Turk J Math
23 (1999) , 557 – 573.

SHAFAREVICH-TATE SET FOR $y^4 = x^4 - \ell^2$

Takashi Ono

Dedicated to Professor Masatoshi Ikeda on the occasion of his 70^{th} birthday

Introduction

This paper consists of two parts, a Text and an Appendix. In (T), we consider a single example, i.e., a plane curve X:$y^4 = x^4 - \ell^2$, ℓ being an odd prime, define the Shafarevich-Tate set $Ш(X/\mathbf{Q})$ without using p-adic numbers and determine its structure. In (A), we take for X a quasi projective algebraic variety defined over a number field k and define the Shafarevich-Tate set $Ш(X/k)$ by conventional mode of Galois cohomology. Two definitions are the same, of course. In (A), we assume the existence of a finite Galois extension K/k so that every $\overline{k}$-automorphism of X is already a K-automorphism. The example in (T) satisfies this assumption with $K = \mathbf{Q}(i, \sqrt{2}, \sqrt{\ell})$. Since the example is so special, we can show that $Ш(X/\mathbf{Q}) = 1$ (Hasse principle). In a certain sense, (T) is much deeper than (A); (T) should be regarded as a torchlight for further research in the framework (A), especially for an algebraic curve X of genus ≥ 2 defined over a number field k because the finiteness of $Ш(X/k)$ is guaranteed by Hurwitz theorem.

1. Structure of automorphism group over C.

First of all, we must review some necessary facts on the curve

$$X : y^4 = x^4 - \ell^2, \quad \ell = \text{ an odd prime} \tag{1.1}$$

Since the projective equation of (1.1) is diagonal, X represents a smooth curve in $P^2(\mathbf{C})$, the complex projective plane. As the degree of X is 4, its genus g=(4-1)(4-2)/2=3. Let us denote by Aut X the group of automorphisms of X, i.e., the group of all birational mappings of X into itself. A good thing about our curve X is that this group is finite. This follows from the celebrated theorem due to Hurwitz:

Let X be a smooth curve of genus $g \geq 2$, then Aut$X$ *is a finite group of order at most* $84(g-1)$* (1.2)

Since our (1.1) has $g = 3$, $\#\mathrm{Aut}\ X \leq 84(3-1) = 168$. It is interesting that the defining equation (1.1) and the upper bound 168 are sufficient to determine the finite group structure of Aut X:

Let $G = \mathrm{Aut\ X}$. *Then G is a semidirect product $G = A \cdot C$, $A \cap C = 1$, A normal in* G, *with* $A = \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, $\quad C = S_3$, *the symmetric group on three letters. Consequently, we have* $\#G = 4 \cdot 4 \cdot 6 = 96 = 2^5 \cdot 3$. (1.3)

In fact, let

$$\varepsilon = \frac{1+i}{\sqrt{2}}, \qquad \theta = \sqrt{\ell^*}, \ell^* = (-1)^{\frac{\ell-1}{2}}\ell. \tag{1.4}$$

Consider rational mappings u,v,w,t given by

$$\begin{aligned} u(x,y) &= (x, iy), \quad v(x,y) = (ix, y), \\ w(x,y) &= (\theta x/y,\ \ell/y), \quad t(x,y) = (\theta y/(ix), \ell/(\varepsilon x)). \end{aligned} \tag{1.5}$$

It is easy to verify that all u, v, w, t belong to Aut X with relations:

$$u^4 = 1,\ v^4 = 1,\ uv = vu, \tag{1.6}$$

* As for a proof of (1.2), see, e.g., [2, p.242].

$$w^2 = 1,\ t^3 = 1,\ wt = t^2 w,\ tw = wt^2, \tag{1.7}$$

$$wuw^{-1} = (uv)^{-1}, wvw^{-1} = v,\ tut^{-1} = v,\ tvt^{-1} = (uv)^{-1}. \tag{1.8}$$

Since $u^2 \neq 1,\ v^2 \neq 1$, (1.6) means that u and v generate an abelian subgroup A of G of order 16 which is a direct product of two cyclic subgroups of order 4:

$$A = \langle u, v \rangle = \langle u \rangle \times \langle v \rangle = \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}.^{\dagger} \tag{1.9}$$

The relation (1.7) shows that $C = \{1, w, t, t^2, wt, tw\}$ forms a subgroup of G of order 6 which is isomorphic to S_3:

$$C = \langle w, t \rangle = S_3, \text{ with } w = (12), t = (123). \tag{1.10}$$

The last relation (1.8) shows that A is normal in $H = \langle u, v, w, t \rangle$. From (1.5)-(1.10), it follows that $H = A \cdot C,\ A \cap C = 1$. Since $2\#H = 2 \cdot 96 = 192 > 168$, we find G=H by (1.2).

