.7), we have $Ш(F/\mathbb{Q},G) = 1$ for all ℓ.

§3. $Ш(K/k, \operatorname{Aut} X)$.

Let X be a quasi-projective variety over a number field k. Assume that there is a finite Galois extension K/k so that every $\bar{k}$-automorphism of X is a K-automorphism. When it is so, we shall call K a (finite) splitting field for $G = \operatorname{Aut} X$ over k. As in §2, we can talk about the Shafarevich–Tate set $Ш(K/k,G)$ which can be identified with the ordinary $Ш(k,G)$ as mentioned in (2.10). By the assumption on X, we have a well-known bijection:

(3.1) $H^1(k,G) \cong \operatorname{Twist}(X/k)$, (similarly for k_p).

Consequently, determination of $Ш(K/k,G)$ amounts to an arithmetical refinement of a geometrical classification of varieties:

(3.2) $Ш(K/k,G) = \{Y/k; Y \cong X \text{ over } \bar{k} \text{ and } k_p \text{ for all } p\}$.

In particular, the Hasse principle for twists means that

(3.3) $Y \cong X$ over $\bar{k}$ and k_p for all $p \Rightarrow Y \cong X$ over k.

If X is a smooth curve of genus $g \geq 2$, then $G = \operatorname{Aut} X$ is a finite group of order at most $84(g-1) = -42E(X)$ by Hurwitz theorem. Therefore G is split by a finite Galois extension K/k.

Example 3. Consider the celebrated quartic

$$X : x^3y + y^3z + z^3x = 0 \text{ over } k = \mathbb{Q}\ .$$

We have $g = 3$ and $G = \operatorname{Aut} X \cong \mathrm{PSL}_2(\mathbb{F}_7)$, a simple group of order $168 = 2^3 \cdot 3 \cdot 7$. Klein [3] shows that

$$G = \langle u, v, w\rangle, \quad u, v, w \in \mathrm{PGL}_3(\mathbb{Q}(\zeta)),$$

where

$$u = \begin{pmatrix} \zeta & & \\ & \zeta^4 & \\ & & \zeta^2 \end{pmatrix}, \quad v = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad w = \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}$$

with

$$a = \frac{\zeta^5 - \zeta^2}{\sqrt{-7}}, \quad b = \frac{\zeta^3 - \zeta^4}{\sqrt{-7}}, \quad c = \frac{\zeta^6 - \zeta}{\sqrt{-7}}, \quad \zeta = \text{ a 7th root of 1}\ .$$

Note that $\sqrt{-7} = \zeta + \zeta^4 + \zeta^2 - \zeta^6 - \zeta^3 - \zeta^5$ (Gauss sum). Consequently, $K = \mathbb{Q}(\zeta)$ splits G. Since $K/\mathbb{Q}$ is cyclic, it is trivial and we have the Hasse principle $Ш(K/\mathbb{Q}, \operatorname{Aut} X) = 1$ without effort.

However, Hasse principle cannot always be obtained without effort as the following example indicates. As for the details of this example see [6].

Example 4. Consider the curve over $k = \mathbb{Q}$:

$$X : y^4 = x^4 - \ell^2, \quad \ell = \text{ an odd prime.}$$

This curve is smooth and of genus 3. We have $G = \operatorname{Aut} X = A \cdot B$, $A \cap B = 1$, A normal in G, where $A = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $B = S_3$, the symmetric group on 3 letters. So $\#G = 96 = 2^5 \cdot 3$. It can be shown that $K = \mathbb{Q}(i, \sqrt{2}, \sqrt{\ell})$ splits G and $g = \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The determination of $\mathbf{H}_{\mathrm{dec}}$ amounts to the exhibition of the Artin reciprocity for the abelian extension $K/\mathbb{Q}$. Thus we find: $K/\mathbb{Q}$ is trivial $\Leftrightarrow g \in \mathbf{H}_{\mathrm{dec}} \Leftrightarrow \ell^* = (-1)^{\frac{\ell-1}{2}}\ell \equiv 5 \mod 8$. So, if $\ell^* \equiv 5 \mod 8$, we get the Hasse principle $Ш(K/\mathbb{Q}, \operatorname{Aut} X) = 1$ without effort. On the other hand, in the remaining case $\ell^* \equiv 1 \mod 8$, we still have $Ш(K/\mathbb{Q}, \operatorname{Aut} X) = 1$, but with some effort.

