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 $E_\ell=\{a\in E\,|\,\ell a=0\}$ 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

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

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* $\ell\equiv1$ (mod 4) *and* $-\ell$ *when* $\ell\equiv 3$ (mod 4).

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

$\cap \{aI \mid a \in (Z/\ell Z)^*\} = \{\pm I\}$. 2) Put $N = \{A \in \mathrm{GL}_2(Z/\ell Z) \mid \det A \in (Z/\ell Z)^2\}$. Then we see easily that $Q(\sqrt{\pm \ell})$ corresponds to $N \cap G$ and N contains $\mathrm{SL}_2(Z/\ell Z)$ and $\{aI \mid a \in (Z \in \ell Z)^*\}$. So $N \cap G \supset SH$. This means $Q(\sqrt{\pm \ell}) \subset M_\ell \cap Q(\zeta_l)$. Q.E.D.

When $G \cong \mathrm{GL}_2(Z/\ell Z)$, we have $M_\ell \cap Q(\zeta_\ell) = Q(\sqrt{\pm \ell})$. But there are cases where $M_\ell \supset Q(\zeta_\ell)$. See Serre [3, p. 309].

Letting f_0, f_1 and f' be the absolute degrees of P in $Q(\zeta_\ell)$, M_ℓ and K'_ℓ respectively, we have the following

Corollary. *$f' = \langle f_0, f_1 \rangle$, i.e. the least common multiple of f_0 and f_1.*

As is well-known, f_0 is the smallest positive integer a for which $p^a \equiv 1 \pmod{\ell}$ holds. From the action of π on $(E \bmod p)_\ell = \{a \in E \bmod p \mid \ell a = 0\} \cong Z/\ell Z \oplus Z/\ell Z$, we can represent π by a matrix $S(\pi)$ in $\mathrm{GL}_2(Z/\ell Z)$ and the characteristic polynomial of $S(\pi)$ is $X^2 - a_p X + p$. Considering the Jordan normal form of $S(\pi)$, if $\ell \nmid (a_p^2 - 4p)$, then f_1 is the smallest positive integer b such that the characteristic polynomial of $S(\pi^b)$ has multiple roots in $F_\ell = Z/\ell Z$. If $\ell \mid (a_p^2 - 4p)$, then f_1 is 1 or ℓ according as $\ell \mid (\mathfrak{o} : Z[\pi])$ or not (here $\mathfrak{o} = \mathrm{End}_{F_p}(E \bmod p)$, see [1, Theorem 1]). Let f be the absolute degree of p in K_ℓ/Q and put $k = Q(\sqrt{a_p^2 - 4p})$.

Proposition 2. *Suppose $\ell \nmid (a_p^2 - 4p)$. If ℓ splits in k/Q, then f_1 and f divide $\ell - 1$, while if ℓ remains prime in k/Q, then f_1 divides $\ell + 1$.*

Proof. Our assumptions mean that $X^2 - a_p X + p$ splits into two different linear factors or is irreducible over F_ℓ. In the former case, $S(\pi)$ is conjugate to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $a, b \in F_\ell$, $a \neq b$. So $S(\pi)^{\ell-1} = \text{identity}$. In the latter case, $S(\pi)$ is conjugate to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $a, b \in F_{\ell^2} - F_\ell$. As a is conjugate to b over F_ℓ, we have $a^{\ell+1} = \text{Norm of } a \text{ relative to } F_{\ell^2}/F_\ell = b^{\ell+1} \in F_\ell$. So f_1 divides $\ell + 1$. Q.E.D.

§ 2. For a natural number $n = 2^a b$, $2 \nmid b$, we put $e(n) = a$.

Theorem 1. *The following three cases occur.*

(i) *If $e(f_0) \neq e(f_1)$, then $f = 2f'$.*

(ii) *If $e(f_0) = e(f_1) > 0$, then $f = f'$.*

(iii) *If $e(f_0) = e(f_1) = 0$, that is, both f_0 and f_1 are odd, then we have both cases. If $a_p = a$ gives $f = f'$, then in case $a_p = -a$ we have $f = 2f'$ (and vice versa).*

Proof. In any case as $[K_\ell : K'_\ell] = 1$ or 2, we know that $f = f'$ or $2f'$. Note that in the cases (i) and (ii), $f' = \langle f_0, f_1 \rangle$ is even by Corollary of Proposition 1.