2. Action of the Galois group on Aut X.

Let ε, θ be the 8th root of unity and the quadratic number, respectively, introduced in (1.4). Clearly $K = \mathbf{Q}(\varepsilon, \theta)$ is a finite algebraic extension of degree 8. As is easily seen it is a Galois extension. The cyclotomic field $E = \mathbf{Q}(\varepsilon)$ may be written $E = \mathbf{Q}(i, \sqrt{2})$; hence K is the union of three distinct quadratic extensions $\mathbf{Q}(i), \mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{\ell^*})$. Therefore the Galois group $\mathfrak{g} = Gal(K/\mathbf{Q}) = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ with generators σ, τ, ρ:

$$\begin{array}{c|cccc} & i & \sqrt{2} & \varepsilon & \theta \\ \hline \sigma & -i & \sqrt{2} & \bar{\varepsilon} & \theta \\ \tau & i & -\sqrt{2} & -\varepsilon & \theta \\ \rho & i & \sqrt{2} & \varepsilon & -\theta \end{array} \tag{2.1}$$

As we see in (1.5) the generators u, v, w, t of G=Aut X are described as rational mappings defined over K. So the Galois group $\mathfrak{g}$ acts on Aut X. The following is the action on the generactors:

[†] For a group G, we write $G = \langle a, b, c, \ldots \rangle$ if the set $\{a, b, c, \ldots\}$ generates G.

$$\begin{array}{c|cccc} & u & v & w & t \\ \hline \sigma & u^{-1} & v^{-1} & w & uv^2t \\ \tau & u & v & w & u^2t \\ \rho & u & v & v^2w & v^2t \end{array} \tag{2.2}$$

The portion of (2.2) on the abelian subgroup A implies:

$$a^{\sigma} = a^{-1}, a^{\tau} = a^{\rho} = a, \quad a \in A. \tag{2.3}$$

In particular,

$$A^{\mathfrak{g}} = \text{ the subgroup of fixed points under } \mathfrak{g} = A^2. \tag{2.4}$$

Unlike A the subgroup C is not stable under the action of $\mathfrak{g}$. However, (2.2) shows that

$$\mathfrak{g} \text{ acts trivially on the quotient group } G/A. \tag{2.5}$$

Later we shall find useful the following table on C:

$$\begin{array}{c|cccccc} & 1 & w & wt & tw & t & t^2 \\ \hline \sigma & 1 & w & u^{-1}vwt & uv^2tw & uv^2t & u^{-1}vt^2 \\ \tau & 1 & w & u^2v^2wt & u^2tw & u^2t & u^2v^2t^2 \\ \rho & 1 & v^2w & wt & u^2tw & v^2t & u^2t^2 \end{array} \tag{2.6}$$

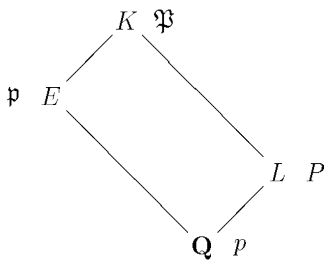
Writing $g = ac, g \in G, a \in A, c \in C$ according to the decomposition $G = A \cdot C$ in (1.3), we have, from (2.4), (2.6):

$$\begin{aligned} g^{\sigma} = g &\iff a^2 = 1 \text{ and } c = 1, w \iff g = a \text{ or } aw, a^2 = 1, \\ g^{\tau} = g &\iff c = 1 \text{ or } w \iff g \in \langle u, v, w\rangle, \\ g^{\rho} = g &\iff c = 1 \text{ or } wt \iff g \in \langle u, v, wt\rangle. \end{aligned} \tag{2.7}$$

3. Generators of decomposition groups.

Notation being as in **2**, for a prime p in $\mathbf{Q}$ let $\mathfrak{P}$ be a prime in $K = \mathbf{Q}(\varepsilon, \theta)$ which divides p. We shall denote by $\mathfrak{g}_p$ the decomposition group of $\mathfrak{P}$, i.e., the the subgroup of $\mathfrak{g} = Gal(K/\mathbf{Q})$ formed by all s $\in \mathfrak{g}$ such that $\mathfrak{P}^s = \mathfrak{P}$. Since $\mathfrak{g}$ is abelian, $\mathfrak{g}_p$ does not depend on the choice of $\mathfrak{P}$. As usual, we write e_p, f_p, for the ramification index, residue class degree, respectively, of p for the extension $K/\mathbf{Q}$; hence $\#\mathfrak{g}_p = e_p f_p$ and $g_p = \#(\mathfrak{g}/\mathfrak{g}_p) =$ the number of distinct prime factors of p in K. It is very important to know generators of $\mathfrak{g}_p$ for each p.

Let $E = \mathbf{Q}(\varepsilon) = \mathbf{Q}(i, \sqrt{2}), L = \mathbf{Q}(\theta) = \mathbf{Q}(\sqrt{\ell^*})$. Then K is the composite of $E, L : K = EL$, and E and L are linearly disjoint over $\mathbf{Q}$.



Suppose $\mathfrak{P}$ divides primes $\mathfrak{p}$, P in E, L, respectively, as the picture shows. From (2.1) we see that L, E correspond to subgroups $\langle \sigma, \tau \rangle, \langle \rho \rangle$, respectively, in the sense of Galois theory. We summarize here the mode of decomposition of p in E and L:

Case $E/\mathbf{Q}$.

p	$e(\mathfrak{p}\|p)$	$f(\mathfrak{p}\|p)$	$g(\mathfrak{p}\|p)$
2	4	1	1
$p \equiv 1 \bmod 8$	1	1	4
$p \equiv 3, 5, 7 \bmod 8$	1	2	2

(3.1)

Case $L/\mathbf{Q}$.

p		$e(P\|p)$	$f(P\|p)$	$g(P\|p)$
ℓ		2	1	1
2	$\ell^* \equiv 1 \bmod 8$	1	1	2
2	$\ell^* \equiv 5 \bmod 8$	1	2	1
p	$(\ell^*/p) = 1$	1	1	2
p	$(\ell^*/p) = -1$	1	2	1

(3.2)

Now, back to the composite $K = EL$, when we fix a prime p of $\mathbf{Q}$, we shall use Z for the decomposition group $\mathfrak{g}_p$ and T for the inertia group for p. Thus, $T = 1$ if and only if $e_p = e(\mathfrak{P}|p) = 1$ and in that case Z is a cyclic group of order $f_p = f(\mathfrak{P}|p)$ generated by the Frobenius automorphism $(K/\mathbf{Q}, p)$. As usual, we denote by K_Z, K_T the corresponding fields in the sense of Galois theory.