Example 5. Let ℓ be an odd prime and X be a hyperelliptic curve of genus 2 over $k = \mathbb{Q}$:

$$X : y^2 = x^5 - \ell^2 x\ . \tag{3.4}$$

Since X is not smooth, we mean by X the normalization (Riemann surface) over $\mathbb{Q}$ associated to the equation (3.4). When we compute the group $G = \operatorname{Aut} X$, we can do it in the function field $\bar{\mathbb{Q}}(x,y)/\bar{\mathbb{Q}}$ for the equation (3.4). It is natural to seek $t \in G : t(x,y) = (x',y')$ such that

$$x' = \frac{ax+b}{cx+d}\,, \quad y' = \frac{ey}{(cx+d)^3}\,.$$

We find, for example, elements $u, v \in G$ as follows:

$$u : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \quad e = \zeta = \tfrac{1+i}{\sqrt{2}},$$
$$v : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & i\sqrt{\ell^*} \\ 1/\sqrt{\ell^*} & -i \end{pmatrix}, \quad e = -(\sqrt{2}/\zeta)^3\,,$$

where $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$.

The group G acts on the space $\Omega^1(X)$ of holomorphic 1-forms. With respect to the standard basis dx/y, xdx/y for $\Omega^1(X)$, we obtain a faithful representation

$$G = \operatorname{Aut} X \to GL_2(\bar{\mathbb{Q}}). \tag{3.5}$$

The matrices U, V corresponding to u, v by (3.5) are:

$$U = \zeta \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad U^8 = 1,$$
$$V = \tfrac{\zeta^3}{\sqrt{2}} \begin{pmatrix} 1 & i/\sqrt{\ell^*} \\ -\sqrt{\ell^*} & i \end{pmatrix}, \quad V^3 = 1\,.$$

Let us put

$$S = VU; \quad \text{hence } S^2 = 1.$$

Call G' the subgroup of G generated by U, V:

$$G \supset G' = \langle U, V \rangle = \langle V, S \rangle.$$

Put

$$\begin{aligned} I &= U^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad I^2 = -1, \\ J &= -i \begin{pmatrix} 0 & 1/\sqrt{\ell^*} \\ \sqrt{\ell^*} & 0 \end{pmatrix}, \quad J^2 = -1\,, \\ K &= IJ. \end{aligned}$$

Then one verifies that $Q_8 = \langle I, J\rangle$ is the quaternion group. Since $VI = JV$, $SI = JS$, we see that Q_8 is normal in G'. Moreover, one verifies that

$$G'/Q_8 \cong S_3$$

by the correspondence

$$[V] = v \bmod Q_8 \leftrightarrow (123), \quad [S] = S \bmod Q_8 \leftrightarrow (12).$$

Hence $\#G' = 8 \cdot 6 = 48$. On the other hand, we have $\#G \leq 48(g-1) = 48(2-1) = 48$. Therefore we have $G = G'$ and so

$$G/Q_8 \cong S_3, \quad G = \operatorname{Aut} X. \tag{3.6}$$

As a splitting field for $G = \operatorname{Aut} X$ over $\mathbb{Q}$, we can take

$$K = \mathbb{Q}(i, \sqrt{2}, \sqrt{\ell^*}) = \mathbb{Q}(\zeta, \sqrt{\ell^*}).$$

Then we have $g = \operatorname{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle \sigma, \tau, \rho\rangle$ with

	i	$\sqrt{2}$	ζ	$\sqrt{\ell^*}$
σ	$-i$	$\sqrt{2}$	$\bar{\zeta}$	$\sqrt{\ell^*}$
τ	i	$-\sqrt{2}$	$-\zeta$	$\sqrt{\ell^*}$
ρ	i	$\sqrt{2}$	ζ	$-\sqrt{\ell^*}$.

The group $G = \langle U, V\rangle$ is naturally a g-group and the action of g is given as follows:

(3.7)

	σ	τ	ρ
U	SV	$-U$	U
V	$VI = JV$	V	$VJ = -KV$
S	S	$-S$	$SK = -KS$
I	$-I$	I	I
J	$-J$	J	$-J$
K	K	K	$-K$.

Next we have to determine the family $\mathbf{H}_{\text{dec}}$ for our $g = \operatorname{Gal}(K/\mathbb{Q})$. This amounts to exposing Hilbert's Galois theory and Artin's law of reciprocity for the abelian extension $K/\mathbb{Q}$. Note that we have an important inclusion $\mathbf{H}_{\text{cyc}} \subset \mathbf{H}_{\text{dec}}$ in (2.2). Hence we have only to determine decomposition groups g_P which are not cyclic. Since this part is the same as the corresponding part of Example 4 (for the curve $X : y^4 = x^4 - \ell^2$) we can copy the table (4.4) in [6]:

(3.8)

ℓ	$\mathbf{H}_{\text{dec}}$
$\ell \equiv 1 \mod 8$	$\mathbf{H}_{\text{cyc}}$ and $\langle \sigma, \tau \rangle$
$\ell \equiv 3 \mod 8$	$\mathbf{H}_{\text{cyc}}$ and $\langle \sigma\tau, \rho \rangle$, g
$\ell \equiv 5 \mod 8$	$\mathbf{H}_{\text{cyc}}$ and $\langle \tau, \rho \rangle$, g
$\ell \equiv 7 \mod 8$	$\mathbf{H}_{\text{cyc}}$ and $\langle \sigma, \rho \rangle$, $\langle \sigma, \tau \rangle$.

