A note on Shafarevich-Tate sets for finite groups

By Takashi ONO

Department of Mathematics, The Johns Hopkins University, U. S. A.

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1998)

1. A problem. Let K/k be a finite Galois extension of number fields and $\mathfrak{g}$ be the Galois group: $\mathfrak{g} = \mathrm{Gal}(K/k)$. For a prime $\mathfrak{P}$ in K, we denote by $\mathfrak{g}_{\mathfrak{P}}$ the decomposition group of $\mathfrak{P}$ for K/k: $\mathfrak{g}_{\mathfrak{P}} = \{s \in \mathfrak{g}\,;\, \mathfrak{P}^s = \mathfrak{P}\}$[1]. Let G be a left $\mathfrak{g}$-group.[2] A cocycle is a map $f : \mathfrak{g} \to G$ which satisfies

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

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

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

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

(1.3) $\quad H(\mathfrak{g}, G) = Z(\mathfrak{g}, G)/\sim$

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

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

Since a decomposition group $\mathfrak{g}_{\mathfrak{P}}$ is a subgroup of $\mathfrak{g}$, we have the restriction map

(1.5) $\quad r_{\mathfrak{P}} : H(\mathfrak{g}, G) \to H(\mathfrak{g}_{\mathfrak{P}}, G)$

induced by $f \mapsto f|\mathfrak{g}_{\mathfrak{P}}$, $f \in Z(\mathfrak{g}, G)$. This map sends the distinguished class in $H(\mathfrak{g}, G)$ to the one in $H(\mathfrak{g}_{\mathfrak{P}}, G)$. Hence Ker $r_{\mathfrak{P}}$ makes sense. One finds easily that Ker $r_{\mathfrak{P}}$ depends only on a prime $\mathfrak{p}$ in k lying below $\mathfrak{P}$ because if $\mathfrak{P}' \mid \mathfrak{P}$ then $\mathfrak{P}' = \mathfrak{P}^t$ for some $t \in \mathfrak{g}$ and $\mathfrak{g}_{\mathfrak{P}}' = t\mathfrak{g}_{\mathfrak{P}}t^{-1}$ which implies that ker $r_{\mathfrak{P}} =$ Ker $r_{\mathfrak{P}}'$.[3] Therefore, the Shafarevich-Tate set:

(1.6) $\quad Ш(K/k, G) = \bigcap_{\mathfrak{p}} \mathrm{Ker}\, r_{\mathfrak{p}}$

makes sense.

(1.7) **Problem.** *Given a Galois extension K/k and a $\mathfrak{g}$-group G, $\mathfrak{g} = \mathrm{Gal}(K/k)$, study the set* $Ш(K/k, G)$.

(1.8) **Remark.** (i) We shall call an extension K/k *trivial* if $\mathfrak{g} = \mathfrak{g}_{\mathfrak{P}}$ for some $\mathfrak{P}$ in K. When that is so, we have $Ш(K/k, G) = 1$, i.e. the Hasse principle holds for $(K/k, G)$ for any $\mathfrak{g}$-group G. For example, every cyclic extension K/k is trivial since any generator s of $\mathfrak{g}$ can be a Frobenius automorphism for some $\mathfrak{P}$, $s = (K/k, \mathfrak{P})$, by Chebotarev theorem. As an example of K/k which is trivial but not cyclic, we think of the case $k = \boldsymbol{Q}$, $K = \boldsymbol{Q}(\zeta_t)$, $\zeta_t = \exp(2\pi i/2^t)$, $t \geq 3$; here we have $\mathfrak{g} = \mathfrak{g}_{\mathfrak{P}}$ for $\mathfrak{P} \mid 2$, because 2 is totally ramified in K. In **2** we shall study the relative cyclotomic field $K = k(\zeta_t)$ with $k = \boldsymbol{Q}(\sqrt{\ell})$, ℓ an odd prime, and show, among others, that $\# Ш(K/k, G) = 2$ if $t = 3$ and $\ell \equiv 7 \bmod 8$, $G = \langle \zeta_t \rangle$.