To determine the structure of $\mathfrak{g}_p = Z$, we shall consider the three cases separately.
Case 1. $p \neq 2, \ell$.

Since p is unramified in both of E, L by (3.1), (3.2), so is in K; hence $T = 1$, and Z is cyclic. As $\mathfrak{g} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \#Z = 1$ or 2. Now we have

$$\begin{aligned} \#Z = 1 \quad &\Longleftrightarrow \quad \text{p splits completely for K}/\mathbf{Q} \\ &\Longleftrightarrow \quad \text{p splits completely for E}/\mathbf{Q} \text{ and L}/\mathbf{Q} \end{aligned}$$

Therefore, by (3.1), (3.2), we have

$$\#Z = 1 \Longleftrightarrow p \equiv 1 \bmod 8 \text{ and } (\ell^*/p) = 1. \tag{3.3}$$

and hence

$$\#Z = 2 \Longleftrightarrow p \not\equiv 1 \bmod 8 \text{ or } (\ell^*/p) = -1. \tag{3.4}$$

In Case 1, we have $Z = \langle (K/\mathbf{Q}, p) \rangle$ because the Frobenius automorphism is the generator of Z:

$$\mathfrak{g}_p = \langle (K/\mathbf{Q}, p) \rangle, \quad p \neq 2, \ell. \tag{3.5}$$

Conversely, for any $s \in \mathfrak{g}$, with $s^2 = 1$, there is a prime $p \neq 2, \ell$, such that $(K/\mathbf{Q}, p) = s$. Although this follows from Chebotarev density theorem, the following table which results from (2.1), (3.1), (3.2) reveals the Artin reciprocity for $K/\mathbf{Q}$:

p	$\mathfrak{g}_p$
$p \equiv 1 \mod 8, \quad (\ell^*/p) = 1$	1
$p \equiv 1 \mod 8, \quad (\ell^*/p) = -1$	$\langle \rho \rangle$
$p \equiv 5 \mod 8, \quad (\ell^*/p) = 1$	$\langle \tau \rangle$
$p \equiv 5 \mod 8, \quad (\ell^*/p) = -1$	$\langle \tau\rho \rangle$
$p \equiv 3 \mod 8, \quad (\ell^*/p) = 1$	$\langle \sigma\tau \rangle$
$p \equiv 3 \mod 8, \quad (\ell^*/p) = -1$	$\langle \sigma\tau\rho \rangle$
$p \equiv 7 \mod 8, \quad (\ell^*/p) = 1$	$\langle \sigma \rangle$
$p \equiv 7 \mod 8, \quad (\ell^*/p) = -1$	$\langle \sigma\rho \rangle$

(3.6)

Case 2. $p = \ell$.

From (3.1), (3.2), we have $e(\mathfrak{p}|\ell) = e(\mathfrak{P}|P) = 1$, $e(P|\ell) = 2$. Hence $\#T = e_\ell = e(\mathfrak{P}|\ell) = e(\mathfrak{P}|P)e(P|\ell) = 2$. Since the quotient group $\mathfrak{g}_\ell/T$ is cyclic, either $\mathfrak{g}_\ell = T$ or $[\mathfrak{g}_\ell : T] = 2$. Now,

ℓ is unramified for $E/\mathbf{Q} \Longleftrightarrow E \subset K_T \Longleftrightarrow \langle \rho \rangle \supset T$. Comparing orders of $\langle \rho \rangle$ and T, we have

$$T = \langle \rho \rangle. \tag{3.7}$$

Next,

$$\begin{aligned} \ell \equiv 1 \text{ mod } 8 \quad &\Longleftrightarrow \quad \ell \text{ splits completely in E/}\mathbf{Q} \Longleftrightarrow E \subset K_Z \\ &\Longleftrightarrow \quad \langle \rho \rangle \supset \mathfrak{g}_\ell \Longleftrightarrow \langle \rho \rangle = \mathfrak{g}_\ell, \end{aligned}$$

so we have

$$\ell \equiv 1 \text{ mod } 8 \Longleftrightarrow \mathfrak{g}_\ell = T = \langle \rho \rangle. \tag{3.8}$$

Suppose now that $\ell \not\equiv 1$ mod 8. from (3.7) (3.8), we find that $\mathfrak{g}_\ell \supset T = \langle \rho \rangle$ and $\#\mathfrak{g}_\ell = 4$. Let F=$\mathbf{Q}$(i); this field corresponds to $\langle \tau, \rho \rangle$. If $\ell \equiv 5$ mod 8, then

ℓ splits completely in $F/\mathbf{Q} \Longleftrightarrow F \subset K_Z \Longleftrightarrow \langle\tau,\rho\rangle \supset \mathfrak{g}_\ell$, and so we have

$$\ell \equiv 5 \bmod 8 \Longleftrightarrow \mathfrak{g}_\ell = \langle\tau,\rho\rangle. \tag{3.9}$$

Replacing $F = \mathbf{Q}(i)$ by $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-2})$, we get statements like (3.9) for the case of $\ell \equiv 7, 3 \bmod 8$, respectively, and obtain the table:

ℓ	$\mathfrak{g}_\ell$
$\ell \equiv 1 \mod 8$	$\langle\rho\rangle$
$\ell \equiv 3 \mod 8$	$\langle\rho,\sigma\tau\rangle$
$\ell \equiv 5 \mod 8$	$\langle\rho,\tau\rangle$
$\ell \equiv 7 \mod 8$	$\langle\rho,\sigma\rangle$

(3.10)

Case 3. p=2.

