J. Math. Soc. Japan
Vol. 35, No. 2, 1983

The 2-adic representations attached to elliptic curves defined over $\boldsymbol{Q}$ whose points of order 2 are all $\boldsymbol{Q}$-rational

By Kumiko NISHIOKA

(Received July 10, 1980)
(Revised Dec. 3, 1981)

0. Introduction.

Let E be an elliptic curve defined over the field $\boldsymbol{Q}$ of rational numbers. Throughout the paper, an elliptic curve defined over $\boldsymbol{Q}$ means an abelian variety of dimension one which is defined over $\boldsymbol{Q}$. Let G be the Galois group of extension $\bar{\boldsymbol{Q}}/\boldsymbol{Q}$, where $\bar{\boldsymbol{Q}}$ denotes an algebraic closure of $\boldsymbol{Q}$. Then the group G, with the Krull topology, is compact and totally disconnected. For each positive integer m, we denote by E_m the kernel of multiplication by m. Let p be a prime number. With the multiplication by $p: E_{p^{n+1}} \to E_{p^n}$, the sequence $\{E_{p^n}\}_{n=1,2,\dots}$ forms a projective system. The Tate module $T_p(E)$ is defined as follows:

$$T_p(E) = \operatorname{proj}\lim_{n\to\infty} E_{p^n}\,.$$

The module $T_p(E)$ is a free $\boldsymbol{Z}_p$-module of rank 2, where $\boldsymbol{Z}_p$ denotes a p-adic completion of the ring $\boldsymbol{Z}$ of rational integers, and G acts on $T_p(E)$. Fix a base (ξ_0, ξ_1) of $T_p(E)$ over $\boldsymbol{Z}_p$. If σ is an element of G, then there exists a unique element $\pi_p(\sigma)$ of $GL_2(\boldsymbol{Z}_p)$ such that

$$(\sigma\xi_0, \sigma\xi_1) = (\xi_0, \xi_1)\pi_p(\sigma)\,.$$

The mapping $\pi \to \pi_p(\sigma)$, which will be denoted by π_p, is a continuous representation $G \to GL_2(\boldsymbol{Z}_p)$.

Serre [7] proved that if E has no complex multiplication, then the image group $\pi_p(G)$ is an open subgroup of $GL_2(\boldsymbol{Z}_p)$. He also states that if E is semistable and $p \geqq 11$, then the Galois group $\mathrm{Gal}(\boldsymbol{Q}(E_p)/\boldsymbol{Q})$ is isomorphic to $GL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ (Theorem 5 in [8]), and therefore $\pi_p(G) = GL_2(\boldsymbol{Z}_p)$. Put

$$H^{(n)} = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\boldsymbol{Z}_p) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod p^n \right\}.$$

This research was partially supported by Grant-in-Aid for Scientific Research (No. 57540029), Ministry of Education.