Selmer Groups and Ideal Class Groups

by

Noboru Aoki

(Received July 9, 1993)

Introduction

Let $E$ and $E'$ be elliptic curves defined over a number field $k$. Suppose that there is a cyclic isogeny $\phi : E \rightarrow E'$ defined over $k$ with prime degree $p$. The aim of this paper is to give an upper bound of the order of the $\phi$-Selmer group $S^{(\phi)}(E/k)$ (see Section 1 for the definition) in terms of the ideal class group of an extension field $K$ of $k$.

When $E(K)$ contains the kernel of $\phi$, $S^{(\phi)}(E/k)$ is known to have a close relation to the ideal class group $Cl_K$ of $K$; it gives usually an upper bound of the size of $S^{(\phi)}(E/k)$ in terms of the $p$-part of $Cl_K$. There are many results in this direction. For example, Brumer and Kramer ([3]) and Washington ([33]) studied the case where $p = 2$ and $[K : k] = 3$. (See Kawachi and Nakano [16] for a further development of [33].) Frey ([8], [9] (See also [10])), Nekovář ([23]) and Quer ([24]) studied the case where $p = 3$, $k = Q$ and $[K : Q] = 2$ by making use of the elliptic curve defined by the equation $y^2 = x^3 + a$. Top ([31]) treated the same case ($p = 3$, $[K : Q] = 2$) in a more general setting. The case of $p = 5, 7$ was studied by Mestre ([20], [21]) and Lecacheux ([18]).

In the above cases $[K : k]$ is always assumed to be prime to $p$. In contrast to them, we shall treat the case where $[K : k] = p$. Our results does not give any new information on the ideal class groups; on the contrary, our proof uses a formula including class numbers (the genus formula). Let us state our results restricting ourselves to the case of $p = 3$. We assume that $k$ contains a primitive cubic root of unity.

First let us consider the elliptic curve $E$ defined over $k$ by the equation

$$y^2 = 4x^3 + a^2(x - b)^2,$$

where $a$ and $b$ are integers of $k$ with $ab(a^2 + 7b) \neq 0$. This curve has a $k$-rational point $P_0 = (0, ab)$ of order three, hence it induces a $k$-rational cyclic 3-isogeny $\phi : E \rightarrow E' := E/\langle P_0 \rangle$.

**Theorem 0.1.** Let $K = k(\sqrt[3]{a^2b(a^2 + 7b)})$ and put $G = Gal(K/k)$. Let $T$ be the set of finite places of $k$ which divide $3ab(a^2 + 7b)$. Then
\[ \dim_{\mathbb{Z}/3\mathbb{Z}} S^{(\phi)}(E/k) \leq 1 + \frac{[k : \mathcal{O}]}{2} + \text{ord}_3 \left( \frac{|(Cl_{k,T})^G|}{|(Cl_{k,T})^3|} \right), \]

where \( Cl_{k,T} \) (resp. \( Cl_{k,T} \)) denotes the \( T \)-ideal class group of \( K \) (resp. \( k \)).

As for the Mordell-Weil rank, we have the following result.

**Theorem 0.2 (Theorem 3.6).** Notation being as above, we have

\[ \text{rank } E(k) \leq [k : \mathcal{O}] + 2 \text{ord}_3 \left( \frac{|(Cl_{k,T})^G|}{|(Cl_{k,T})^3|} \right). \]

As a second example let us consider the curve \( E \) defined over \( k = \mathcal{O}(\sqrt{-3}) \) by the equation

\[ y^2 = 4x^3 + a^2, \]

where \( a \) is a non-zero cube-free integer of \( k \). In this case the point \((0, a)\) is \( k \)-rational and of order three. Hence, as before, it induces a \( k \)-rational cyclic 3-isogeny \( \phi \).

**Theorem 0.3 (Theorem 4.7, Corollary 4.8).** Let \( K = \mathcal{O}(\sqrt{a}) \) and put \( G = \text{Gal}(K/k) \). Suppose that \( a \equiv \pm 1 \pmod{3} \) but \( \neq \pm 1 \pmod{3} \). Let \( T \) be the set of finite places of \( k \) which divide \( a \). Then

\[ \dim_{\mathbb{Z}/3\mathbb{Z}} S^{(\phi)}(E/k) = 1 + \text{ord}_3 |(Cl_{k,T})^G|. \]

Moreover we have

\[ \text{rank } E(k) \leq 2 \text{ord}_3 |(Cl_{k,T})^G|. \]

Buhler and Gross ([3]), extending results of Gross ([14]), proved that a similar equality holds for the \( \mathcal{O} \)-curves. However, our result is not entirely contained in their cases.

If \( E \) is already defined over \( \mathcal{O} \), then \( \text{rank } E(k) = 2 \text{ rank } E(\mathcal{O}) \). Therefore the above theorem implies the following result.

**Theorem 0.4 (Corollary 4.9).** Let \( E \) be an elliptic curve defined by (0.2) with \( a \in \mathbb{Z} \). Let \( K \) and \( T \) be as in Theorem 0.3. Then, if \( a \) satisfies the condition \( a \equiv 2, 4, 5, 7 \pmod{9} \), we have

\[ \text{rank } E(\mathcal{O}) \leq \text{ord}_3 |(Cl_{k,T})^G|. \]

This paper is organized as follows. In Section 1 we shall recall some general facts about Selmer groups mainly from Silverman’s book ([28]). In Section 2 we shall introduce some well-known results on local pairings which will be needed later. Section 3 will be devoted to the proof of one of our main results (Theorem 3.3) and its applications. The key point in the proof is the genus formula (or more exactly \( T \)-genus formula) for the cyclic extension \( K/k \) due to Federer ([7]) and Gras ([13]), which we shall review in the final section. (We recommend the reader to read Section
5 before reading the proof of Theorem 3.3.) In connecting the Selmer group with the genus formula, Corollary 2.3, which is an immediate consequence of Tate’s local duality theorem (see Theorem 2.2), will play an important role. The idea goes back to the work of Cassels ([5]). In Section 4 we shall apply the results obtained in Section 3 to elliptic curves with complex multiplication. Moreover another formula for the order of the \( \phi \)-Selmer group will be given at the end of the section. The main term of the formula is the rank of a matrix with entries in a finite field, and so it is more suitable for actual calculations.

1. The Selmer and the Shafarevich-Tate groups

Suppose that we are given two elliptic curves \( E, E' \) defined over a number field \( k \) and a non-zero isogeny

\[
\phi : E \longrightarrow E'
\]

which is also defined over \( k \). Then there is an exact sequence of \( G(\bar{k}/k) \)-modules,

\[
0 \longrightarrow E_\phi \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0
\]

(1.1)

where \( E_\phi \) denotes the kernel of \( \phi \). For any field \( L \) containing \( k \), taking Galois cohomology group \( H^*(L, -) \) yields a long exact sequence

\[
0 \longrightarrow \cdots \longrightarrow E(L)_\phi \longrightarrow E(L) \longrightarrow E'(L)
\]

\[
\delta_L : H^1(L, E_\phi) \longrightarrow H^1(L, E) \longrightarrow H^1(L, E);
\]

and from this we obtain a fundamental exact sequence

\[
0 \longrightarrow E'(L)/\phi(E(L)) \xrightarrow{\delta_L} H^1(L, E_\phi) \longrightarrow H^1(L, E_\phi) \longrightarrow 0
\]

(1.2)