From (3.1), (3.2), we have $e(P|2) = e(\mathfrak{P}|\mathfrak{p}) = 1$, $e(\mathfrak{p}|2) = 4$. Hence $\#T = 4 = e_2 = e(\mathfrak{P}|2) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|2) = 4$. Since 2 is unramified for $L/\mathbf{Q}$, we have $L \subset K_T$, i.e., $\langle\sigma,\tau\rangle \supset T$. Compairing orders of $\langle\sigma,\tau\rangle$ and T, we have

$$T = \langle\sigma,\tau\rangle. \tag{3.11}$$

Therefore, either $\mathfrak{g}_2 = T$ or $\mathfrak{g}_2 = \mathfrak{g}$. Next,

$$\begin{aligned} \ell^* \equiv 1 \bmod 8 \quad &\Longleftrightarrow \quad 2 \text{ splits completely in } L/\mathbf{Q} \Longleftrightarrow L \subset K_Z \\ &\Longleftrightarrow \quad \langle\sigma,\tau\rangle \supset \mathfrak{g}_2 \Longleftrightarrow T = \mathfrak{g}_2, \end{aligned}$$

so we obtain the table:

2		$\mathfrak{g}_2$
$\ell^* \equiv 1 \mod 8$	$(\ell \equiv 1, 7 \bmod 8)$	$\langle\sigma,\tau\rangle$
$\ell^* \equiv 5 \mod 8$	$(\ell \equiv 3, 5 \bmod 8)$	$\mathfrak{g}$

(3.12)

Case 4. $p = \infty$

In accordance with the convention, we understand by the decomposition field of $p = \infty$, the maximal real subfield $\mathbf{Q}(\sqrt{2}, \sqrt{\ell})$ of K. As $i^\sigma = -i$, we have

$$\mathfrak{g}_\infty = \langle \sigma \rangle. \tag{3.13}$$

4. The family $H(\ell)$.

Having determined generators of $\mathfrak{g}_p$ ($p = \infty$ inclusive), it is natural to introduce a family $H(\ell)$ and its subfamily $H^*(\ell)$ of subgroups of $\mathfrak{g} = Gal(K/\mathbf{Q})$, $K = \mathbf{Q}(\varepsilon, \theta)$, $\varepsilon = (1+i)/\sqrt{2}$, $\theta = \sqrt{\ell^*}$, as follows.

$$H(\ell) = \{\mathfrak{h} \subset \mathfrak{g}; \quad \mathfrak{h} = \mathfrak{g}_p \text{ for some } p \ (p = \infty \text{ inclusive})\}, \tag{4.1}$$

$$H^*(\ell) = \{\mathfrak{h} \in H(\ell); \ \mathfrak{h} \text{ is maximal }\} \tag{4.2}$$

where $\mathfrak{h}$ is maximal if it is not contained in any group in $H(\ell)$ other than $\mathfrak{h}$ itself. The tables in **3** help us to determine $H(\ell)$. First of all, from (3.6), we see that, for each $\ell, H(\ell)$ contains a subfamily H_0 in common:

$$H_0 = \{1, \langle\sigma\rangle, \langle\tau\rangle, \langle\rho\rangle, \langle\sigma\tau\rangle, \langle\sigma\rho\rangle, \langle\tau\rho\rangle, \langle\rho\tau\sigma\rangle\} \tag{4.3}$$

Next, using (3.10), (3.12), we obtain the following tables:

(4.4)

ℓ	$H(\ell)$
$\ell \equiv 1 \bmod 8$	$H_0, \langle\sigma, \tau\rangle$
$\ell \equiv 3 \bmod 8$	$H_0, \langle\sigma\tau, \rho\rangle, \mathfrak{g}$
$\ell \equiv 5 \bmod 8$	$H_0, \langle\tau, \rho\rangle, \mathfrak{g}$
$\ell \equiv 7 \bmod 8$	$H_0, \langle\sigma\rho\rangle, \langle\sigma\tau\rangle,$

(4.5)

ℓ	$H^*(\ell)$
$\ell \equiv 1 \bmod 8$	$\langle\rho\rangle, \langle\sigma\rho\rangle, \langle\tau\rho\rangle, \langle\sigma\tau\rho\rangle, \langle\sigma, \tau\rangle$
$\ell \equiv 3 \bmod 8$	$\mathfrak{g}$
$\ell \equiv 5 \bmod 8$	$\mathfrak{g}$
$\ell \equiv 7 \bmod 8$	$\langle\tau\rho\rangle, \langle\sigma\tau\rho\rangle, \langle\sigma, \tau\rangle, \langle\sigma, \rho\rangle,$