(ii) As another trivial case, let us mention that $Ш(K/k, G) = 1$ for any extension K/k and G, if $\mathfrak{g}$ acts trivially on G. This follows again from Chebotarev theorem, because $H(\mathfrak{g}, G) = \mathrm{Hom}(\mathfrak{g}, G)$, $H(\mathfrak{g}_{\mathfrak{P}}, G) = \mathrm{Hom}(\mathfrak{g}_{\mathfrak{P}}, G)$ and $\mathfrak{g} = \bigcup_{t, \mathfrak{P}} t\mathfrak{g}_{\mathfrak{P}}t^{-1}$, $t \in \mathfrak{g}$.

2. An example. As announced in (1.8), (i), we shall consider the Galois extension $K = k(\zeta_t)$, $\zeta_t = \exp(2\pi i/2^t)$, $t \geq 3$, $k = \boldsymbol{Q}(\sqrt{\ell})$, ℓ an odd prime. Let $\mathfrak{P}$ be as before a prime in K and $\mathfrak{p}$ be the one in k such that $\mathfrak{P} \mid \mathfrak{p}$. Since K/k is abelian, we can use $\mathfrak{g}_{\mathfrak{p}}$ instead of $\mathfrak{g}_{\mathfrak{P}}$ for the decomposition subgroup at $\mathfrak{P}$ of $\mathfrak{g} = \mathrm{Gal}(K/k)$. Furthermore, we shall set $F = \boldsymbol{Q}(\zeta_t)$. Let P, p be primes in F, $\boldsymbol{Q}$, respectively, both lying under the prime $\mathfrak{P}$ in K. We have $[k : \boldsymbol{Q}] = [K : F] = 2$, $[F : \boldsymbol{Q}] = [K : \boldsymbol{Q}] = 2^{t-1}$. Note that $\mathfrak{g} = \mathrm{Gal}(K/k) \cong \mathrm{Gal}(F/\boldsymbol{Q}) \cong \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2^{t-2}\boldsymbol{Z}$ which is not cyclic. Now if $p \neq 2$, then $e(P \mid p) = 1$ and so $e(\mathfrak{P} \mid \mathfrak{p}) = 1$; hence $\mathfrak{g}_{\mathfrak{p}} = \langle (K/k, \mathfrak{P}) \rangle \neq \mathfrak{g}$.[4] So we have the following lemma:

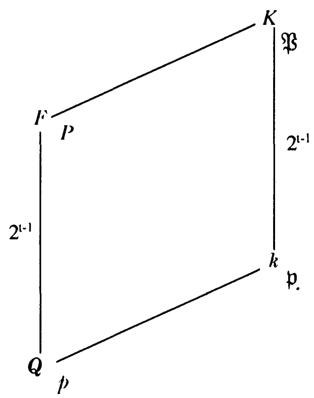
---

1) By a prime we include one at infinity as usual; in this work, however, such a prime does not play any significant role.

2) If $s \in \mathfrak{g}$ and $a \in G$, then the action of s on a will be denoted by sa or a^s, interchangeably. Note that $(a^t)^s = a^{(st)}$ because $s(ta) = (st)a$.

3) For $s \in \mathfrak{g}_{\mathfrak{P}}$, let $s' = tst^{-1} \in \mathfrak{g}_{\mathfrak{P}}'$. If $f(s) = a^{-1}a^s$, $f \in \mathrm{Ker}\, r_{\mathfrak{P}}$, then, $f(s') = a'^{-1}a'^{s'}$ with $a' = a^t f(t)^{-1}$.

4) We use standard notation like $e(\mathfrak{P} \mid \mathfrak{p})$, $f(\mathfrak{P} \mid \mathfrak{p})$ in Hilbert theory of Galois extensions.



(2.1) **Lemma.** *K/k is trivial $\Leftrightarrow \mathfrak{g}_{\mathfrak{p}} = \mathfrak{g}$ for some $\mathfrak{p} \mid 2$.*[5)]

(2.2) **Lemma.** *If $\ell \equiv 1 \bmod 4$, then K/k is trivial.*

In fact, since $e(\mathfrak{p} \mid 2) = 1$, we have $e(\mathfrak{P} \mid P) = 1$, so $e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid 2) = e(\mathfrak{P} \mid P)\, e(P \mid 2) = 2^{t-1} = [K : k]$, and hence $\mathfrak{g}_{\mathfrak{p}} = \mathfrak{g}$.

Q.E.D.

