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.