(i) Suppose $e(f_0) > e(f_1)$. Then $f_1 \mid (f'/2)$, $f_0 \nmid (f'/2)$. Hence if

$S(\pi^{f'})=$ identity, then $S(\pi^{f'/2})=\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $a^2=\det S(\pi^{f'/2})=-1$, $a\in \boldsymbol{F}_\ell$. But then, as $S(\pi^{f'})=\begin{pmatrix} a^2 & 0 \\ 0 & a^2 \end{pmatrix}$, we have $a^2=1$. This is a contradiction. So $f=2f'$.

(i)′ Suppose $e(f_0)<e(f_1)$. Then $f_0|(f'/2)$, $f_1\nmid(f'/2)$. So, if $S(\pi^{f'})=$ id., then $S(\pi^{f'/2})$ is conjugate to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $a\neq b$, $ab=1$, $a, b\in \boldsymbol{F}_\ell$. As $S(\pi^{f'})=\begin{pmatrix} a^2 & 0 \\ 0 & b^2 \end{pmatrix}=$ id., we have $a^2=b^2=1$. Hence $1=ab=a^2$. Therefore $a(a-b)=0$, a contradiction.

(ii) Suppose $S(\pi^{f'})\neq$ id. As $S(\pi^{2f'})=$ id., we have $S(\pi^{f'})=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Since f' is even and both f_0 and f_1 do not divide $f'/2$, we see that $S(\pi^{f'/2})$ is conjugate to $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$, $c, d\in \boldsymbol{F}_\ell$, $c^2=d^2=-1$, $c\neq d$, $cd=-1$. Hence $c^2=-1=cd$. So we have $c(c-d)=0$. A contradiction.

(iii) Note that f_0 and f_1 (and hence f') take the same value for $a_p=\pm a$. Take $A, B\in \mathrm{GL}_2(\boldsymbol{F}_\ell)$ which satisfy $\mathrm{tr}\,A=-\mathrm{tr}\,B$ and $\det A=\det B=p$. Suppose the orders of their images into $\mathrm{PGL}_2(\boldsymbol{F}_\ell)$ coincide. What we have to show is that if A has order m then B has order $2m$ or $m/2$ according as $2\nmid m$ or $2\|m$. But, for odd n, we easily see that

$$\mathrm{tr}\,(A^n)=\mathrm{tr}\,(A)^n-np\,\mathrm{tr}\,(A^{n-2})-\binom{n}{2}p^2\,\mathrm{tr}\,(A^{n-4})-\cdots-np^{(n-1)/2}\,\mathrm{tr}\,(A).$$

Hence by induction we get $\mathrm{tr}\,(A^n)=-\mathrm{tr}\,(B^n)$. So our assertion is clear. This completes our proof.

Proposition 3. *If ℓ remains prime in $\boldsymbol{Q}(\sqrt{a_p^2-4p})$, then the case* (ii) *in Theorem* 1 *never occurs.*

Proof. If $\ell\,|\,(a_p^2-4p)$, then $f_1=1$ or ℓ. So the assertion is clear. Now suppose $\ell\nmid(a_p^2-4p)$. Then $S(\pi)$ is conjugate to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $a, b\in \boldsymbol{F}_{\ell^2}-\boldsymbol{F}_\ell$, $a\neq b$. If $e(f_0)=e(f_1)>0$, then by Theorem 1 we have $S(\pi^{f'})=$ identity. So $a^{f'}=b^{f'}=1$. As f' is even and both f_0 and f_1 do not divide $f'/2$, we have $\{a^{f'/2}, b^{f'/2}\}=\{+1, -1\}$. But a is conjugate to b over $\boldsymbol{F}_\ell$, so their orders in $\bar{\boldsymbol{F}}_\ell^*$ must coincide. This is a contradiction.

Q.E.D.

Remark. As an application of Theorem 1, we can show that if E has complex multiplication (say by $\sqrt{-q}$) we have $K_\ell\neq K'_\ell$ for all $\ell>2$ and $\ell\neq q$. Indeed, put $k_0=\boldsymbol{Q}(\sqrt{-q})$. Let p be a prime which remains prime in k_0 and satisfies $p\equiv 1 \pmod{\ell}$. Then $a_p=0$ and the order f_0 of p in $\boldsymbol{F}_\ell^*$ is 1. Hence $f_1=2$ and $e(f_1)>e(f_0)=0$. So the case (i) occurs. This means that $K_\ell\neq K'_\ell$.