Let us denote by \( M_k \) the set of the places of \( k \). When \( L=k_v \) \((v \in M_k)\), the completion of \( k \) with respect to \( v \), we write \( \delta_v \) for \( \delta_{k_v} \). The subgroup of \( H^1(k, E) \) defined by

\[
\Sha(E/k) = \text{Ker} \left( \prod v \in M_k \text{ res}_v : H^1(k, E) \longrightarrow \prod v \in M_k H^1(k_v, E) \right)
\]

is called the Shafarevich-Tate group of \( E/k \). The \( \phi \)-Selmer group \( S^{(\phi)}(E/k) \) is defined by the exact sequence

\[
0 \longrightarrow S^{(\phi)}(E/k) \longrightarrow H^1(k, E_\phi) \longrightarrow \prod v \in M_k H^1(k_v, E).
\]

Then we have an exact sequence called the \( \phi \)-descent sequence:

\[
0 \longrightarrow E(k)/\phi(E(k)) \longrightarrow S^{(\phi)}(E/k) \longrightarrow \Sha(E/k) \longrightarrow 0.
\]

(1.3)

Now suppose that \( \phi \) is a cyclic isogeny of degree \( m \), that is, an isogeny whose
kernel is a cyclic group of order $m$. In order to compute the rank of $E(k)$, we need to consider the dual isogeny $\phi^*: E' \to E$ of $\phi$ and the $\phi^*$-descent sequence.

\begin{equation}
0 \to E(k)/\phi(E(k)) \to S^{(\phi^*)}(E'/k) \to \Phi(E'/k)_{\phi^*} \to 0.
\end{equation}

Then the exact sequence

\begin{equation}
0 \to \frac{E'(k)}{\phi(E(k))_m} \to \frac{E'(k)}{\phi(E(k))} \to \frac{E(k)}{mE(k)} \to \frac{E(k)}{\phi'(E(k))} \to 0
\end{equation}

gives a formula for the rank of $E(k)$. To see this we assume that $m$ is a prime. Then each term of (1.5) is a vector space over $\mathbb{Z}/m\mathbb{Z}$, and the rank of $E(k)$ is given by the formula

\begin{equation}
\text{rank } E(k) = \dim E'(k)/\phi(E(k)) + \dim E(k)/\phi'(E(k))
- \dim E(k)/\phi(E(k))_m - \dim E(k)_m.
\end{equation}

Here we note that

\begin{equation}
\dim E'(k)/\phi(E(k))_m + \dim E(k)_m = \dim E(k) + \dim E'(k)_{\phi^*}.
\end{equation}

On the other hand (1.3) shows that

\begin{equation}
\dim E'(k)/\phi(E(k)) \leq \dim S^{(\phi^*)}(E/k),
\end{equation}

and similarly (1.5) shows that

\begin{equation}
\dim E(k)/\phi'(E(k)) \leq \dim S^{(\phi^*)}(E'/k).
\end{equation}

From (1.6), (1.7), (1.8) and (1.9) we have the following bound of rank $E(k)$.

**Proposition 1.1.** Suppose that $m$ is a prime. Then

\[ \text{rank } E(k) \leq \dim S^{(\phi)}(E/k) + \dim S^{(\phi^*)}(E'/k) - \dim E(k)_{\phi} - \dim E'(k)_{\phi^*}. \]

Let us return to the case of general $m$. In order to give an upper bound for $|S^{(\phi)}(E/k)|$ and $|S^{(\phi^*)}(E'/k)|$, let $S$ be the set of places of $k$ consisting of the infinite places and those which divide $m\Delta_k$, where $\Delta_k$ denotes the discriminant of $E$. Then it is well known that both $E$ and $E'$ have good reduction outside $S$. (See [27].)

**Proposition 1.2.** If $k_S$ denotes the maximal Galois extension of $k$ which is unramified outside $S$, then

\[ S^{(\phi)}(E/k) = \text{Ker} \left( H^1(k_S/k, E_{\phi}) \to \bigoplus_{v \in S} H^1(k_v, E) \right). \]

**Proof.** We know that there is an exact sequence

\[ 0 \to H^1(k_S/k, E_{\phi}) \to H^1(k, E_{\phi}) \to \prod_{v \notin S} H^1(k_v, E) \]

([22] Chap. I. Proposition 6.5). Then the assertion immediately follows from this
and the definition of \( S^\phi(E/k) \).

Clearly Proposition 1.2 implies that

\[
S^\phi(E/k) = \{ \xi \in H^1(k_{S^m}/k, E_\phi) \mid \text{res}_v(\xi) \in \text{Im}(\delta_v) \ (\forall v \in S) \}.
\]

Suppose that \( E(k)_\phi \cong \mathbb{Z}/m\mathbb{Z} \) and that \( k \) contains \( \mu_m \), the group of \( m \)-th roots of unity. Then \( H^1(k_{S^m}/k, E_\phi) \cong H^1(k_{S^m}/k, \mu_m) \), hence we can regard \( H^1(k_{S^m}/k, E_\phi) \) as a subgroup of \( k^*/k^{*m} \). Kummer theory shows that there is an isomorphism

\[
H^1(k_{S^m}/k, \mu_m) \cong \{ x \in k^*/k^{*m} \mid \text{ord}_v(x) \equiv 0 \ (\text{mod. } m) \text{ for any } v \in S \}.
\]

Let \( Cl_{k,S} \) be the \( S \)-ideal class group of \( k \). We define a map \( j : H^1(k_{S^m}/k, \mu_m) \rightarrow (Cl_{k,S})_m \) by

\[
j(x) = \text{the class of the ideal } \left( \prod_{v \in S} \mathfrak{p}_v^{(1/m)\text{ord}_v(x)} \right),
\]

where \( \mathfrak{p}_v \) denotes the prime ideal of \( k \) corresponding to \( v \). If \( U_{k,S} \) denotes the \( S \)-units of \( k \), then we have an exact sequence

\[
0 \rightarrow U_{k,S} k^*/k^{*m} \rightarrow H^1(k_{S^m}/k, \mu_m) \rightarrow (Cl_{k,S})_m \rightarrow 0.
\]

Thus we get an inequality

\[
|S^\phi(E/k)| \leq m^{S^m} \cdot |(Cl_{k,S})_m|.
\]

This, however, gives only a very rough estimate of \( |S^\phi(E/k)| \) in general.

If \( E \) has complex multiplication by an imaginary quadratic field \( F \), we can say more about rank \( E(k) \). Let \( \phi \in R := \text{End}(E) \) be an endomorphism of degree \( m \). We suppose that \( \phi \) is defined over \( k \). Then (1.3) reads as

\[
0 \rightarrow E(k)/\phi(E(k)) \rightarrow S^\phi(E/k) \rightarrow \text{III}(E/k)_\phi \rightarrow 0.
\]

Thus, if \( m \) is a prime, we find that the following inequality holds:

\[
\text{End}_R E(k) \leq \dim S^\phi(E/k) - \dim E(k)_\phi.
\]

Moreover, if the defining field of \( E \) can be descended to a subfield \( k_0 \) of \( k \) such that \([k : k_0] = 2\) and \( k = k_0 F \), then we can easily show that

\[
\text{rank}_R E(k) = \text{rank} E(k_0) .
\]

Therefore by (1.13) we have

\[
\text{rank} E(k_0) \leq \dim S^\phi(E/k) - \dim E(k)_\phi.
\]
2. Local pairings

In this section we assume that \( k \) contains \( \mu_m \) and that \( E(k) \) contains a torsion point \( P_0 \) of order \( m \). Then there is a cyclic \( m \)-isogeny

\[
\phi : E \longrightarrow E'
\]

with \( E_{\phi} = \langle P_0 \rangle \), the cyclic group of order \( m \) generated by \( P_0 \). Clearly both \( \phi \) and \( E' \) are defined over \( k \). Moreover the dual isogeny

\[
\phi' : E' \longrightarrow E
\]

is also defined over \( k \), and \( E'_{\phi} \) is a cyclic group of order \( m \) generated by a \( k \)-rational torsion point \( P'_0 \). Indeed, this follows from the fact that \( E'_{\phi} \) is the Cartier dual of \( E_{\phi} \) ([15]).