If $\ell^* \equiv 5 \mod 8$, i.e., if $\ell \equiv 3, 5 \mod 8$, then, in (3.8), g belongs to $\mathbf{H}_{\text{dec}}$ and so $K/\mathbb{Q}$ is trivial; hence $\text{Ш}(K/\mathbb{Q}, G) = 1$ without worrying about the action of g on G. On the other hand, if $\ell^* \equiv 1 \mod 8$, i.e., if $\ell \equiv 1, 7 \mod 8$, then g is not in $\mathbf{H}_{\text{dec}}$; hence $K/\mathbb{Q}$ is not trivial and the action of g on G given in (3.7) plays a crucial role. It will turn out that

(3.9) *If* $\ell^* \equiv 1 \mod 8$, *then* $\#\text{Ш}(K/\mathbb{Q}, G) = 2$ *and the single nontrivial cocycle* $[f]$ *in* $\text{Ш}(K/\mathbb{Q}, G)$ *is given by* $f(\sigma) = f(\tau) = 1$, $f(\rho) = K = IJ \in Q_8$.

The rest of the paper is devoted to prove (3.9). First of all, notice that, in the table (3.8), the subgroup $\langle \sigma, \tau \rangle$ appears simultaneously in $\mathbf{H}_{\text{dec}}$ when $\ell^* \equiv 1 \mod 8$. Hence for any $[f]$ in $\text{Ш}(K/\mathbb{Q}, G)$, after a normalization, we may assume that

(3.10) $f(\sigma) = f(\tau) = 1$ and $f(\rho) = A^{-1}A^{\rho}$ for some $A \in G$.

Since $\pm A$ give the same $f(\rho)$, we may assume that A is one of 24 elements: $A = CB$, $B \in \{1, V, V^2, S, SV, SV^2\}$, $C \in \{1, I, J, K\}$. Hence $f(\rho) = B^{-1}C^{-1}C^{\rho}B^{\rho} = \pm B^{-1}B^{\rho}$. As one verifies by (3.7) that $B^{-1}B^{\rho} = 1, J, K$, we find

(3.11) $f(\rho) = \pm 1, \quad \pm J, \quad \pm K.$

(i) If $f(\rho) = 1$, then $f = 1$, i.e., $[f]$ is trivial.

(ii) If $f(\rho) = -1$, then from (3.7) we find that $K^{-1}K^{\sigma} = 1 = f(\sigma)$, $K^{-1}K^{\tau} = 1 = f(\tau)$ and $K^{-1}K^{\rho} = -1 = f(\rho)$; hence $f \sim 1$, i.e., $[f]$ is trivial, again.

(iii) If $f(\rho) = \varepsilon J$, $\varepsilon = \pm 1$, then we have

$$\begin{array}{l} f(\sigma\rho) = f(\sigma)f(\rho)^{\sigma} = (\varepsilon J)^{\sigma} = \varepsilon J^{\sigma} \\ \quad \| \\ f(\rho\sigma) = f(\rho)f(\sigma)^{\rho} = f(\rho) = \varepsilon J \ , \end{array}$$

which is absurd as $J^\sigma = -J$ by (3.7). So there is no such cocycle f. To prove our assertion (3.9), it remains to verify the following statements (iv), (v) and (vi).

(iv) $f(\rho) = \varepsilon K$, $\varepsilon = \pm 1$, together with $f(\sigma) = f(\tau) = 1$, really provides us with a cocycle which restricts a coboundary on each subgroup in $\mathbf{H}_{\text{dec}}$.

(v) Call f, g the cocycles in (iv) corresponding to $\varepsilon = +1, -1$, respectively. Then $f \sim g$, i.e., $[f] = [g]$.

(vi) The cocycle f in (v) is nontrivial: $f \not\sim 1$.