To proceed further, we need the following lemma which is a special case of a theorem on decomposition of primes in a Kummer extension of prime relative degree.[6)]

(2.3) **Lemma.** *Let F be a number field, ℓ a prime $\neq 2$ such that $\sqrt{\ell} \notin F$. Let $\mathfrak{P}$ be a prime ideal in $K = F(\sqrt{\ell})$ and P be the one in F such that $\mathfrak{P} \mid P$. Assume that $P^a \parallel 2$ with $a > 0$. Then we have*

(i) $P = \mathfrak{P}\mathfrak{P}'$, $\mathfrak{P} \neq \mathfrak{P}'$, *if* $[\ell, P^{2a+1}] = +1$,

(ii) $P = \mathfrak{P}$, *if* $[\ell, P^{2a+1}] = -1$ *but* $[\ell, P^{2a}] = +1$,

(iii) $P = \mathfrak{P}^2$, *if* $[\ell, p^{2a}] = -1$.[7)]

Applying (2.3) to our situation where $F = \boldsymbol{Q}(\zeta_t)$, $\mathfrak{P} \mid 2$, $a = 2^{t-1}$, we obtain the rule of decomposition of primes for the quadratic extension K/F:

$$(2.4)\quad \begin{cases} \text{(i) } e(\mathfrak{P} \mid P) = f(\mathfrak{P} \mid P) = 1 \quad \text{if } [\ell, P^{2^t+1}] = +1, \\ \text{(ii) } e(\mathfrak{P} \mid P) = 1,\ f(\mathfrak{P} \mid P) = 2 \\ \quad \text{if } [\ell, P^{2^t+1}] = -1 \quad \text{but } [\ell, P^{2^t}] = +1, \\ \text{(iii) } e(\mathfrak{P} \mid P) = 2,\ f(\mathfrak{P} \mid P) = 1 \quad \text{if } [\ell, P^{2^t}] = -1. \end{cases}$$

Now, suppose that $\ell \equiv 3 \bmod 4$. Then $e(\mathfrak{p} \mid 2) = 2$. Hence $e(\mathfrak{P} \mid 2) = e(\mathfrak{P} \mid \mathfrak{p})\, e(\mathfrak{p} \mid 2) = 2e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid P)\, e(P \mid 2) = 2^{t-1} e(\mathfrak{P} \mid P)$; and so

(2.5) $e(\mathfrak{P} \mid \mathfrak{p}) = 2^{t-2} e(\mathfrak{P} \mid P)$, if $\ell \equiv 3 \bmod 4$.

In the case (2.4), (iii), since $e(\mathfrak{P} \mid P) = 2$, we have $e(\mathfrak{P} \mid \mathfrak{p}) = 2^{t-1} = [K : k]$, and so $\mathfrak{g}_{\mathfrak{p}} = \mathfrak{g}$, i.e. K/k is trivial. On the other hand, in the case (2.4), (ii), since $e(\mathfrak{P} \mid P) = 1$, we have $e(\mathfrak{P} \mid \mathfrak{p}) = 2^{t-2}$. As for $f(\mathfrak{P} \mid \mathfrak{p})$, since $f(\mathfrak{P} \mid 2) = f(\mathfrak{P} \mid \mathfrak{p}) f(\mathfrak{p} \mid 2) = f(\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{P} \mid P) f(P \mid 2) = f(\mathfrak{P} \mid P)$ and $f(\mathfrak{P} \mid P) = 2 = f(\mathfrak{P} \mid \mathfrak{p})$, we have $\# \mathfrak{g}_{\mathfrak{p}} = e(\mathfrak{P} \mid \mathfrak{p}) f(\mathfrak{P} \mid \mathfrak{p}) = 2^{t-1} = [K : k]$, and so $\mathfrak{g}_{\mathfrak{p}} = \mathfrak{g}$, i.e. K/k is trivial, again. Therefore we obtain:

(2.6) **Lemma.** *If $\ell \equiv 3 \bmod 4$ and $[\ell, p^{2^t+1}] = -1$ (i.e. the case (2.4), (ii), (iii)), then K/k is trivial.*

