"Hasse principle" for $\mathrm{PSL}_2(\boldsymbol{Z})$ and $\mathrm{PSL}_2(\boldsymbol{F}_p)$

By Takashi ONO

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

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

1. The S-T set for a group. In [1], we introduced a "Shafarevich-Tate set" $\text{Ш}_{\mathrm{H}}(g, G)$ for any g-group G and a family $\boldsymbol{H}$ of subgroups of a group g:

(1.1) $\text{Ш}_{\mathrm{H}}(g, G) = \cap_h \operatorname{Ker} r_h,\ h \in \boldsymbol{H}$,

where r_h is the restriction map: $H(g, G) \to H(h, G)$ of 1-cohomology sets (with origin). In this paper, we consider exclusively the case where $g = G$, acting on itself as inner automorphisms, and $\boldsymbol{H} =$ the family of all cyclic subgroups of G. Hence we have a right to set simply

(1.2) $\text{Ш}(G) = \text{Ш}_{\mathrm{H}}(G, G)$.

Extending the usage of language in Galois cohomology, we call $\text{Ш}(G)$ in (1.2) the S-T set of G. Furthermore G will be said to enjoy the Hasse principle, if $\text{Ш}(G) = 1$. It is easy to verify this for abelian groups, dihedral groups and the quaternion group.

2. Results. In this paper, we shall prove the following

(2.1) **Theorem.** *Let G be either* $\mathrm{PSL}_2(\boldsymbol{Z})$ *or* $\mathrm{PSL}_2(\boldsymbol{F}_p)$, *$p$ being any prime. Then G enjoys the Hasse principle.*

(2.2) **Corollary.** In view of the well-known isomorphisms $\mathrm{PSL}_2(\boldsymbol{F}_2) \cong S_3$, $\mathrm{PSL}_2(\boldsymbol{F}_3) \cong A_4$ and $\mathrm{PSL}_2(\boldsymbol{F}_5) \cong A_5$, three groups S_3, A_4 and A_5 enjoy the Hasse principle.

Before proving (2.1), let us gather some basic facts on $G = \mathrm{PSL}_2(A)$ where $A = \boldsymbol{Z}$ or $\boldsymbol{F}_p$. If $M \in SL_2(A)$, we often use the same symbol M to denote its image in the group $G = PSL_2(A) = SL_2(A)/\{\pm 1\}$. Let S, T and U be elements of G defined by

(2.1)
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

One has:

(2.2) $U = ST,\ S^2 = 1,\ U^3 = 1$,

(2.3) G is generated by S and T : $G = \langle S, T\rangle$.

(2.4) G is generated by S and U : $G = \langle S, U\rangle$.

3. Proof of (2.1). *Case* 1. $A \neq \boldsymbol{F}_2$. We use (2.3). Let $[f]$ be an element of $\text{Ш}(G)$. On replacing the cocycle f by one equivalent to it, we may assume that

(3.1) $f(S) = 1,\ f(T) = M^{-1}M^T,$
$M^T = TMT^{-1}$, for some $M \in G$.

From (2.2) it follows that

(3.2)
$$\begin{aligned} 1 &= f(U^3) = f(U)f(U)^U f(U)U^2 = (f(U)U)^3 \\ &= (Sf(T)T)^3 = (SM^{-1}M^TT)^3 = \\ &(SM^{-1}TM)^3. \end{aligned}$$

Now set

(3.3)
$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G.$$

Then, (3.2) is equivalent to

(3.4)
$$\begin{pmatrix} c^2 & cd-1 \\ cd+1 & d^2 \end{pmatrix}^3 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Furthermore, set

(3.5)
$$t = c^2 + d^2.$$

Then, (3.2), (3.4) amount to the following relation

(3.6)
$$\begin{pmatrix} c^2t^2-t-c^2 & (cd-1)(t^2-1) \\ (cd+1)(t^2-1) & d^2t^2-t-d^2 \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We find also that

(3.7)
$$f(T) = M^{-1}M^T = \begin{pmatrix} 1+cd & -1-cd+d^2 \\ -c^2 & 1-cd+c^2 \end{pmatrix}.$$

Now, to prove (2.1) in Case 1 amounts to find an $X \in G$ so that

(3.8)
$$\begin{cases} X^{-1}X^S = 1 \\ X^{-1}X^T = f(T). \end{cases}$$

Since $cd \neq 1$ or $cd \neq -1$ in this case, we see from (3.6) that $t = \pm 1$. Put $X = \begin{pmatrix} d & -c \\ c & d \end{pmatrix}$ if $t = 1$, and $X = \begin{pmatrix} -d & c \\ c & d \end{pmatrix}$ if $t = -1$. In view of (3.5), (3.7), one verifies immediately that X satisfies (3.8).

Case 2. $A = \boldsymbol{F}_2$. We use (2.4). Let $[f]$ be an element of $\text{Ш}(G)$. On replacing the cocycle f by one equivalent to it, we may assume that

(3.9) $f(S) = 1,\ f(U) = M^{-1}M^U,\ M^U = UMU^{-1}$,

for some $M \in G$.

In this case, we have

(3.10) $G = \{U^i, U^iS, 0 \leqq i \leqq 2\}$, with $SU = U^2S$.

If $M = U^i$, then $f(U) = 1$ and so $f \sim 1$. If $M = U^iS$, then $f(U) = SU^{-i}UU^iSU^{-1} = SUSU^{-1} =$

$U^2SSU^{-1} = U$. Now we see at once that $X = S$ is a solution to

$$(3.11) \qquad \begin{cases} X^{-1}X^S = 1 \\ X^{-1}X^U = f(U) = U. \end{cases}$$

Q. E. D.

References

[1] (a) T. Ono: A note on Shafarevich-Tate sets of finite groups. Proc. Japan Acad., **74A**, 77–79 (1998); (b) T. Ono: On Shafarevich-Tate sets. Proc. The 7th MSJ Int. Res. Inst. Class Field Theory-its centenary and prospect (to appear).