Now let \( v \) be a place of \( k \). Then the Weil pairing with respect to \( \phi \)

\[
e_{\phi}(,): E_{\phi} \times E'_{\phi} \longrightarrow \mu_m
\]

defines a cup product

\[
\langle , \rangle_v : H^1(k_v, E_{\phi}) \times H^1(k_v, E'_{\phi}) \longrightarrow H^2(k_v, \mu_m) = \frac{1}{m} \mathbb{Z}/\mathbb{Z},
\]

where we have identified \( H^2(k_v, \mu_m) \) with \((1/m)\mathbb{Z}/\mathbb{Z}\) via the invariant map \( \text{inv}_v \). Moreover \( e_{\phi}(,\cdot) \) induces an isomorphism

\[
(i_v : H^1(k_v, E_{\phi}) \sim H^1(k_v, \mu_m))
\]

which sends the cocycle \([\sigma \mapsto n_{\sigma}P_0]\) to the cocycle \([\sigma \mapsto \zeta^{n_{\sigma}}]\), where \( \zeta = e_{\phi}(P_0, P'_0) \).

Similarly we obtain an isomorphism

\[
(i'_v : H^1(k_v, E'_{\phi}) \sim H^1(k_v, \mu_m))
\]

which sends the cocycle \([\sigma \mapsto n'_{\sigma}P'_0]\) to the cocycle \([\sigma \mapsto \zeta^{n'_{\sigma}}]\). By Kummer theory we have an isomorphism

\[
\kappa_v : H^1(k_v, \mu_m) \sim k_v^*/k_v^{*m},
\]

hence using (2.1) and (2.2) we obtain isomorphisms

\[
j_v : H^1(k_v, E_{\phi}) \sim k_v^*/k_v^{*m} \quad \text{and} \quad j'_v : H^1(k_v, E'_{\phi}) \sim k_v^*/k_v^{*m}.
\]

Let

\[
( , )_v : k_v^*/k_v^{*m} \times k_v^*/k_v^{*m} \longrightarrow \mu_m
\]
be the Hilbert norm residue symbol of $k_v$.

**Proposition 2.1.** The pairing $\langle \cdot, \cdot \rangle_v$ is compatible with $(\cdot, \cdot)_v$ in the sense that the diagram

$$
\begin{array}{ccc}
H^1(k_v, E_\phi) \times H^1(k_v, E_\phi') & \xrightarrow{\langle \cdot, \cdot \rangle_v} & (1/m)Z/Z \\
\downarrow i_v \times i'_v & & \downarrow i \\
k_v^* / k_v^{*m} \times k_v^* / k_v^{*m} & \xrightarrow{(\cdot, \cdot)_v} & \mu_m
\end{array}
$$

commutes, where $i$ denotes an isomorphism defined by $i(n/m) = e_\phi(P_0, P'_0)^n$.

**Proof.** This proposition is essentially the same as [19], Lemma 2.7, so we have only to mimic the proof. Let $\xi \in H^1(k_v, E_\phi)$ and $\xi' \in H^1(k_v, E_\phi')$ be represented by the cocycles $[\sigma \mapsto n_0P_0]$ and $[\sigma \mapsto n'_0P'_0]$ respectively. Then

$$(\xi \cup \xi')(\sigma, \tau) = e_\phi(n_0P_0, n'_0P'_0) = \xi^{n_0n'_0},$$

where we have put $\zeta = e_\phi(P_0, P'_0)$. It is easy to see that $i_v(\xi)$ and $i'_v(\xi')$ are represented by the cocycles $[\sigma \mapsto \zeta^{n_0\sigma}]$ and $[\sigma \mapsto \zeta^{n'_0\sigma}]$ respectively, hence

$$(i_v(\xi) \cup i'_v(\xi'))(\sigma, \tau) = \zeta^{n_0\sigma} \otimes \zeta^{n'_0\sigma} = \xi^{n_0\sigma} \otimes \zeta.$$

Thus we have a commutative diagram

$$
\begin{array}{ccc}
H^1(k_v, E_\phi) \times H^1(k_v, E_\phi') & \xrightarrow{\langle \cdot, \cdot \rangle_v} & H^2(k_v, \mu_m) \\
\downarrow i_v \times i'_v & & \downarrow \otimes \zeta \\
H^1(k_v, \mu_m) \times H^1(k_v, \mu_m) & \xrightarrow{\cup} & H^2(k_v, \mu_m^\otimes 2).
\end{array}
$$

On the other hand, by [26], Ch. XIV Proposition 5 we have a commutative diagram

$$
\begin{array}{ccc}
H^1(k_v, \mu_m) \times H^1(k_v, \mu_m) & \xrightarrow{\cup} & H^2(k_v, \mu_m^\otimes 2) \\
\downarrow \kappa_v \times \kappa'_v & & \downarrow \nu \\
k_v^* / k_v^{*m} \times k_v^* / k_v^{*m} & \xrightarrow{(\cdot, \cdot)_v} & \mu_m.
\end{array}
$$

where $\nu$ is an isomorphism defined by the composition of maps

$$
H^2(k_v, \mu_m^\otimes 2) \xrightarrow{\sim} H^2(k_v, \mu_m) \otimes \mu_m \xrightarrow{\text{inv}_v} \frac{1}{m}Z/Z \otimes \mu_m \xrightarrow{\sim} \mu_m.
$$

It is easy to check that the composite map

$$
\frac{1}{m}Z/Z \xrightarrow{\text{inv}_v^{-1}} H^2(k_v, \mu_m) \xrightarrow{\otimes \zeta} H^2(k_v, \mu_m^\otimes 2) \xrightarrow{\nu} \mu_m
$$

coincides with $i$. Combining (2.3) with (2.4), we completes the proof. $\square$
The following theorem is called Tate's local duality theorem.

**Theorem 2.2 (Tate).** Let $A$ be an elliptic curve defined over a local field $k_v$. Then there is a perfect pairing

$$A(k_v) \times H^1(k_v, A) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$ 

Moreover this pairing is compatible with the cup product

$$H^1(k_v, A_m) \times H^1(k_v, A_m) \longrightarrow \frac{1}{m} \mathbb{Z}/\mathbb{Z}$$

induced by Weil's $e_n$-pairing.

**Proof.** See [30] or [22].

For any subgroup $V$ of $k_v^*/k_v^{*m}$, let

$$V^\perp = \{ \xi \in k_v^*/k_v^{*m} | (\xi, \zeta)_v = 1 \text{ for all } \zeta \in V \}.$$ 

Recall that we have injections

$$\delta_v : E(k_v)/\phi(E(k_v)) \longrightarrow H^1(k_v, E_\phi)$$

and

$$\delta'_v : E(k_v)/\phi'(E(k_v)) \longrightarrow H^1(k_v, E_{\phi'}).$$

In the following, we identify $\text{Im}(\delta_v)$ and $\text{Im}(\delta'_v)$ with the corresponding subgroups of $k_v^*/k_v^{*m}$ via $j_v$ and $j'_v$ respectively. The above theorem then gives us the following important relation between $\text{Im}(\delta_v)$ and $\text{Im}(\delta'_v)$, which is proved by Cassels ([5]) when $E = E'$. (See also [19], Proposition 1.14.) To state it, let $| \cdot |_v$ be the $v$-adic absolute value normalized as $|p|_v = p^{-n_v}$, where $p$ is the characteristic of the residue field of $v$ and $n_v = [k_v : \mathbb{Q}_p]$.

