"Shafarevich-Tate sets" for profinite groups

By Takashi Ono

Department of Mathematics, The Johns Hopkins University, Baltimore, MD 21218, U.S.A.

(Communicated by Shokichi Iyanaga, M.J.A., June 15, 1999)

1. Ш(*G*) for a topological group *G*. Let G be a topological group. By a cocycle of G we mean a continuous map $f : G \to G$ such that

$$f(st) = f(s)f(t)^s, \text{ with } a^s = sas^{-1}, \quad s, t \in G,\ a \in G. \tag{1.1}$$

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

$$f(s) = a^{-1}f'(s)a^s,\ s \in G. \tag{1.2}$$

Cocycles f, f' are *locally equivalent*, written $f \underset{\text{loc}}{\sim} f'$, if there is an $a_s \in G$ for each $s \in G$ such that

$$f(s) = {a_s}^{-1}f'(s){a_s}^s. \tag{1.3}$$

Two subsets $B(G)$, $B_{\text{loc}}(G)$ of $Z(G)$ are defined by

$$B(G) = \{f \in Z(G); f \sim 1\}, \quad B_{\text{loc}}(G) = \{f \in (Z(G)); f \underset{\text{loc}}{\sim} 1\}, \tag{1.4}$$

respectively, where 1 denotes the constant function on G of value 1_G. A cocycle in $B(G)$ is a coboundary and one in $B_{\text{loc}}(G)$ is a local coboundary. Clearly a coboundary is a local cobundary : $B(G) \subset B_{\text{loc}}(G)$. The S–T set Ш$(G)$ is the quotient of $B_{\text{loc}}(G)$ with respect to the equivalence (1.2). $B(G)$ forms a distinguished point in Ш(G). When Ш$(G) = 1$, i.e. $B_{\text{loc}}(G) = B(G)$, we say that G enjoys the "Hasse principle".

2. *Z*(*G*) and End(*G*). Let G be a topological group and End(G) the semigroup of continuous homomorphisms of G into G. I owe M. Mazur an excellent idea of associating an $F \in \text{End}(G)$ to each $f \in Z(G)$ by

$$F(s) = f(s)s,\ s \in G. \tag{2.1}$$

It is easy to verify that the map $f \mapsto F$ is a bijection

$$\mu : Z(G) \xrightarrow{\sim} \text{End}(G), \tag{2.2}$$

and $Z(G)$ becomes a semigroup with the multiplication

$$f * f'(s) = f(f'(s)s)f'(s), \quad f, f' \in Z(G). \tag{2.3}$$

The equivalence in End(G) corresponding to the one in (1.2) turns out to be

$$F \sim F' \iff F(s) = a^{-1}F'(s)a,\ a \in G. \tag{2.4}$$

In particular, to a coboundary $f(s) = a^{-1}a^s$ corresponds the inner automorphism $F(s) = a^{-1}sa$. In other words, the map (2.2) induces a bijection

$$B(G) \xrightarrow{\sim} \text{Inn}(G) \tag{2.5}$$

and $B(G)$ becomes a group.
Similarly, another equivalence in End(G) corresponding to the local equivalence (1.3) turns out to be

$$F \underset{\text{loc}}{\sim} F' \iff F(s) = {a_s}^{-1}F'(s)a_s \iff F(s) \sim F'(s), \text{ the (pointwise) conjugacy in } G. \tag{2.6}$$

In particular, to a local coboundary $f(s) = {a_s}^{-1}{a_s}^s$ corresponds an endomorphism F such that $F(s) \sim s$. In other words, the map (2.2) induces a bijection

$$B_{\text{loc}}(G) \xrightarrow{\sim} \text{End}_c(G) \tag{2.7}$$

where the right hand side is the set of $F's$ such that $F(s) \sim s$, i.e., the set of endomorphisms which preserve conjugacy classes of G. It should be noted that every F in End$_c(G)$ is injective but not surjective in general. Denoting by i_a the inner automorphism of G such that $i_a(s) = asa^{-1}$, we have, for $F, F' \in \text{End}_c(G)$,

$$F \sim F' \iff F'(s) = aF(s)a^{-1} \iff F' = i_aF,\ a \in G. \tag{2.8}$$

Consequently, we obtain a bijection

$$\text{Ш}(G) \approx B(G) \setminus B_{\text{loc}}(G) \approx \text{Inn}(G) \setminus \text{End}_c(G). \tag{2.9}$$

Let Aut(G) be the group of automorphisms of G. Set

$$\text{Aut}_c(G) = \text{Aut}(G) \cap \text{End}_c(G) \tag{2.10}$$

the subgroup of Aut(G) preserving conjugacy classes of G. Therefore if the condition

(♯) *every F in* End$_c(G)$ *is surjective and F^{-1} is continuous* holds, then (2.9) turns out to be

$$\text{(2.11)} \qquad Ш(G) \approx \mathrm{Aut}_c(G)/\mathrm{Inn}(G).$$

In other words, under (♯), the S-T set obtains a structure of a group.