Now it remains to consider the last case (2.4), (i); $\ell \equiv 3 \bmod 4$, and $[\ell, P^{2^t+1}] = 1$. In this case, by (2.5), we have $e(\mathfrak{P} \mid \mathfrak{p}) = 2^{t-2}$, and $f(\mathfrak{P} \mid 2) = f(\mathfrak{P} \mid \mathfrak{p}) f(\mathfrak{p} \mid 2) = f(\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{P} \mid P) f(P \mid 2) = 1$; hence $\# \mathfrak{g}_{\mathfrak{p}} = e(\mathfrak{P} \mid \mathfrak{p}) f(\mathfrak{P} \mid \mathfrak{p}) = 2^{t-2} < 2^{t-1} = \# \mathfrak{g}$, so $\mathfrak{g}_{\mathfrak{p}} \neq \mathfrak{g}$ i.e. K/k is not trivial in view of (2.1). Summarizing all arguments above, we have proved:

(2.7) **Theorem.** *Let K/k be the relative cyclotomic extension defined by $k = \boldsymbol{Q}(\sqrt{\ell})$, ℓ an odd prime, $K = k(\zeta_t)$, ζ_t a 2^t-th root of unity, $t \geq 3$. Then K/k is not trivial (in the sense of (1.8), (i)) if and only if $\ell \equiv 3 \bmod 4$ and the congruence $x^2 \equiv \ell \bmod (1 - \zeta_t)^{2^t+1}$ has a solution in the ring of integers of $\boldsymbol{Q}(\zeta_t)$.*

In order to get a counter example to the Hasse principle, i.e. to get a pair $(K/k, G)$ with $Ш(K/k, G) \neq 1$, we need to start with an extension K/k which is not trivial and then to search for a group G. To do this, let us assume $t = 3$ in (2.7) and solve the congruence

(2.8) $x^2 \equiv \ell \bmod 4P$, $P = (1 - \zeta_3)$,
$\ell \equiv 3 \bmod 4$,

where we used that $2^t + 1 = 9$, $2 = P^4$ and $P^9 = 4P$. Now, let $\ell \equiv 7 \bmod 8$. Then $\ell^2 \equiv 1 \bmod 16$. If we put $x = (\ell + 1 + (\ell - 1)i)/2$, then $x^2 - \ell = (\ell^2 - 1)i/2 \equiv 0 \bmod 4P$ because $4(1 - \zeta)(1 + \zeta - \zeta^2 - \zeta^3) = -8i$, where $\zeta = \zeta_3 = (1 + i)/\sqrt{2}$.

Having found that the extension K/k with $k = \boldsymbol{Q}(\sqrt{\ell})$, $\ell \equiv 7 \bmod 8$, $K = k(\zeta) = k(i, \sqrt{2})$, is not trivial, it is natural to examine the group

5) Note that, for $\mathfrak{p} \mid \infty$, $\mathfrak{g}_{\mathfrak{p}}$ is cyclic (of order at most 2).

6) See Satz 119 of [1] §39.

7) For a positive integer b, we set

$$[\ell, P^b] = \begin{cases} +1, & \text{if } x^2 \equiv \ell \bmod P^b \text{ has a solution in } \mathfrak{o}_F, \\ -1, & \text{otherwise.} \end{cases}$$

$G = \langle \zeta \rangle$ on which $\mathfrak{g} = \mathrm{Gal}(K/k)$ acts canonically. This time, $\mathfrak{g} = \langle \sigma, \tau \rangle = \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$, and the action is given by

(2.9) $\qquad \zeta^{\sigma} = \zeta^{-1} = \bar{\zeta},\ \zeta^{\tau} = \zeta^{5}.$

Since K/k is not trivial the family $\mathfrak{H} = \{\mathfrak{g}_{\mathfrak{p}}\}$ is simply that of all cyclic subgroups of $\mathfrak{g}$; $\mathfrak{H} = \{\langle 1 \rangle, \langle \sigma \rangle, \langle \tau \rangle, \langle \sigma\tau \rangle\}$. Let $[f]$ be an element of $\text{Ш}(K/k, G) \subset H(\mathfrak{g}, G)$. Since each $f(s)$, $s \in \mathfrak{g}$, is of the form $a(s)^{-1}a(s)^{s}$, $a(s) \in G$, on replacing f by a cocycle equivalent to it using $a(\sigma)$, we may assume that

(2.10) $\qquad f(\sigma) = 1,\ f(\tau) = a^{-1}a^{\tau}.$

Write $a = \zeta^{\alpha}$, $0 \leq \alpha \leq 7$. Then $f(\tau) = (\zeta^{-1}\zeta^{5})^{\alpha} = (\zeta^{4})^{\alpha} = (-1)^{\alpha} = \pm 1$. So there are only two possibilities for f. The one with $f(\tau) = 1$ is of course the constant function $f = 1$; the other one with $f(\tau) = -1$ can be realized by setting