**Corollary 2.3.** Notation being as above, we have $\text{Im}(\delta_v) = \text{Im}(\delta'_v)^{-1}$. In particular, if $v$ is a finite place, then $| \text{Im}(\delta_v) | \cdot | \text{Im}(\delta'_v) | = \frac{m^2}{m_1^{-1}}$.

**Proof.** By the above theorem, we have a perfect pairing

$$E(k_v)/\phi'(E(k_v)) \times H^1(k_v, E_\phi) \longrightarrow \frac{1}{m} \mathbb{Z}/\mathbb{Z}$$

which is compatible with the pairing $\langle , \rangle_v$. Since $H^1(k_v, E_\phi) \cong H^1(k_v, E_{\phi'})/\text{Im}(\delta_v)$, this shows that $\text{Im}(\delta'_v)$ is the exact annihilator of $\text{Im}(\delta_v)$ with respect to $\langle , \rangle_v$. Therefore the first statement follows from Proposition 2.1. The second statement follows from the formula $| k_v^*/k_v^{*m} | = m^2 | m_1^{-1} |$ (See [1]).

3. **An estimate of the Selmer group**

We continue to use the notation of the previous sections. We assume that $m \geq 3$.
and $k$ contains $\mu_m$. Let $K = k(\phi^{-1}(E'(k)_m))$. The $K$ is a Galois extension of $k$; let $G = Gal(K/k)$. Let us start with the following well known result.

**Proposition 3.1.** Let $B = \delta(E'(k)_m)$ be the subgroup of $k^*|k^{star}$ generated by the image of $E'(k)_m$. Then $K = k(\sqrt[m]{\delta})$. In particular, $[K : k] = |E'(k)_m/\phi(E(k)_m)|$.

**Proof.** Let $L$ be any field containing $k$. Then we have a commutative diagram

\[
\begin{array}{ccc}
E'(k)/\phi(E(k)) & \xrightarrow{\delta} & H^1(k, E_\phi) \cong k^*/k^{star} \\
\downarrow & & \downarrow \text{res}_{L/k} \\
E'(L)/\phi(E(L)) & \xrightarrow{\delta_L} & H^1(L, E_\phi) \cong L^*/L^{star},
\end{array}
\]

(3.1)

where the left vertical map is the one induced from the inclusion $E'(k) \subset E'(L)$ and $\text{res}_{L/k}$ denotes the restriction map. Let $P$ be any $k$-rational point of $E'$. Then we can show that $L$ contains $k(\phi^{-1}(P))$ precisely when $L$ contains $k(\sqrt[m]{\delta(P)})$ as follows:

- $k(\phi^{-1}(P)) \subset L$
- $P \in \phi(E(L))$
- $\delta_L(P) = 0$ (by the injectivity of $\delta_L$)
- $\delta(P) \in k^* \cap L^{star}/k^{star}$ (by the commutativity of (3.1))
- $k(\sqrt[m]{\delta(P)}) \subset L$.

Therefore $k(\sqrt[m]{\delta(P)}) = k(\phi^{-1}(P))$ for any $P \in E'(k)$, hence $K = k(\sqrt[m]{\delta})$ as required. Kummer theory shows that there is an isomorphism $Gal(K/k) \cong Bk^{star}/k^{star}$, which is isomorphic to the cyclic group $E'(k)_m/\phi(E(k)_m)$. This completes the proof.

Now we consider the following condition:

(C) $E'(k)_m/\phi(E(k)_m)$ is cyclic.

This condition is satisfied, for example, if $E'(k)_m$ itself is cyclic.

**Corollary 3.2.** If the condition (C) holds, then $K$ is a cyclic extension of $k$ of degree $|E'(k)_m/\phi(E(k)_m)|$.

To state our main result of this section, we fix some notation. We denote by $R$ the set of finite places of $k$ which ramify in $K$, and put $T = S \cap R$. For any $v \in R$ we denote by $e_v$ the relative ramification index of $v$ in $K/k$, and put

\[
e = \prod_{v \in R} e_v.
\]

(3.2)

If $L$ is a finite extension of $k$, we denote by $T(L)$ the set of places of $L$ lying above places in $T$ and by $Cl_{L, T}$ the $T(L)$-ideal class group of $L$.

**Theorem 3.3.** Assume that the condition (C) holds. Then
\[ |S^{(\phi)}(E/k)| \leq \frac{[K : k]m^{d/2} + |T|}{e} \cdot \frac{|(Cl_{K,\tau})^G|}{|(Cl_{k,\tau})^m|}, \]

where \( d = [k : Q] \).

Before starting the proof we prove a lemma which will be needed in the proof. A similar results is already proved in [5].

**Lemma 3.4.** For any finite place \( v \) of \( k \), let \( \nu_v = |E(k_v)_{\infty}| \) and \( \nu'_v = |E(k_v)_{m\infty}| \). Then we have \( |\text{Im}(\delta_v)| \geq m \cdot \nu'_v / \nu_v \) and \( |\text{Im}(\delta'_v)| \geq m \cdot \nu_v / \nu'_v \). Moreover, if \( v \) is prime to \( m \), then \( \text{Im}(\delta_v) \) and \( \text{Im}(\delta'_v) \) are generated by images of \( E(k_v)_{m\infty} \) and \( E(k_v)_{m\infty} \) respectively, and their orders are given by

\[ |\text{Im}(\delta_v)| = m \cdot \frac{\nu'_v}{\nu_v}, \quad |\text{Im}(\delta'_v)| = m \cdot \frac{\nu_v}{\nu'_v}. \]

**Proof.** The inclusion map \( E'(k_v)_{m\infty} \hookrightarrow E'(k_v) \) induces the injection

\[ E'(k_v)_{m\infty} / \phi(E(k_v)_{m\infty}) \hookrightarrow E'(k_v) / \phi(E(k_v)). \]

Since \( |\phi(E(k_v)_{m})| = \nu_v / m \), this implies that

\[ |E'(k_v) / \phi(E(k_v))| \geq m \cdot \frac{\nu'_v}{\nu_v}, \]

which proves the first inequality. The proof of the second one is quite similar. If \( v \notin S_m \), then by Corollary 2.3 we have

\[ |E'(k_v) / \phi(E(k_v))| \cdot |E(k_v) / \phi'(E(k_v))| = m^2. \]

Therefore both inequalities above are actually equalities, which proves the second statement.

**Proof of Theorem 3.3.** In Section 1 we have seen that \( S^{(\phi)}(E/k) \) consists of elements \( \xi \in H^1(k_{\phi}/k, E_{\phi}) \cong k^*/k^{*m} \) satisfying \( \text{res}_v(\xi) \in \text{Im}(\delta_v) \) for all \( v \in S \). Since \( k \) is totally imaginary, we have only to consider the finite places. Take \( P \in E'(k)_{m\infty} \) whose image generates \( E'(k)_{m\infty} / \phi(E(k)_{m\infty}) \) and put \( a = \delta(P) \in k^*/k^{*m} \). Then \( K = k(\sqrt[n]{a}) \) by Proposition 3.1. By Lemma 3.4, \( \text{Im}(\delta_v) \) is generated by the image of \( P \), hence by Corollary 2.3 we have \( \text{Im}(\delta_v) \subset \langle a \rangle_v \), where \( \langle a \rangle_v \) denotes the subgroup of \( k^*/k^{*m} \) generated by \( a \). Since \( K = k(\sqrt[n]{a}) \), this shows that \( \langle a \rangle_v \cong N_{K_{w}/k_v}(K_w^*) \) (mod. \( k_v^{*m} \)), where \( w \) is any place of \( K \) lying above \( v \). If \( K_{w}/k_v \) is an unramified extension, then \( N_{K_{w}/k_v}(K_w^*) \equiv N_{K_{w}/k_v}(C_w^*) \) (mod. \( k_v^{*m} \)), where \( C_w^* \) denotes the maximal order of \( K_w \). Thus we have proved the following inclusion:

\[ \text{Im}(\delta_v) \subset \begin{cases} N_{K_{w}/k_v}(K_w^*) / k_v^{*m} \cong k_v^{*m} / k_v^{*m}, & \text{if } v \in T, \\ N_{K_{w}/k_v}(C_w^*) / k_v^{*m} \cong k_v^{*m} / k_v^{*m}, & \text{if } v \notin T. \end{cases} \]