(2.12) Finite groups. For a finite group G, the condition (♯) holds obviously. Hence, by (2.11), the determination of $Ш(G)$ boils down to a typical problem of that of the quotient group $\mathrm{Aut}_c(G)/\mathrm{Inn}(G)$. In particular, if $\mathrm{Aut}(G) = \mathrm{Inn}(G)$, then $Ш(G) = 1$, i.e., G enjyoys the Hasse principle. This is, for example, the case $G =$ the Monster ([1]). Recently, K. Harada informed me that he has checked $Ш(G) = 1$ for all 26 sporadic simple groups and alternating simple groups. It would be interesting if one proves $Ш(G) = 1$ for all simple groups without using the classification. As for some results on (finite or infinite) linear groups, see [6], [10].

(2.13) Free groups. Let G be a free group F_r of rank r. We consider G as a discrete group. This time, we use the bijection (2.9) the other way around. Namely, since we know that $Ш(F_r) = 1$ (see [7]), it follows from (2.9) a result on F_r, i.e., $\mathrm{End}_c(F_r) = \mathrm{Aut}_c(F_r) = \mathrm{Inn}(F_r)$, an interesting property of free groups. It is to be noted that $Ш(\overline{\varGamma}(N)) = 1$ for all $N \geq 1$ since $\overline{\varGamma}(N)$ are all free for $N \geq 2$ (cf. [3], p.362, 3D) and $Ш(\overline{\varGamma}(1)) = Ш(PSL_2(\mathbf{Z})) = 1$ by [6].

3. Profinite groups. Let G be a profinite group, i.e., a topological group wihch is compact and totally disconnected. We shall use repeatedly the property that in G every neighborhood of 1 contains an open normal subgroup. In order to check the condition (♯) above for G, it is enough to show that F is surjective because the continuity of F^{-1} follows from the compactness. For an $F \in \mathrm{End}_c(G)$, let t_0 be any point of G. We shall find an s_0 so that $F(s_0) = t_0$. So let N be any open normal subgroup of G. If $t \in N$, then since $F(t) \sim t$, we have $F(t) \in N$. Therefore F induces an endomorphism $F_N : G/N \to G/N$ such that $F_N(sN) = F(s)N$, $s \in G$. If $F_N(sN) = N$, then $F(s)N = N$ which implies that $s \sim F(s) \in N$, hence $s \in N$. Thus F_N is an automorphism of the finite group G/N. Call s_N an element of G such that $F_N(s_N N) = t_0 N$. Then we have $t_0 \in F(s_N)N$. Since G is compact, there is an element s_0 so that $s_N \to s_0$ when $N \to 1$. Then we have $F(s_0) = t_0$. So we proved

(3.1) Theorem. *Let G be a profinite group, then there is a bijection*

$$Ш(G) \approx \mathrm{Aut}_c(G)/\mathrm{Inn}(G).$$

In particular, $Ш(G)$ gets a group structure.

Now let K be a finite Galois extension over $\mathbf{Q}$ and $G_K = \mathrm{Gal}(\bar{\mathbf{Q}}/K)$. Then celebrated results due to Neukirch, Ikeda, Iwasawa and Uchida (cf. [4], [2], and [11]) tell us that us that there is an isomorphism

$$\text{(3.2)} \qquad \mathrm{Aut}(G_K)/\mathrm{Inn}(G_K) \approx \mathrm{Gal}(K/\mathbf{Q}).$$

Combining (3.1), (3,2) we see that the S-T group $Ш(G_K)$ can be embedded in the finite group $\mathrm{Gal}(K/\mathbf{Q})$. In particular, $Ш(G_{\mathbf{Q}}) = 1$, i.e., the full Galois group $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ enjoys the Hasse principle.

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson: An ATLAS of Finite Groups. Clarendon Press, Oxford (1985).

[2] M. Ikeda: Completeness of the absolete Galois group of the rational numbr field. J. Reine Angew. Math., **291**, 1–22 (1977).

[3] J. Lehner: Discontinuous groups and automorphic functions. AMS, Providence, Rhode Island (1964).

[4] J. Neukirch: Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. Invent. Math., **6**, 296–314 (1969).

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

[6] T. Ono: "Hasse principle" for $PSL_2(\mathbf{Z})$ and $PSL_2(\mathbf{F}_p)$. Proc. Japan Acad., **74A**, 130–131 (1998).

[7] T. Ono and H. Wada: "Hasse principle" for free groups. Proc. Japan Acad., **75A**, 1–2 (1999).

[8] T. Ono: On Shafarevich-Tate sets. The 7th MSJ Int. Res. Inst. Class Field Theory-its centenary and prospect (to appear).

[9] T. Ono and H. Wada: "Hasse principle" for symmetric and alternating groups. Proc. Japan Acad., **75A**, 61–62 (1999).

[10] H. Wada: "Hasse principle" for $SL_n(D)$. Proc. Japan Acad., **75A**, 67–69 (1999).

[11] K. Uchida: Isomorphisms of Galois groups of algebraic number fields, Algebraic number theory-Kyoto Int. Symp., 1976. Japan Soc. Prom. Sci. (ed. S. Iyanaga). pp. 263–266 (1977).