5. Shafarevich-Tate set for X over Q.

Let $G = \mathrm{Aut}X$ and $\mathfrak{g} = Gal(K/\mathbf{Q})$ as in **1,2**. We remind the reader the definition of the cohomology set $H(\mathfrak{g}, G)$. First, we define a cocycle to be a function $f : \mathfrak{g} \to G$ which satisfies

$$f(st) = f(s)f(t)^s, \quad s, t \in \mathfrak{g}. \tag{5.1}$$

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

$$f'(s) = g^{-1}f(s)g^s. \tag{5.2}$$

The quotient

$$H(\mathfrak{g}, G) = Z(\mathfrak{g}, G)/\sim \tag{5.3}$$

is the cohomology set. $Z(\mathfrak{g}, G)$ contains a distinguished function 1 given by $1(s) = 1$ for all $s \in \mathfrak{g}$ We set

$$B(\mathfrak{g}, G) = \{f \in Z(\mathfrak{g}, G); f \sim 1\}. \tag{5.4}$$

A function f in (5.4) is a coboundary and, by (5.2),

$$f \text{ is a coboundary } \iff f(s) = g^{-1}g^s \text{ for some } g \in G. \tag{5.5}$$

Let $\mathfrak{h}$ be a subgroup of $\mathfrak{g}$. We have the restriction map

$$r_{\mathfrak{h}} : H(\mathfrak{g}, G) \to H(\mathfrak{h}, G) \tag{5.6}$$

induced by $\longmapsto f|\mathfrak{h}$, $f \in Z(\mathfrak{g}, G)$. This mapping sends the distinguished class in $H(\mathfrak{g}, G)$ to the one in $H(\mathfrak{h}, G)$. Hence Ker $r_{\mathfrak{h}}$ makes sense. If $\mathfrak{h}'$ is a subgroup of $\mathfrak{h}$ then we see at once that Ker $r_{\mathfrak{h}} \subset$ Ker $r_{\mathfrak{h}'}$. Therefore, in view of (4.1), (4.2) the following definition of the Shafarevich-Tate set makes sense:

$$Ш(X/\mathbf{Q}) = \bigcap_{\mathfrak{h}\in H(\ell)} \text{Ker } r_{\mathfrak{h}} = \bigcap_{\mathfrak{h}\in H^*(\ell)} \text{Ker } r_{\mathfrak{h}}. \tag{5.7}$$

We have $Ш(X/\mathbf{Q}) = 1$ if $\ell^* \equiv 5 \bmod 8$. (5.8)

Proof. If $\ell^* \equiv 5 \bmod 8$, i.e., if $\ell \equiv 3, 5 \bmod 8$, then $\mathfrak{g} \in H^*(\ell)$ by (4.5). Since $r_{\mathfrak{g}}$ is the identity mapping of $H(\mathfrak{g}, G)$, we find $Ш(X/\mathbf{Q}) = 1$ by the definition (5.7), Q.E.D.

Needless to say, the remaining case where $\ell^* \equiv 1 \bmod 8$ is more interesting. In this case, again by (4.5), we have

$$\begin{aligned} Ш(X/\mathbf{Q}) &= \bigcap_{\mathfrak{h}} \text{Ker } r_{\mathfrak{h}}, \mathfrak{h} = \langle\rho\rangle, \langle\sigma\rho\rangle, \langle\tau\rho\rangle, \langle\sigma\tau\rho\rangle, \langle\sigma,\tau\rangle \\ \text{if } \ell &\equiv 1 \bmod 8 \end{aligned} \tag{5.9}$$

and

$$\begin{aligned} Ш(X/\mathbf{Q}) &= \bigcap_{\mathfrak{h}} \text{Ker } r_{\mathfrak{h}}, \mathfrak{h} = \langle\tau\rho\rangle, \langle\sigma\tau\rho\rangle, \langle\sigma,\tau\rangle, \langle\sigma,\rho\rangle \\ \text{if } \ell &\equiv 7 \bmod 8 \end{aligned} \tag{5.10}$$

Since $\mathfrak{h} = \langle\sigma,\tau\rangle$ is contained in $H(\ell)$ by (4.4), if we take a class [f] $\in Ш(X/\mathbf{Q})$, with $f \in Z(\mathfrak{g}, G)$, we have $f(\sigma) = g^{-1}g^{\sigma}, f(\tau) = g^{-1}g^{\tau}$, $g \in G$. Replacing f by a cocycle equivalent to it using g, we may assume without loss of generality that

$$f(\sigma) = f(\tau) = 1, \quad \text{for any } [f] \in Ш(X/\mathbf{Q}). \tag{5.11}$$

Since $\mathfrak{h} = \langle\rho\rangle$ is contained in $H(\ell)$, we have

$$f(\rho) = g^{-1}g^{\rho} \quad \text{for some } g \in G. \tag{5.12}$$

It is useful to determine explicitly the values (5.12) in A using tables in **2**. By (1.3), write $g = ac, a \in A = \langle u, v\rangle, c \in C = \langle w, t\rangle = S_3$. The $g^{-1}g^{\rho} = c^{-1}c^{\rho}$ by (2.3). By (1.8), (2.6), we have

$$\begin{array}{c|cccccc} c & 1 & w & wt & tw & t & t^2 \\ \hline c^\rho & 1 & v^2w & wt & u^2tw & v^2t & u^2t^2 \\ f(\rho) & 1 & v^2 & 1 & u^2 & u^2 & v^2 \end{array} \tag{5.13}$$