Let \( J_{K, \tau} \) be the \( T \)-idèle group of \( K \) (see Section 5 for the definition). Then (3.3)
combined with (5.4) implies that there is an injection
\[ S^{(\phi)}(E/k) \hookrightarrow \ker(H^1(k_T/k, \mu_m) \longrightarrow \tilde{H}^0(G, J_{K,T})). \]
Let us define a map
\[ \lambda_T : U_{k,T}k^{*m}/k^{*m} \longrightarrow \tilde{H}^0(G, J_{K,T}) \]
as the composition of the natural surjection \( U_{k,T}k^{*m} \twoheadrightarrow \tilde{H}^0(G, U_{K,T}) \) and the map
\[ \alpha_2 : H^0(G, U_{K,T}) \longrightarrow \tilde{H}^0(G, J_{K,T}) \]
defined in Section 5. (Note that \( H^2 = \tilde{H}^0 \) since \( G \) is assumed to be cyclic.) It then follows from the definition of \( \lambda_T \) that
\[ |\ker \lambda_T| = \left| \frac{U_{k,T}/U_{k,T}^m}{\tilde{H}^0(G, U_{K,T})} \right| \cdot |\ker \alpha_2| = \frac{m^{d/2 + |T|}}{|\tilde{H}^0(G, U_{K,T})|} \cdot |\ker \alpha_2|. \]
On the other hand the exact sequence (1.11) replaced \( S \) by \( T \) implies that
\[ |S^{(\phi)}(E/k)| \leq |(C_{k,T})_m| \cdot |\ker \lambda_T|. \]
Consequently from (3.4) Theorem 5.1 we get
\[ |S^{(\phi)}(E/k)| \leq |(C_{k,T})_m| \cdot \frac{|K : k| m^{d/2 + |T|}}{|C_{k,T}|}. \]
Here note that \( f_T = 1 \) since \( T \subset R \) by definition. Moreover we have
\[ \frac{|C_{k,T}|}{|(C_{k,T})_m|} = |(C_{k,T})_m|. \]
From (3.5) and (3.6) we obtain the required inequality. \( \square \)

In what follows we assume that \( m = p \) is an odd prime number. For \( E' \), we define \( K', R' \) and \( T' \) in the same manner as for \( E \).

**Theorem 3.5.** Suppose that both \( E'(k)_{p^\infty}/\phi(E(k)_{p^\infty}) \) and \( E(k)_{p^\infty}/\phi'(E'(k)_{p^\infty}) \) are cyclic groups of order \( p \). Then
\[ \operatorname{rank} E(k) \leq [k : Q] - r + \operatorname{ord}_p \left( \frac{|(C_{K,T})_T^G|}{|(C_{k,T})_m^G|} \right) + \operatorname{ord}_p \left( \frac{|(C_{K,T}^T)^G|}{|(C_{k,T})_m^T|^p} \right), \]
where \( r = |R \setminus T| + |R' \setminus T'|. \)

**Proof.** By Corollary 3.2, the assumption implies that \([K : k] = [K' : k] = p\). It then follows from Theorem 3.3 that
\[ \operatorname{dim} S^{(\phi)}(E/k) \leq 1 + \frac{d}{2} + |T| - |R| + \operatorname{ord}_p \left( \frac{|(C_{K,T})_T^G|}{|(C_{k,T})_m^T|^p} \right), \]
where \( d = [k : Q] \). Similarly, applying the same theorem to \( E' \) we get
(3.8) \[ \dim S^{(\phi)}(E'/k) \leq 1 + \frac{d}{2} + |T'| - |R'| + \text{ord}_p \left( \frac{|(Cl_{k,T})^e|}{|(Cl_{k,T})^p|} \right). \]

Then from (3.7), (3.8) and Proposition 1.1 we obtain a bound of rank \( E(k) \):

(3.9) \[ \text{rank } E(k) \leq d - r + \text{ord}_p \left( \frac{|(Cl_{k,T})^e|}{|(Cl_{k,T})^p|} \right) + \text{ord}_p \left( \frac{|(Cl_{k,T})^e|}{|(Cl_{k,T})^p|} \right), \]

where \( r = |R \setminus T| + |R' \setminus T'| \). This proves the theorem. □

As an example of Theorem 3.6, let us consider the elliptic curve \( E \) defined by the equation

(3.10) \[ y^2 = 4x^3 + a^2(x - b)^2, \]

where \( a \) and \( b \) are integers of \( k \) with \( ab(a^2 + 27b) \neq 0 \). Then the order of the point \( P_0 = (0, ab) \in E(k) \) is three, and it induces a \( k \)-rational cyclic 3-isogeny \( \phi : E \to E' := E/\langle P_0 \rangle \). Conversely it is easy to see that every elliptic curve defined over \( k \) with a non-zero \( k \)-rational 3-torsion point may be defined either by (3.10) or by the equation \( y^2 = 4x^3 + a^2 \). The latter curve has complex multiplication and will be treated in the next section. The following explicit description of \( E' \) and \( \phi \) are essentially given in [31]:

\[ E' : y^2 = 4x^3 - 27a^2(x - a^2 - 27b)^2, \]

\[ \phi((x, y)) = \left( \frac{9(y^2 + a^2b^2 - (1/3)a^2x^2 - 2x^3)}{2x^2}, \frac{27y(2a^2b^2 - a^2bx - x^3)}{2x^3} \right). \]

It easily follows from this explicit formula that

\[ K = K' = k(\sqrt[3]{a^2b(a^2 + 27b)}) \]

hence \( R = R' \). The discriminants of \( E \) and \( E' \) are given by \( -a^4b^3(a^2 + 27b) \) and \( -3^{12}a^4b(a^2 + 27b)^3 \) respectively. If we denote by \( S_0 \) the set of finite places in \( S \), this shows that

\[ S_0 = \{ v \in M_{k,0} \mid \text{ord}_v(3ab(a^2 + 27b)) > 0 \}. \]

Thus \( R \subset S_0 \) and \( T = T' = R \). Then Theorem 3.5 for \( E/k \) reads as follows:

**Theorem 3.6.** Let \( E \) be an elliptic curve defined over \( k \) by the equation (3.10) and put \( K = k(\sqrt[3]{a^2b(a^2 + 27b)}) \). Suppose that \( k \) contains \( \mathcal{O}(\sqrt{-3}) \) and \( k \neq K \). Then

\[ \text{rank}(E/k) \leq [k: \mathcal{O}] + 2 \text{ord}_3 \left( \frac{|(Cl_{k,R})^e|}{|(Cl_{k,R})^p|} \right), \]

where \( R \) denotes the set of finite places of \( k \) which ramify in \( K \).
4. Elliptic curves with complex multiplication

Let $p$ be an odd prime as before. In this section we assume that $E$ has complex multiplication by $\mathbb{Z}[\sqrt{-p}]$, that is $\text{End}(E)$ contains $\mathbb{Z}[\sqrt{-p}]$. (We refer to [27] or [29] for the basic results on complex multiplication theory.) Moreover we assume that $k$ contains $H(\sqrt{-p}, \mu_p)$, where $H$ denotes the Hilbert class field of $\mathbb{Q}(\sqrt{-p})$. Let us take $\pi=\sqrt{-p} \in \text{End}(E)$ for $\phi$ in the previous section. Thus $E=E'$. Under the above assumption, $\phi$ is defined over $k$ and $E(k) \cong \mathbb{Z}/p\mathbb{Z}$. Let $P_0$ be a generator of $E_\pi$. Let $K=k(E_\pi)$ and put $G=\text{Gal}(K/k)$. If we take an element $a \in \mathcal{O}_k$ such that $a \equiv \delta(P_0) \pmod{k^{*p}}$, then we can show as before that $K=k(\sqrt[p]{a})$. Moreover we suppose that $K$ is strictly larger than $k$. If this condition is satisfied, then $[K:k]=p$ and the condition (C) in Section 3 is satisfied. Recall that $S_0$ denotes a subset of $S$ consisting of finite places in $S$ and that $R$ denotes the set of places of $k$ which ramify in $K$. Let $S_p$ be the set of places of $k$ lying above $p$.

