10. *A Reciprocity Law in Some Relative Quadratic Extensions*

By Hideji ITO
Department of Mathematics, Akita University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1980)

Introduction. Let E be an elliptic curve defined over $\boldsymbol{Q}$, and ℓ a rational prime ($\neq 2$). Put $E_\ell = \{a \in E \mid \ell a = 0\}$ and $K_\ell = \boldsymbol{Q}(E_\ell)$, i.e. the number field generated over $\boldsymbol{Q}$ by all the coordinates of the points of order ℓ on E. K_ℓ contains a subfield K'_ℓ which is generated over $\boldsymbol{Q}$ by all the x-coordinates of the points of order ℓ on E. The degree of K_ℓ/K'_ℓ is 1 or 2, and usually the latter is the case, for example, when $\mathrm{Gal}(K_\ell/\boldsymbol{Q}) \cong \mathrm{GL}_2(\boldsymbol{Z}/\ell\boldsymbol{Z})$ or when E has complex multiplication (see Remark in § 2).

The aim of this note is to investigate the law of decomposition of primes in these extensions K_ℓ/K'_ℓ.

Let p be a good prime for E. Put $\pi = \pi_p$ be the Frobenius endomorphism of $E \bmod p$, and $a_p = \mathrm{tr}(\pi)$, where trace is taken with respect to the ℓ-adic representation of $E \bmod p$. Then the main result of this note is the following: If $\left(\frac{p}{\ell}\right) = -1$, then the relative degree of $\mathfrak{p}$ (=any extension of p to K'_ℓ) in K_ℓ/K'_ℓ coincides with the absolute degree of ℓ in $\boldsymbol{Q}(\sqrt{a_p^2 - 4p})/\boldsymbol{Q}$. One might say that this is some sort of reciprocity law, although in case $\left(\frac{p}{\ell}\right) = 1$ that cannot always hold.

§ 1. The following two fields are contained in K_ℓ:

i) $\boldsymbol{Q}(\zeta_\ell)$, where ζ_ℓ is a primitive ℓ-th root of unity,

ii) $M_\ell = \boldsymbol{Q}(j_1, j_2, \cdots, j_{\ell+1})$, where j_i's are the j-invariants of elliptic curves which are ℓ-isogenous to E, in other words, M_ℓ is the splitting field of the modular equation $J_\ell(X, j(E)) = 0$, where $j(E)$ is the j-invariant of E.

Both of them are Galois extensions of $\boldsymbol{Q}$. Put $G = \mathrm{Gal}(K_\ell/\boldsymbol{Q})$. Then we can identify G with a subgroup of $\mathrm{GL}_2(\boldsymbol{Z}/\ell\boldsymbol{Z})$. And the corresponding subgroups for $\boldsymbol{Q}(\zeta_\ell)$ and M_ℓ by the Galois theory are

$$S = G \cap \mathrm{SL}_2(\boldsymbol{Z}/\ell\boldsymbol{Z}), \qquad H = G \cap \{aI \mid a \in (\boldsymbol{Z}/\ell\boldsymbol{Z})^*\},$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, respectively.

Proposition 1. 1) $K'_\ell = M_\ell(\zeta_\ell)$, 2) $M_\ell \cap \boldsymbol{Q}(\zeta_\ell) \supset \boldsymbol{Q}(\sqrt{\pm \ell})$. *Here we take* $+\ell$ *when* $\ell \equiv 1 \pmod 4$ *and* $-\ell$ *when* $\ell \equiv 3 \pmod 4$.

Proof. 1) Note that K'_ℓ corresponds to $G \cap \{\pm I\}$ and $\mathrm{SL}_2(\boldsymbol{Z}/\ell\boldsymbol{Z})$