If $f(\rho) = 1$, then $f(\sigma) = f(\tau) = f(\rho) = 1$ and so $f \sim 1$.Next, suppose that $f(\rho) = v^2$. Consider a coboundary defined by $\varphi(s) = w^{-1}w^s$, $s \in \mathfrak{g}$. Then, by (2.2), we have $\varphi(\sigma) = w^{-1}w^\sigma = 1 = f(\sigma), \varphi(\tau) = w^{-1}w^\tau = 1 = f(\tau)$ and $\varphi(\rho) = w^{-1}w^\rho = v^2 = f(\rho)$; hence $f = \varphi \sim 1$, again. The last possibility is:

$$f(\sigma) = f(\tau) = 1, \ f(\rho) = u^2. \tag{5.14}$$

Now, by the definition of the cocycle, we have, from (5.14),

$$f(\tau\rho) = f(\rho\tau) = f(\rho)f(\tau)^\rho = u^2. \tag{5.15}$$

On the other hand, since $\mathfrak{h} = \langle \tau\rho \rangle$ belongs to $H(\ell)$ and $[f] \in Ш(X/\mathbf{Q})$, we must have

$$f(\tau\rho) = x^{-1}x^{\tau\rho}, \text{ for some } x \in G. \tag{5.16}$$

Comparing (5.15), (5.16), we have

$$x^{-1}x^{\tau\rho} = u^2. \tag{5.17}$$

Writing, as usual, $x = ac$, $a \in A = \langle u, v \rangle$, $c \in C = \langle w, t \rangle$, we find $x^1 x^{\tau\rho} = c^{-1}c^{\tau\rho}$ by (2.3). In view of (5.17), we are reduced to solve the following equation in the group $C = S_3$:

$$c^{-1}c^{\tau\rho} = u^2. \tag{5.18}$$

Now, look at the following table similar to (5.13)

$$\begin{array}{c|cccccc} c & 1 & w & wt & tw & t & t^2 \\ \hline c & 1 & v^2w & u^2v^2tw & tw & u^2v^2t & v^2t^2 \\ f(\tau\rho) & 1 & v^2 & u^2v^2 & 1 & v^2 & u^2v^2 \end{array} \tag{5.19}$$

Since u^2 does not appear in the last row, we see that the equation (5.18) has no solutions. Hence the last possibility (5.14) is unreal. Consequently, in view of (5.8), we proved

(5.20) *For the curve* $X : y^4 = x^4 - \ell^2, \ell$ *an odd prime, we have*

$$Ш(X/\mathbf{Q}) = 1.$$

□

(5.21) Remark. The famous quartic $X : x^3y + y^3z + z^3x = 0$ is a smooth curve over $\mathbf{Q}$ with $g = 3$ and $G = \mathrm{Aut}X = PSL_2(\mathbf{F}_7)$, a simple group of order $168 = 2^3 \cdot 3 \cdot 7$. In [3], Klein shows that each automorphism of X is induced by a collineation of $\mathbf{P}^2(\mathbf{C})$ and finds collineations u, v, w in $PGL_3(\mathbf{C})$ which generate G. Three matrices in $GL_3(\mathbf{C})$ inducing u, v, w are described in terms of elements in $K = \mathbf{Q}(\zeta), \zeta$ a primitive 7th root of unity. Since the prime 7 is totally ramified for the absolute cyclotomic extension $K/\mathbf{Q}$, the decomposition group $\mathfrak{g}_7 = \mathfrak{g} = Gal(K/\mathbf{Q})$ and so we obtain $Ш(X/\mathbf{Q}) = 1$ without any effort.

Appendix

Let X be an algebraic variety defined over a number field k of finite degree over $\mathbf{Q}$. The curve $y^4 = x^4 - \ell^2$ is an example of X with $k = \mathbf{Q}$. Another variety Y over k is called a k-twist (or a k-form) of X if Y is isomorphic with X over $\bar{k}$, an algebraic closure of k. Let α be an isomorphism $X \simeq Y$ over $\bar{k}$. Then, for $s \in \mathfrak{g}_k = Gal(\bar{k}/k), \alpha^s$ is also such an isomorphism; and so $f(s) = \alpha^{-1}\alpha^s$ becomes an automorphism of X over $\bar{k} : f(s) \in Aut_{\bar{k}}(X)$. For simplicity we shall set $G = \mathrm{Aut}_{\bar{k}}(X)$. Then, the map f is continuous for the Krull topology on $\mathfrak{g}_k$ and the discrete topology on G with the equation $f(st) = f(s)f(t)^s, s, t \in \mathfrak{g}_k$, i.e., a cocycle of the Galois group $\mathfrak{g}_k$ in the group G. Two cocycles f, f' are equivalent: $f \sim f'$ if there exists $g \in G$ such that $f'(s) = g^{-1}f(s)g^s$, and the quotient set $H(k, G)$ is the cohomology set. Notice that there is a distinguished class in it. Let us denote by $\mathrm{Twist}(X/k)$ the set of all k-twists of X modulo k- isomorphisms. Then, in most cases (e.g. X is quasi projective, i.e. X is isomorphic to a locally closed subvariety of some projective space), the above cocyle induces a bijection:

$$\mathrm{Twist}(X/k) \cong H(k,G). \tag{A.1}$$

When a cocycle $f = f(s)$ comes from $Y \in \mathrm{Twist}(X/k)$ as above, we have the following chain of equivalences showing that the distinguished elements of two sets in (A.1) correspond each other:

$$\begin{aligned}
&f \sim 1 \Longleftrightarrow f(s) = \alpha^{-1}\alpha^s = g^{-1}g^s, g \in G \\
&\Longleftrightarrow g\alpha^{-1} = (g\alpha^{-1})^s, \text{ for all } s \in \mathfrak{g}_k \Longleftrightarrow g\alpha^{-1} \\
&\text{is defined over k } \Longleftrightarrow X \cong Y \text{ over } k.
\end{aligned}$$

