Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 537–547

On Shafarevich–Tate Sets

Takashi Ono

Let K/k be a finite Galois extension of number fields with the Galois group $g = \mathrm{Gal}(K/k)$. Let g_P be the decomposition group at a prime P in K. Let G be a g-group. For each P in K, we have the restriction map $r_P : H(g,G) \to H(g_P, G)$ of 1-cohomology sets for which Ker r_P makes sense. The *Shafarevich–Tate Set* for $(K/k, G)$ is defined by $Ш(K/k, G) = \cap_P \operatorname{Ker} r_P$.

Let X be a smooth curve of genus ≥ 2 over $\mathbb{Q}$. Then $G = \mathrm{Aut}\ X$ is finite by Schwarz theorem and there is a finite Galois extension $K/\mathbb{Q}$ so that G is a finite g-group, $g = \mathrm{Gal}(K/\mathbb{Q})$. The set $Ш(K/k, G)$ becomes finite. As is well-known, the determination of the finite set amounts to an arithmetical refinement of geometrical classification of curves. In this paper, we shall show, among others, that for a hyperelliptic curve $X : y^2 = x^5 - \ell^2 x$, $\ell =$ an odd prime, we have $Ш(K/\mathbb{Q}, G) = 1$ (Hasse principle) if $\ell \equiv 3, 5 \mod 8$, but $\#Ш(K/\mathbb{Q}, G) = 2$ if $\ell \equiv 1, 7 \mod 8$.

There is a way to associate an $S - T$ set $Ш_{\mathbf{H}}(g, G)$ for any group g and a g-group G once we specify a family of subgroups of g (such as the family of decomposition groups g_P when $g = \mathrm{Gal}(K/k)$). E.g., for any finite group G, let $g = G$, acting on itself as inner automorphisms, and let $\mathbf{H}$ be the family of all cyclic subgroups of G. One checks $Ш_{\mathbf{H}}(G, G) = 1$ ("Hasse principle") for some easy groups. Here is an interesting question: *Does the Monster enjoy the Hasse principle?*

§1. $Ш_{\mathbf{H}}(g, G)$.

Let g be a group and G be a (left) g-group. A cocycle is a map $f : g \to G$ such that

$$f(st) = f(s)f(t)^s, \quad s, t \in g.$$

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

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

Received July 29, 1998.