Lemma 4.1. $S_0 \setminus S_p \subset R \setminus S_p$.

Proof. For $v \in S_0 \setminus S_p$, let $w$ be a place of $K$ lying above $v$. Then $E$ has good reduction at $w$ since $E(K_w) \cong E_p$ and $p \geq 3$ (see [27]), and consequently $K_w/k_v$ is a ramified extension ([28] VII, Proposition 5.4). This shows that $v \in R \setminus S_p$.

Lemma 4.2. If $v \in S_0 \setminus S_p$, then $\text{Im}(\delta_v)$ is generated by the image of $P_0$.

Proof. If $v \in S_0 \setminus S_p$, then $v$ ramifies in $K/k$ by the above lemma. Hence $K_{k_v} \neq k_v$, so $E(k_v)^* \neq E_\pi$. Then the assertion follows from Lemma 3.4.

Now in view of Lemma 4.2 the same argument as in the proof of Theorem 3.3 shows that $\text{Im}(\delta_v) = N_{K_{k_v}/k_v}(K_v)^{*k_v}/(k_v)^{*p}$ for all $v \in S_0 \setminus S_p$. As for $\text{Im}(\delta_v), v \in S_p$, we can use a result due to Berković [2]. To state it we introduce some notation.

For each $v \in S_p$, put $e_{v,0}=[k_v : \mathcal{O}_v]/(p-1)$. Since $k$ contains $\mathcal{O}(\mu_p)$, $e_{v,0}$ is an integer. For each integer $i \geq 0$, let

$$U_{v,i} = \{ x \in \mathcal{O}_v^* | \text{ord}_v(x-1) \geq i \}.$$  

Thus $U_{v,0}$ equals $\mathcal{O}_v^*$. This induces a filtration on $\mathcal{O}_v^*/\mathcal{O}_v^{*p}$:

$$\mathcal{O}_v^*/\mathcal{O}_v^{*p} = C_{v,0} \supset C_{v,1} \supset \cdots \supset C_{v,e_{v,0}+1} = \{1\}.$$  

Lemma 4.3. Suppose that $p \geq 5$. Then $\text{Im}(\delta_v) = C_{v,(e_{v,0}+1)/2}$.

Proof. See [2], Corollary 3.3.3 and Corollary 3.4.4.

In order to state the main result of this section, let

$$R_p = \{ v \in S_p \mid a \notin U_{v,e_{v,0}} \}.$$  

Then $R \cap S_p = R_p$. (See [17], Chapter 1, Proposition 1.84.) Let

$$(4.2) \quad T = S_0 \setminus S_p.$$
Then by Lemma 4.1, we find that \((S_0 \setminus S_p) \cup R_p \subseteq R\).

**Theorem 4.4.** Let \(p \geq 5\). Then

\[
\dim S^{(\infty)}(E/k) \leq 1 + \frac{[k : \mathcal{O}]}{2} - |R_p| + \text{ord}_p \left( \frac{|(\text{Cl}_{K, T})^G|}{|((\text{Cl}_{K, T})^p)|} \right).
\]

**Proof.** As in the proof of Theorem 3.3 we see that the image \(\text{Im}(\delta_v)\) for every \(v \in S_0\) is contained in \(N_{K_w/k_v}(K_v^*)k^*/k^*\). For \(v \in S_p\), Lemma 4.3 shows that \(\text{Im}(\delta_v)\) is contained in the image of \(N_{K_w/k_v}(K_v^*) \cap \mathcal{O}_v^* = N_{K_w/k_v}(\mathcal{O}_v^*)\). Therefore,

\[
\text{Im}(\delta_v) = \begin{cases} 
N_{K_w/k_v}(K_v^*)k^*/k^*, & \text{if } v \in T, \\
N_{K_w/k_v}(\mathcal{O}_v^*)k^*/k^*, & \text{if } v \notin T.
\end{cases}
\]

Now the remaining part of the proof is quite similar to that of Theorem 3.3. \(\square\)

**Corollary 4.5.** **Notation being as in Theorem 4.4, we have**

\[
\text{rank } E(k) \leq \frac{[k : \mathcal{O}]}{2} - 2|R_p| + 2\text{ord}_p \left( \frac{|(\text{Cl}_{K, T})^G|}{|((\text{Cl}_{K, T})^p)|} \right).
\]

**In particular, if Cl}_{K, T} = 0, then** \(\text{rank } E(k) \leq 2|S \setminus S_p|\).

**Proof.** The first statement follows from (1.13) and the above theorem. The second one follows from this and Corollary 5.5. \(\square\)

Now suppose that there is a subfield \(k_0\) of \(k\) such that \([k : k_0] = 2\) and \(k = k_0(\sqrt{-3})\). When \(E\) is already defined over \(k_0\), we obtain a bound of rank \(E(k_0)\) by (1.14).

**Corollary 4.6.** **If \(E\) is defined over \(k_0\), then**

\[
\text{rank } E(k_0) \leq \frac{[k : \mathcal{O}]}{2} - |R_p| + \text{ord}_p \left( \frac{|(\text{Cl}_{K, T})^G|}{|((\text{Cl}_{K, T})^p)|} \right).
\]

**In particular, if Cl}_{K, T} = 0, then** \(\text{rank } E(k_0) \leq |S \setminus S_p|\).

It seems very likely that Theorem 4.4 holds also for \(p = 3\). For example, in a special case with \(p = 3\), we can prove that the equality of the theorem holds. To state it, we restrict ourselves to the case of \(k = \mathcal{O}(\sqrt{-3})\) in the remaining part of this section. Let \(E\) be an elliptic defined by the equation

\[
y^2 = 4x^3 + a^2,
\]

where \(a\) is a non-zero cube-free integer of \(k\). Let \(\omega\) be a primitive cubic root of unity. Then \(E\) has complex multiplication by \(\mathcal{O}_k = \mathbb{Z}[\omega]\); the action of \(\omega\) is given by \((x : y) \rightarrow (\omega x : y)\). Let \(\pi = \sqrt{-3} \in \text{End}(E)\). Then

\[
E_\pi = \{O, (0, a), (0, -a)\}.
\]

A simple calculation shows that the other 3-torsion points are \((-\omega^{13}\sqrt{a^2}, \pm \sqrt{-3a})\).
with \( i = 0, 1, 2 \). Therefore \( k = k(\sqrt[3]{a}) \). The discriminant of this curve is \(-27a^4\), hence \( S_0 \) is the set of places of \( k \) dividing \( 3a \). Let \( T = S_0 \setminus S_3 \) as before.