Now, for each place v of k, let k_v denote the completion of k at v. We take an algebraic closure $\bar{k}_v$ of k_v and embed $\bar{k}$ in $\bar{k}_v$. For simplicity, put $\mathfrak{g} = \mathfrak{g}_k = Gal(\bar{k}/k)$, $\mathfrak{g}_v = Gal(\bar{k_v}/k_v)$. Since $\bar{k}_v$ is the composite of $\bar{k}$ and k_v over k, $\mathfrak{g}_v$ may be identified with $Gal(\bar{k}/(\bar{k} \cap k_v))$ and we shall consider $\mathfrak{g}_v$ as a subgroup of $\mathfrak{g}$. In this situation, the Shafarevich-Tate set makes sense:

$$\begin{aligned}
Ш(X/k) &\overset{def}{=} Ш(k,G) \\
&= Ker\left\{H(k,G) \to \prod_v H(k_v,G)\right\} \\
&= \{Y; Y \cong X \text{ over } \bar{k} \text{ and over } k_v, \text{for all } v\}
\end{aligned}$$

In particular, the Hasse principle (for twists) means:

$$Ш(X/k) = Ш(k,G) = 1,$$

in other words,

$Y \cong X$ over $\bar{k}$ and k_v for all $v \Longleftrightarrow Y \cong X$ over k.

If the group $\mathfrak{g} = Gal(\bar{k}/k)$ *acts trivially on* G *then* (A.2)
$Ш(X/k) = Ш(k,G) = 1.$

In fact, by the assumption, $\mathfrak{g}$ and $\mathfrak{g}_v$ act on G trivially. Hence the set $Ш(k, G)$ is nothing else than the kernel of the natural map

$$\theta : Hom(\mathfrak{g}, G) \to \prod_v Hom(\mathfrak{g}_v, G).$$

Now take any $\rho \in$ Ker θ. Then there is an open normal subgroup $\mathfrak{h}$ of $\mathfrak{g}$ such that $\rho(\mathfrak{h}) = 1$, and hence $\rho(\mathfrak{g}_v \mathfrak{h}) = 1$ for all v. Call K/k the finite Galois extension corresponding to $\mathfrak{h}$. To $\mathfrak{g}_v \mathfrak{h}$ corresponds the decomposition field of a place w of K which induces v on k. For any $s \in \mathfrak{g}$, put $s^* = s\mathfrak{h} \in \mathfrak{g}/\mathfrak{h} = Gal(K/k)$. By Chebotarev density theorem, we have $t^* s^* (t^*)^{-1} \in Gal(K/(K \cap k_{\mathfrak{p}}))$ for some finite prime $\mathfrak{p}$ of k and $t^* \in Gal(K/k)$. If $t^* = t\mathfrak{h}$ with $t \in \mathfrak{g}$, then $tst^{-1} \in \mathfrak{g}_{\mathfrak{p}}\mathfrak{h}$. Since $\rho(\mathfrak{g}_{\mathfrak{p}}\mathfrak{h}) = 1$, we have $\rho(tst^{-1}) = 1$, and hence $\rho(s) = 1$ for any $s \in \mathfrak{g}$, i.e., θ is injective, Q.E.D.

(A.3) *Let $\mathfrak{h}$ be an open normal subgroup of $\mathfrak{g} = Gal(\bar{k}/k)$ and K/k be a finite Galois extension corresponding to $\mathfrak{h}$. Assume that $\mathfrak{h} = Gal\ (\bar{k}/K)$ acts trivially on G. Then there is a bijection*

$$Ш(k, G) \approx Ш(K/k, G), \textit{ where}$$
$$Ш(K/k, G) = Ker \left\{ H(K/k, G) \to \prod_v H(K_{(v)}/k_v, G) \right\}$$

and $K_{(v)}$ is the field which is the completion of K in $\bar{k}_v$.

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
1 & \to & Ш(K/k, G) & \xrightarrow{\alpha} & Ш(k, G) & \xrightarrow{\beta} & Ш(K, G) \\
 & & \downarrow & & \downarrow & & \\
1 & \to & H(K/k, G) & \xrightarrow{inf} & H(k, G) & \xrightarrow{res} & H(K, G) \\
 & & \downarrow\gamma & & \downarrow\delta & & \\
1 & \to & \prod_v H(K_{(v)}/k_v, G) & \xrightarrow{\varepsilon} & \prod_v (k_v, G) & \to & \prod_w H(K_w, G)
\end{array}$$

where all columns and the middle row are exact, α, inf, ε are injective and K_w is the completion at a place w of K. We shall show that Im α = Ker β. In fact, take

$x \in Ш(K/k, G)$. Then we have $\beta\alpha(x) = res\ \inf(x) = 1$ and hence $\mathrm{Im}\ \alpha \subset \mathrm{Ker}\ \beta$. Next, take $y \in \mathrm{Ker}\ \beta \subset \mathrm{Ker}(res)$. Then $y = \inf(x)$ for some $x \in H(K/k, G)$. It then follows that $1 = \delta(y) = \delta\ \inf(x) = \varepsilon\gamma(x)$. Since ε is injective, we have $\gamma(x)=1$, i.e., $x \in Ш(K/k, G)$ which shows that $\mathrm{Ker}\ \beta \subset \mathrm{Im}\ \alpha$. Now, as $Ш(K, G) = 1$ by (A.2), the relation $\mathrm{Im}\ \alpha = \mathrm{Ker}\ \beta$ means that α is surjective, which proves our assertion.

