TOKYO J. MATH.
VOL. 25, NO. 2, 2002

Isogenies of Degree p of Elliptic Curves over Local Fields and Kummer Theory

Mayumi KAWACHI

Tokyo Metropolitan University

(Communicated by K. Nakamula)

Abstract. Let p be a prime number. In order to calculate the Selmer group of a p-isogeny $\nu : E \to E'$ of elliptic curves, we determine the image of a local Kummer map $E'(K)/\nu E(K) \to H^1(K, \ker\nu)$ over a finite extension K of $\mathbf{Q}_p$. We describe the image using a filtration on a unit group of a local field and the valuation of a coefficient of a leading term in a formal power series of an isogeny.

1. Introduction.

Let $\nu : E \to E'$ be an isogeny of elliptic curves over a number field $\mathcal{K}$. We are interested in its Selmer group $\mathrm{Sel}(\nu)$ which is a subgroup of $H^1(\mathcal{K}, \ker\nu)$ generated by the elements whose local images in $H^1(\mathcal{K}_v, \ker\nu)$ are in $\mathrm{Im}\,\delta_v$ for all primes v. Here δ_v is a connecting homomorphism of an exact sequence over $\mathcal{K}_v$

$$1 \longrightarrow \ker\,\nu \longrightarrow E \xrightarrow{\nu} E' \longrightarrow 1\,.$$

So δ_v fits in an exact sequence

$$1 \longrightarrow E'(\mathcal{K}_v)/\nu E(\mathcal{K}_v) \xrightarrow{\delta_v} H^1(\mathcal{K}_v, \ker\nu) \longrightarrow H^1(\mathcal{K}_v, E)$$

for each v. Let p be a prime number. We assume ν is a p-isogeny, namely $\ker\nu$ is a group of order p. In order to study such Selmer group $\mathrm{Sel}(\nu)$, one of the difficult problems is to know $\mathrm{Im}\,\delta_v$ for primes v over p. If E has good reduction at v and v does not divide p, then $\mathrm{Im}\,\delta_v = H^1_{ur}(\mathcal{K}_v, \ker\nu)$, where $H^1_{ur}(\mathcal{K}_v, \ker\nu) = \ker(H^1(\mathcal{K}_v, \ker\nu) \to H^1(\mathcal{K}_v^{ur}, \ker\nu))$. But if v divides p then the equation does not hold. This paper is devoted to the study of $\mathrm{Im}\,\delta_v$ for v over p. In [1], Berkovič treated the case when E has a complex multiplication and $\nu \in \mathrm{End}(E)$, and expressed $\mathrm{Im}\,\delta_v$ as a subgroup of $\mathcal{K}_v^\times/\mathcal{K}_v^{\times p}$, under the assumption $\mathcal{K}_v \supset \mu_p$ and $E(\mathcal{K}_v) \supset \ker\nu$. In this paper we treat the case when ν is a general p-isogeny.

We also assume that $\mathcal{K}_v \supset \mu_p$ and $E(\mathcal{K}_v) \supset \ker\nu$. Let $\mathcal{O}_v$ be the ring of integers of $\mathcal{K}_v$, $\mathfrak{M}_v$ the maximal ideal of $\mathcal{O}_v$ and U the unit group of $\mathcal{O}_v$. Let $U^0 = U$ and $U^i = 1 + \mathfrak{M}_v^i$ for $i \geq 1$. This gives a filtration on the unit group of $\mathcal{K}_v$, $\mathcal{K}_v^\times \supset U^0 \supset U^1 \supset U^2 \supset \cdots$. It also induces a filtration $\mathcal{K}_v^\times/\mathcal{K}_v^{\times p} \supset C^0 \supset C^1 \supset \cdots \supset C^{pe_0+1} = \{1\}$, where $C^i = U^i/K^{\times p} \cap U^i$ for $i \geq 0$ and e_0 is the ramification index of $\mathcal{K}_v$ over $\mathbf{Q}_p(\zeta_p)$. On the other hand let E

Received March 22, 2000; revised March 5, 2002