**Theorem 4.7.** Let \( E \) be an elliptic curve defined over \( k = \mathbb{Q}(-3) \) by (4.3). Suppose that \( a \equiv \pm 1 \) (mod. 3) but \( \not\equiv \pm 1 \) (mod. \( 3\sqrt{-3} \)). Then

\[
\dim S^{(\alpha)}(E/k) = 1 + \text{ord}_3 |(Cl_{K,T})^G|.
\]

**Proof.** By a direct calculation we can easily check that \( \text{Im}(\delta_v) = C_{v,2} \) in the notation of (4.1) for the unique \( v \) lying above \( 3 \), namely Lemma 4.3 holds in this case also. Then we find that

\[
(4.4) \quad \text{Im}(\delta_v) = \begin{cases} N_{K_i/k}(K^{*}_{i})k^{*p}/k^{*p}, & \text{if } v \in T, \\ C_{v,2}, & \text{if } v \notin T. \end{cases}
\]

If \( a \) satisfies the assumption of the statement, then \( \langle a \rangle _{v}^{\perp} = C_{v,2} \) for \( v \in S_3 \), hence \( \langle a \rangle _{v}^{\perp} = \text{Im}(\delta_v) \). Since \( K = k(\sqrt[3]{a}) \), we have

\[
\langle a \rangle _{v}^{\perp} = N_{K_i/k}(K^{*}_{i})k^{*p}/k^{*p}.
\]

Consequently from this and (4.4) we find that \( \langle a \rangle _{v}^{\perp} = \text{Im}(\delta_v) \) for all \( v \in S \). Therefore every inequality in the proof of Theorem 3.3 may be replaced by the equality. Thus we have a formula:

\[
\dim S^{(\phi)}(E/k) = 1 + \frac{d}{2} - |R \setminus T| + \text{ord}_3 |(Cl_{K,T})^G|.
\]

The assumption on \( a \) implies that \( R = S_0 \). Hence \( d/2 - |R \setminus T| = 1 - 1 = 0 \), which completes the proof.

**Corollary 4.8.** Let \( E \) be as in theorem 4.7. Then

\[
\text{rank } E(k) \leq 2 \text{ord}_3 |(Cl_{K,T})^G|.
\]

In particular, \( \text{rank } E(k) \leq 2(|S| - 1) \).

Now let us consider the case where the defining field of \( E \) can be descended to \( \mathbb{Q} \). In this case, by (1.14) we obtain the following result.

**Corollary 4.9.** Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) by (4.3) with \( a \in \mathbb{Z} \). Suppose that \( a \equiv 2, 4, 5, 7 \) (mod. 9). Then

\[
\text{rank } E(\mathbb{Q}) \leq \text{ord}_3 |(Cl_{K,T})^G|,
\]

where \( K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{a}) \) and where \( T \) denotes the set of places of \( \mathbb{Q}(\sqrt{-3}) \) dividing \( a \). In particular, \( \text{rank } E(\mathbb{Q}) \leq (|S| - 1) \).

In actual calculations of \( S^{(\phi)}(E/k) \), the formula (3.4) is more convenient than the above theorem. To make it clear, let
ind : $\mu_p \sim \mathbb{Z}/p\mathbb{Z}$

be any isomorphims. For $T = \{v_1, \cdots, v_t\} \subset R$, let $\{u_1, \cdots, u_s\}$ ($s = t + d/2$) be a basis of $U_{k, T}$. If $K = k(\sqrt[2]{a})$ with some $s \in k$, then the kernel of the map $\lambda_T$ defined in Section 3 have the following representation:

$$\dim(\ker \lambda_T) = t - \text{rank } A_T,$$

where $A_T$ is a $t \times s$-matrix with entries in $\mathbb{Z}/p\mathbb{Z}$ defined by

$$A_T = (\text{ind}(u_p, a)_{ij})_{1 \leq i \leq t, 1 \leq j \leq s}.$$

Of course the matrix $A_T$ depends on the choice of the isomorphism ind, but the rank of $A_T$ does not. Thus from (3.4) we obtain the following formula:

**Theorem 4.10.** If $p \geq 5$, notation being as in Theorem 4.4, we have

$$\dim S^t(E/k) \leq \dim Cl_{k, T} + |T| - \text{rank } A_T.$$

If $p = 3$, notation being as in Theorem 4.7, we have

$$\dim S^t(E/k) = |T| - \text{rank } A_T.$$

It is easy to see that the second part of the above theorem is closely related to the work of Satge ([24]).

### 5. Appendix: The genus formula

The aim of this section is to prove Theorem 5.1 below. We refer to [1], [6], [17] or [26] for the fundamental results of class field theory that we will use in this section. The notation of this section will be independent of that of the previous sections.

Let $K/k$ be a finite Galois extension of algebraic number fields and $G = Gal(K/k)$ its Galois group. As in Section 1, let $M_k$ (resp. $M_K$) be the set of the places of $k$ (resp. $K$). Let $T$ be a finite set of places of $k$ and $T(K)$ the set of places of $K$ lying above places of $T$. Let $J_K$ be the idele group of $K$. We consider the subgroup $J_{K, T}$ of $J_K$ defined by

$$J_{K, T} = \prod_{w \in M_K \setminus T(K)} \mathcal{O}_w^* \times \prod_{w \in T(K)} K_w^* ,$$

where, for an infinite place $w$, $\mathcal{O}_w^*$ denotes $\mathbb{R}$ or $\mathbb{C}$ according as $w$ is real or complex. The group of $T(K)$-units of $K$ is defined by

$$U_{K, T} = \left\{ u \in K^* \mid w(u) > 0 \text{ for all real } w \in M_{K, \infty} \setminus T(K) \text{ and ord}_w(u) = 0 \text{ for all } w \in M_{K, 0} \setminus T(K) \right\} ,$$

where $M_{K, \infty}$ (resp. $M_{K, 0}$) denotes the set of infinite (resp. finite) places of $K$. We define a group $C_{K, T}$ by the exact sequence
Selmer Groups and Ideal Class Groups

(5.1) \[ 0 \rightarrow U_{K,T} \xrightarrow{\alpha} J_{K,T} \xrightarrow{\beta} C_{K,T} \rightarrow 0, \]

where \( \alpha \) denotes the diagonal embedding. Then, taking cohomology groups, we obtain a long exact sequence

\[
\begin{align*}
0 & \longrightarrow H^0(G, U_{K,T}) \xrightarrow{\alpha_0} H^0(G, J_{K,T}) \xrightarrow{\beta_0} H^0(G, C_{K,T}) \\
& \quad \longrightarrow H^1(G, U_{K,T}) \xrightarrow{\alpha_1} H^1(G, J_{K,T}) \xrightarrow{\beta_1} H^1(G, C_{K,T}) \\
& \quad \longrightarrow H^2(G, U_{K,T}) \xrightarrow{\alpha_2} H^2(G, J_{K,T}) \xrightarrow{\beta_2} H^2(G, C_{K,T}) \\
& \quad \cdots
\end{align*}
\]

(5.2)

For \( v \in M_k \), we denote by \( e_v \) and \( f_v \) the relative ramification index and the relative degree of \( v \) in \( K/k \) respectively. Put

\[ e_T = \prod_{v \in T} e_v, \quad f_T = \prod_{v \in T} f_v. \]

When \( T \) contains all the places which ramify in \( K/k \), we simply write \( e \) for \( e_T \).

**Theorem 5.1.** Suppose that \( G \) is cyclic. Then

\[ |\text{Ker}(\alpha_2)| = \frac{|K : k| \cdot |\hat{H}^0(G, U_{K,T})| \cdot |(\text{Cl}_{K,T})^G|}{ef_T \cdot |\text{Cl}_{K,T}|}. \]

When \( T = M_{k,\infty} \), this is nothing but the well known genus formula (see [7], [12], [13], or [32]). When \( |G| \) is a prime, this is proved by Gras [13], and in the general case this follows from Federer’s formula ([7] Appendix, Theorem 30.3). Our proof is essentially the same as that of Federer, but not entirely identical; we shall use idèle groups, which is more suitable for our application, while she used ideal groups.