Let X be, as before, a quasi projective variety defined over a number field k. *Assume that there is a finite Galois extension K/k so that $G = \mathrm{Aut}_{\bar{k}}(X) = \mathrm{Aut}_K(X)$*, i.e., *every $\bar{k}$-automorphism of X is a K-automorphism.* This is certainly the case of our curve (1.1) with $k = \mathbf{Q}, K = \mathbf{Q}(\varepsilon, \theta)$. In accordance with notation in the text, put $\mathfrak{g} = Gal(K/k)$, $\mathfrak{g}_\mathfrak{p}$ =the decomposition group of a prime $\mathfrak{P}$ in K which lies above a prime $\mathfrak{p}$ in k.‡ As in **4**, we introduce a family $H(K/k)$ and its subfamily $H^*(K/k)$ of subgroups of $\mathfrak{g} = Gal(K/k)$ as follows.

$$\begin{aligned} H(K/k) &= \{\mathfrak{h} \subset \mathfrak{g}; \mathfrak{h} = \mathfrak{g}_\mathfrak{p} \text{ for some } \mathfrak{p}\ (\mathfrak{p}|\infty \text{ inclusive})\} \\ H^*(K/k) &= \{\mathfrak{h} \in H(K/k); \mathfrak{h} \text{ maximal}\}. \end{aligned} \tag{A.4}$$

For a subgroup $\mathfrak{h}$ of $\mathfrak{g}$, we have the restriction map $r_\mathfrak{h}\colon\ H(\mathfrak{g}, G) \to H(\mathfrak{h}, G)$. If $\mathfrak{h}'$ is a subgroup of $\mathfrak{h}$, then we see that $\mathrm{Ker}\ r_\mathfrak{h} \subset \mathrm{Ker}\ r_{\mathfrak{h}'}$. By (A.4), we can speak of the Shafarevich-Tate set

$$Ш(X/k) = \bigcap_{\mathfrak{h} \in H(K/k)} \mathrm{Ker}\ r_\mathfrak{h} = \bigcap_{\mathfrak{h} \in H^*(K/k)} \mathrm{Ker}\ r_\mathfrak{h}. \tag{A.5}$$

In view of (A.3), (A.4) and (A.5), the two modes of defining the Shafarevich-Tate set $Ш(X/k)$ coincide with each other.

For a prime $\mathfrak{p}$ in k, set

$$P_\mathfrak{p} = \{\mathfrak{P};\ \text{prime in } K \text{ dividing } \mathfrak{p}\}. \tag{A.6}$$

‡ We include as a prime $\mathfrak{p}$ the one at infinity in k. I beg of readers to be generous with a crash of notation $\mathfrak{g}, \mathfrak{g}_\mathfrak{p}$, occuring above in Appendix. Since the conjugacy of subgroups of $\mathfrak{g}$ does not affect the cohomology, we can use the notation $\mathfrak{g}_\mathfrak{p}$ safely.

The finite group $\mathfrak{g} = Gal(K/k)$ acts on this finite set. We see that $\mathfrak{g}$ has a fixed point in $P_{\mathfrak{p}}$ if and only if $H^*(K/k) = \{\mathfrak{g}\}$. Now, assuming that K is a field of rationality for $G = \mathrm{Aut}_{\bar{k}}(X)$, we obtain, from (A.5), an inexpensive theorem

(A.7) (Hasse principle for X/k). *Let X be a quasi projective variety over k, G the group of automorphisms of X over $\bar{k}$. Assume that there is a finite Galois extension K/k so that every element of G is defined over K. If, for a prime $\mathfrak{p}, \mathfrak{g} = Gal(K/k)$ has has a fixed point in the set* (A.6), *then the Shafrarevich-Tate set* $\text{Ш}(X/k) = 1$.

(A.8) Remark. The statement (5.8) for our curve $X : y^4 = x^4 - \ell^2$ is a (very) special case of (A.7). On the other hand, (5.20) is not a consequence of (A.7). $\square$

References

[1] Cassels, J. W. S and Fröhlich, A, eds., Algebraic Number Theory, Academic Press, London-New York, 1990.

[2] Farkas, H. M. and Kra, I., Riemann Surfaces, Springer-Verlag, New York-Heidelberg-Berlin, 1980.

[3] Klein, F., Über die Transformation siebenter Ordnung elliptischen Funktionen, Math. Ann.14, (1878/79), 428-471 (=Klein, F., Gesammelte Mathematische Abhandlungen, vol. III, Springer, Berlin, 1923, 90-135).

Takashi Ono
Department of Mathematics
The Johns Hopkins University
Baltimore MD.21218 USA

Received 15.01.1998