(2.12) $\quad f(\sigma) = 1,\ f(\tau) = \zeta^{-1}\zeta^{\tau},\ f(\sigma\tau) = i^{-1}i^{\sigma\tau}.$

Moreover, this $f \not\sim 1$. Because, if there were a $b \in G$ such that $f(\sigma) = b^{-1}b^{\sigma}$, $f(\tau) = b^{-1}b^{\tau}$, then we would have $1 = f(\sigma) = b^{-1}\bar{b}$ which implies that $b = \pm 1$, but then $-1 = f(\tau) = b^{-1}b^{\tau} = 1$, a contradiction. Consequently, we have proved:

(2.13) *When* $\ell \equiv 7 \bmod 8$, $k = \boldsymbol{Q}(\sqrt{\ell})$, $K = k(\zeta)$, $G = \langle \zeta \rangle$, $\zeta = \exp(\pi i/4)$, *the set* $\text{Ш}(K/k, G)$ (*with the natural action of* $\mathfrak{g} = \mathrm{Gal}(K/k)$ *on* G) *consists of two elements*; *the nontrivial cocycle is given by* (2.12).

3. Correction to [2]. We take this opportunity to point out that (0.1) Theorem in [2] is incorrect as it stands. Let k be a number field, a a nonzero number in k and n an integer ≥ 1. The erroneous statement is:

(3.1) *The equation* $x^{n} = a$ *has a solution* x *in* k *if and only if it has a solution* x_v *in* k_v *for every place* v *of* k.

First, let us translate (3.1) into the language of the Shafarevich-Tate sets. Let μ_n be the group of nth roots of unity in $\bar{k}$. Passing to the cohomology sequence of the short exact sequence

$$1 \to \mu_n \to \bar{k}^{\times} \xrightarrow{n} \bar{k}^{\times} \to 1$$

of $\mathrm{Gal}(\bar{k}/k)$-modules, we have

$$\cdots k^{\times} \to k^{\times} \to H^{1}(k, \mu_n) \to H^{1}(k, \bar{k}^{\times}) = 1$$

by Hilbert theorem 90. Hence we get an isomorphism

(3.2) $\quad k^{\times}/k^{\times n} \cong H^{1}(k, \mu_n)$, (similarly for k_v).

The Shafarevich-Tate group of μ_n (in Galois cohomology) is

(3.3) $\quad \text{Ш}(k, \mu_n) = \mathrm{Ker}\,(H^{1}(k, \mu_n) \to \prod_v H^{1}(k_v, \mu_n)).$

From (3.2), (3.3), we find

(3.4) $\qquad (3.1) \Leftrightarrow \text{Ш}(k, \mu_n) = 1.$

Let $K = k(\mu_n)$, the relative nth cyclotomic field over k. Then it can be shown that

(3.5) $\qquad \text{Ш}(k, \mu_n) \cong \text{Ш}(K/k, \mu_n)$

where the set on the right hand side is the one in (1.6).[8] Hence, by (3.4), (3.5), we get

(3.6) $\qquad (3.1) \Leftrightarrow \text{Ш}(K/k, \mu_n) = 1.$

Now (2.13) shows that the set on the right hand side contains two elements when $n = 8$, $k = \boldsymbol{Q}(\sqrt{\ell})$, ℓ a prime $\equiv 7 \bmod 8$. Consequently, (3.1) is erroneous: The equation $x^{8} = 16$ in k gives a counter example. In [2] we overlooked the case where K/k can be nontrivial (in the sense of (1.8)) though $\boldsymbol{Q}(\mu_n)/\boldsymbol{Q}$ is trivial.

On the other hand, (0.6) in [2] (Hasse principle for elliptic curves over k) is correct because only $n = 2, 4, 6$, occur there and, in these cases, K/k's are all trivial.

8) See, e.g. Appendix of [3], especially (A.3), (A.5).

References

[1] E. Hecke: Vorlesungen über die Theorie der algebraischen Zahlen. Chelsea, New York (1970).

[2] T. Ono and T. Terasoma: On Hasse principle for $x^{n} = a$. Proc. Japan Acad., **73A**, 143–144 (1997).

[3] T. Ono: Shafarevich-Tate set for $y^{4} = x^{4} - \ell^{2}$ (to appear).