§ 3. When $\left(\frac{p}{\ell}\right)=-1$, we have the following simple decomposition law of primes.

Theorem 2. *Suppose* $\left(\frac{p}{\ell}\right)=-1$. *Then the relative degree of* $\mathfrak{p}$ ($=$*any prime in* K'_ℓ *lying above* p) *in* K_ℓ/K'_ℓ *coincides with the absolute degree of* ℓ *in* $\boldsymbol{Q}(\sqrt{a_p^2-4p})/\boldsymbol{Q}$.

Proof. By our assumption, we see $\ell \nmid (a_p^2-4p)$ and both f_0 and f_1 are even. Indeed, by Proposition 1, $M_\ell \cap \boldsymbol{Q}(\zeta_\ell) \supset \boldsymbol{Q}(\sqrt{\pm\ell})$. If $\ell\equiv 1 \pmod 4$, then $\left(\frac{\ell}{p}\right)=\left(\frac{p}{\ell}\right)=-1$. When $\ell\equiv 3 \pmod 4$, we easily see that $\left(\frac{-\ell}{p}\right)=-1$. Now put $k=\boldsymbol{Q}(\sqrt{a_p^2-4p})$. Suppose $\ell\equiv 3 \pmod 4$. Then we clearly have $e(f_0)=1$. If ℓ remains prime in k, then by Proposition 3 the case (ii) of Theorem 1 never occurs, so the case (i) occurs (by the way, this means especially that $4 \mid f_1$). If ℓ splits in k, then by Proposition 2, $f_1 \mid (\ell-1)$. Therefore $e(f_1)=1$. So we have the case (ii). Now suppose $\ell\equiv 1 \pmod 4$. If 2^n exactly divides $\ell-1$, then $e(f_0)=n\geqq 2$, because $\left(\frac{p}{\ell}\right)=-1$. If ℓ remains prime in k, then by Proposition 2, $f_1 \mid (\ell+1)$, so $e(f_1)=1$. Hence the case (i) occurs. If ℓ splits in k, then $f \mid (\ell-1)$. Assume $f=2f'=2\langle f_0, f_1\rangle$. Then 2^{n+1} divides f, because $e(f_0)=n$. So we have $2^{n+1} \mid (\ell-1)$, a contradiction. Therefore we must have $f=f'$. This completes the proof of our theorem.

§ 4. We can explain the reason why in the case both f_0 and f_1 are odd (and only in that case) the relation between f and f' cannot be determined in terms of f_0 and f_1 (as in Theorem 1, (iii)).

First note that K'_ℓ is unchanged when we replace E with any other $\boldsymbol{C}$-isomorphic elliptic curves$/\boldsymbol{Q}$, while K_ℓ is not. Suppose A is an elliptic curve$_{/\boldsymbol{Q}}$ which is $\boldsymbol{C}$-isomorphic to E, but is not $\boldsymbol{Q}$-isomorphic to E. Put $L_\ell=\boldsymbol{Q}(A_\ell)$. If $j(E)\neq 0$, 1728, then over some quadratic field $\boldsymbol{Q}(\sqrt{d})$, $d\in\boldsymbol{Z}$, they become isomorphic. Hence $K_\ell(\sqrt{d})=L_\ell(\sqrt{d})$. By a simple reasoning, when f' is even, we see that any prime $\mathfrak{p}$ of K'_ℓ lying above p always splits in $K'_\ell(\sqrt{d})/K'_\ell$. Therefore the decomposition of $\mathfrak{p}$ in K_ℓ/K'_ℓ agrees with that in L_ℓ/K'_ℓ. If f' is odd and p splits in $\boldsymbol{Q}(\sqrt{d})$, then the situation is the same as before, but when f' is odd and p remains prime in $\boldsymbol{Q}(\sqrt{d})$, the decomposition of $\mathfrak{p}$ in K_ℓ/K'_ℓ differs from that in L_ℓ/K'_ℓ, because above $\mathfrak{p}$ remains prime in $K'_\ell(\sqrt{d})/K'_\ell$.

References

[1] H. Ito: A note on the law of decomposition of primes in certain galois extension. Proc. Japan Acad., **53**A, 115–118 (1977).
[2] S. Lang: Elliptic Functions. Addison Wesley, Reading (1973).
[3] J. P. Serre: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math., **15**, 259–331 (1972).