Vol. 71, No. 2 DUKE MATHEMATICAL JOURNAL © August 1993

IWASAWA THEORY OF ELLIPTIC CURVES AND GALOIS MODULE STRUCTURE

A. AGBOOLA

0. Introduction. In this paper we apply techniques arising from Iwasawa theory to study the Galois module structure of principle homogeneous spaces constructed via points of infinite order on CM elliptic curves defined over a number field. This theory was introduced by M. J. Taylor in [T1] (see also [ST], [CN-S], and [CN-T]) and is motivated by the fact that such principal homogeneous spaces are very closely connected with certain rings of integers.

Let E be an elliptic curve with complex multiplication by $\mathfrak{O}$, the ring of integers of an imaginary quadratic field K. If $\alpha \in \mathfrak{O}$, we shall often (but not always) write $[\alpha]$ for the corresponding endomorphism of E. Let F/K be a finite extension over which E is defined and acquires everywhere-good reduction. We write $\Delta = \mathrm{Gal}(F/K)$, and we assume that all endomorphisms of E are defined over F. For any field L, we write L^c for an algebraic closure of L, and we set $\Omega_L = \mathrm{Gal}(L^c/L)$.

Let p be an odd rational prime which splits in $\mathfrak{O}$, with $p\mathfrak{O} = \mathfrak{p}\mathfrak{p}^*$. Assume that $p \nmid |\Delta|$. Choose $\pi \in \mathfrak{p}$ with $\mathfrak{p}^h = \pi\mathfrak{O}$ for some $h \geqslant 1$ and write π^* for the complex conjugate of π. Set $q = \pi\pi^*$.

Write G_i for the subgroup of elements of $E(\mathbb{Q}^c)$ which are killed by $[\pi^{*i}]$. Let $\mathfrak{B}_i$ denote the $\mathfrak{O}_F$-Hopf algebra which represents the $\mathfrak{O}_F$-group scheme of $[\pi^{*i}]$-torsion on E, and let $\mathfrak{A}_i$ be the Cartier dual of $\mathfrak{B}_i$. A detailed description of these algebras is given in [T1] (see also [ST]). There it is shown that $\mathfrak{B}_i$ is an $\mathfrak{O}_F$-order in the algebra $\mathscr{B}_i = \mathrm{Map}_{\Omega_F}(G_i, \mathbb{Q}^c)$ and $\mathfrak{A}_i$ is an order in the algebra $\mathscr{A}_i = (F^c G_i)^{\Omega_F}$ (where here Ω_F acts upon both G_i and F^c). (Here and elsewhere, we shall omit from our notation the dependence of our constructions upon the underlying field F unless there is some danger of ambiguity.)

Suppose that $Q \in E(F)$ and write

$$G_Q(i) = \{Q' \in E(\mathbb{Q}^c) : [\pi^{*i}]Q' = Q\}. \tag{0.1}$$

Define the Kummer algebra $F_Q(i)$ by

$$F_Q(i) = \mathrm{Map}_{\Omega_F}(G_Q(i), \mathbb{Q}^c). \tag{0.2}$$

Received 18 February 1992. Revision received 8 December 1992.
Author partially supported by an NSF Postdoctoral Research Fellowship.