Proof of (iv). We need to show that the function f defined as above on the generators σ, τ, ρ extends on the whole group g consistently. The cocycle condition, $f(st) = f(s)f(t)^s$, $s, t \in g$, forces us to put $f(\sigma\tau) = 1$, $f(\sigma\rho) = f(\tau\rho) = f(\sigma\tau\rho) = \varepsilon K$. The consistency such as $f(\sigma\rho) = f(\rho\sigma)$, $f(\sigma\tau\rho) = f(\rho\sigma\tau)$, $f(\rho^2) = f(1) = 1$ follows from relations $K^\sigma = K^\tau = K$ and $K^\rho = -K$ in (3.7). E.g., $f(\rho^2) = f(\rho)f(\rho)^\rho = \varepsilon K(\varepsilon K)^\rho = KK^\rho = -K^2 = 1$. All other cases are checked likewise. Therefore the value $f(s)$ is εK or 1 according as s contains ρ or not, and we verify at once the cocyle conditions using (3.7). As for the coboundary condition, note that $S^{-1}S^t = \pm K$ whenever $t \in g$ involves ρ. Replacing, S by $\chi(t)S$, if necessary, where $\chi(t) = C^{-1}C^t = \pm 1$, with $C \in \{1, I, J, K\}$, we obtain $\varepsilon K = A_t^{-1}A_t^t$, $A_t \in G$ whenever t involves ρ; hence the cocycle f stated in (iv) induces a coboundary on each cyclic subgroup of g . There is one more group to be considered, i.e., $\langle\sigma, \rho\rangle \in \mathbf{H}_{\text{dec}}$ in case $\ell \equiv 7 \mod 8$. So let $X = S$ or SK according as $\varepsilon = +1$ or -1. Then one finds that $X^{-1}X^\sigma = 1$ and $X^{-1}X^\rho = \varepsilon K$, which means f restricts a coboundary on $\langle\sigma, \rho\rangle$ too.

Proof of (v). By (3.7), we see that $X = K$ is a solution to the following simultaneous equations:

$$X^{-1}X^\sigma = 1, \quad X^{-1}X^\tau = 1, \quad X^{-1}KX^\rho = -K\ .$$

This means that $g \sim f$.

Proof of (vi). Suppose, on the contrary, that $f \sim 1$. Then there is an $X \in G$ such that

$$\begin{aligned} f(\sigma) &= X^{-1}X^\sigma = 1\ , \\ f(\tau) &= X^{-1}X^\tau = 1\ , \\ f(\rho) &= X^{-1}X^\rho = K\ . \end{aligned} \tag{3.12}$$

Write $X = QA$ with $A \in \{1, V, V^2, S, SV, SV^2\}$, $Q \in \{1, I, J, K\}$. Since $Q^{-1}Q^{\tau} = 1$ for all Q, we have $A^{\tau} = A$ by (3.7), and so $A = 1$, V or V^2. Now,

a) $A = 1 \Rightarrow K = Q^{-1}Q^{\rho} = \pm 1$, absurd,

b) $A = V \Rightarrow 1 = V^{-1}Q^{-1}Q^{\sigma}V^{\sigma} = \pm V^{-1}V^{\sigma} = \pm I$, absurd,

c) $A = V^2 \Rightarrow 1 = V^{-2}Q^{-1}Q^{\sigma}V^{2\sigma} = \pm VV^{-\sigma}$, absurd because $V^{\sigma} = VI$ by (3.7) . So the system (3.12) has no solution as required.

References

[1] V.I. Danilov and V.V. Shokurov, "Algebraic Curves", Algebraic Manifolds and Schemes, Springer, Berlin-Heidelberg-New York, 1998.

[2] E. Hecke, "Vorlesungen über die Theorie der algebraischen Zahlen", Chelsea, New York, 1970.

[3] F. Klein, *Über die Tranformation siebenter Ordnung elliptischen Funktionen*, Math. Ann., **14** (1878/79), 428–471.

[4] B. Mazur, *On the passage from local to global in number theory*, Bull. Amer. Math. Soc., **29** (1993), 14–50.

[5] T. Ono, *A note on Shafarevich-Tate sets for finite groups*, Proc. Japan Acad., **74A** (1998), 77–79.

[6] T. Ono, *Shafarevich-Tate set for $y^4 = x^4 - \ell^2$*, Turkish J. Math., **23** (1999), no. 4, 557–573.

Added in Proof. After this paper had been written, I learned from Prof. K. Harada that the Monster enjoys the Hasse principle in the sense described in the last paragraph of the introduction of this paper. Later, Prof. W. Feit communicated to me that any finite simple group enjoys the Hasse principle. This is a consequence of Theorem C in the paper: W. Feit and G. M. Seitz, On finite rational groups and related topics, Illinois J. Math., 33 (1988), 103–131.

The Johns Hopkins University,
Baltimore, Maryland 21218, U.S.A.
E-mail address: `ono@chow.mat.jhu.edu`