Before going into the proof, we prove some lemmas. Let

\[ C_K = J_K/K^* \]

be the idèle class group of \( K \). Then the inclusion map \( J_{K,T} \hookrightarrow J_K \) induces a map \( C_{K,T} \rightarrow C_K \). Since the kernel of this map is \((K^* \cap J_{K,T})/U_{K,T} = 0\), we can regard \( C_{K,T} \) as a subgroup of \( C_K \). Let \( \text{Cl}_{K,T} \) (resp. \( \text{Cl}_{k,T} \)) be the \( T(K) \)-ideal class group of \( K \) (resp. \( T \)-ideal class group of \( k \)).

**Lemma 5.2.** There is an exact sequence

\[
0 \rightarrow C_{K,T} \rightarrow C_K \rightarrow \text{Cl}_{K,T} \rightarrow 0.
\]

In particular, \( C_K/C_{k,T} \cong \text{Cl}_{k,T} \).
Proof. We can easily see that the quotient group $J_K/J_{K, T}$ is isomorphic to $Cl_{K, T}$. Therefore the exact sequence
\[ 0 \rightarrow K^*/U_{K, T} \rightarrow J_K/J_{K, T} \rightarrow C_K/C_{K, T} \rightarrow 0 \]
shows that $C_K/C_{K, T}$ is isomorphic to $Cl_{K, T}$. The second statement follows from this applied to $K = k$. \hfill \Box

To state the next lemma, let us denote by $i_{k \rightarrow K} : C_K \rightarrow C_K$ the natural map induced by the inclusion $k \hookrightarrow K$. Then this map is known to be injective and $i_{k \rightarrow K}(C_k) = (C_K)^G$.

Lemma 5.3. $\text{Ker}(\alpha_1) \cong (C_{K, T})^G/i_{k \rightarrow K}(C_K)$.

Proof. Since $(U_{K, T})^G = U_T$ and $(J_{K, T})^G = J_T$, we have an exact sequence
\[ 0 \rightarrow U_T \rightarrow J_T \rightarrow (C_{K, T})^G \rightarrow \text{Ker}(\alpha_1) \rightarrow 0. \]
Hence we see that
\[ \text{Ker}(\alpha_1) \cong \text{Coker}(\beta_0) \cong (C_{K, T})^G/i_{k \rightarrow K}(C_K), \]
which proves the lemma. \hfill \Box

Lemma 5.4. $|H^0(G, J_{K, T})| = e_T f_T$.

Proof. For each $v \in M_K$, we choose and fix a place $w$ of $K$ lying above $v$. Then by semi-local therem, we have
\begin{equation}
\hat{H}^0(G, J_{K, T}) \cong \bigoplus_{v \notin T(K)} \hat{H}^0(G, \mathcal{O}_w^\times) \oplus \bigoplus_{v \in T(K)} \hat{H}^0(G, K_v^\times).
\end{equation}
Since $\hat{H}^0(G, \mathcal{O}_w^\times) \cong \mathbb{Z}/e_v \mathbb{Z}$ and $\hat{H}^0(G, K_v^\times) \cong \mathbb{Z}/[K_w : k_v] \mathbb{Z}$ by local class field theory, we have
\[ |\hat{H}^0(G, J_{K, T})| = \frac{e}{e_T} \cdot \prod_{v \notin T} [K_w : k_v]. \]
Since $[K_w : k_v] = e_v f_v$, the right hand side equals $e_T f_T$, hence the assertion holds. \hfill \Box

Proof of Theorem 5.1. By (5.2), we have
\begin{equation}
|\text{Ker}(\alpha_2)| = \frac{|H^1(G, U_{K, T})|}{|H^1(G, J_{K, T})|} \cdot \frac{|H^1(G, C_K)|}{|\text{Ker}(\alpha_1)|}.
\end{equation}
Since $Cl_{K, T}$ is finite, taking the Herbrand quotient of each term in the exact sequence of Lemma 5.2, we have $Q(C_K) = Q(C_K)$. By class field theory we know that $Q(C_K) = [K : k]$, hence
\begin{equation}
Q(C_{K, T}) = [K : k].
\end{equation}
Let us compute the first factor of the right hand side of (5.5). By the exact sequence (5.1) we obtain $Q(J_{K, T}) = Q(U_{K, T})Q(C_K)$. This implies that
Selmer Groups and Ideal Class Groups

\[ \frac{|H^1(G, U_{K,T})|}{|H^1(G, J_{K,T})|} = \frac{|\hat{H}^0(G, U_{K,T})|}{|\hat{H}^0(G, J_{K,T})|} \cdot Q(C_{K,T}) \cdot e_f. \]

It then follows from Lemma 5.4 and (5.6) that
\[ (5.7) \quad \frac{|H^1(G, U_{K,T})|}{|H^1(G, J_{K,T})|} = \frac{[K : k] \cdot |\hat{H}^0(G, U_{K,T})|}{ef_T}. \]

Next we compute \(|H^1(G, C_{K,T})|\). Taking cohomology of the short exact sequence
\[ (5.3) \quad 0 \rightarrow (C_{K,T})^G \rightarrow (C_K)^G \rightarrow (Cl_{K,T})^G \rightarrow H^1(G, C_{K,T}) \rightarrow H^1(G, C_K) \rightarrow \cdots. \]

By class field theory again, we know that \(H^1(G, C_K) = 0\), hence the above exact sequence shows that
\[ (5.8) \quad |H^1(G, C_{K,T})| = \frac{|(Cl_{K,T})^G|}{|i_{k \rightarrow K}(C_k)/(C_{K,T})^G|}. \]

Therefore, combining (5.5), (5.7), (5.8) with Lemma 5.4, we obtain the formula
\[ |\text{Ker}(\alpha_2)| = \frac{|[K : k] \cdot |\hat{H}^0(G, U_{K,T})|}{ef_T} \cdot \frac{|(Cl_{K,T})^G|}{|i_{k \rightarrow K}(C_k)/(C_{K,T})^G| \cdot |(C_{K,T})^G/(i_{k \rightarrow K}(C_{K,T}))|}. \]

Here we note that the denominator of the second factor in the right hand side is
\[ |i_{k \rightarrow K}(C_k)/(i_{k \rightarrow K}(C_{K,T}))| = |C_k/C_{K,T}|, \]

which is equal to \(|Cl_{k,T}|\) by Lemma 5.2. This completes the proof. \(\square\)

**Corollary 5.5.** If \([K : k] = p\) is a prime and \(T \subset R\), then
\[ \text{ord}_p \left( \frac{|(Cl_{K,T})^G|}{|Cl_{k,T}|} \right) \leq |R| - 1. \]

**Proof.** By the definition of \(\alpha_2\) we have \(|\ker(\alpha_2)| \leq |\hat{H}^0(G, U_{K,T})|\). Then Theorem 5.1 implies that
\[ (5.9) \quad \left| \frac{|(Cl_{K,T})^G|}{|Cl_{k,T}|} \right| \leq \frac{ef_T}{[K : k]}. \]

By assumption we have \(f_T = 1\), hence taking \(\text{ord}_p\) of both sides of (5.9) yields the required inequality. \(\square\)

**References**

[1] Artin, E. and Tate, J.; *Class Field Theory*, Benjamin (1967).


[27] Serre, J. P. and Tate, J.; Good reduction of abelian varieties, Ann. of Math., 68 (1968), 492–517.


[31] Top, J.; Descend by 3-isogeny and 3-rank of quadratic fields, Advances in Number Theory, Oxford


Department of Mathematics
Rikkyo University
Nishi-Ikebukuro
Tokyo 117, Japan