ON l -CLASS GROUPS OF CERTAIN NUMBER FIELDS

FRANK GERTH III

1. *Introduction.* Let M be a finite extension field of the rational numbers $\mathbb{Q}$, and let C_M denote the ideal class group of M . Let l be a rational prime, and let A_M denote the l -class group of M (i.e., the Sylow l -subgroup of C_M). If G is any finite abelian l -group, we define

$$\text{rank } G = \dim_{\mathbb{F}_l}(G \otimes_{\mathbb{Z}_l} \mathbb{F}_l),$$

where $\mathbb{Z}_l$ is the ring of l -adic integers and $\mathbb{F}_l$ is the finite field of l elements. One of the classical results of algebraic number theory is the specification of $\text{rank } A_M$ when M is a quadratic extension of $\mathbb{Q}$ and $l = 2$. This result was obtained by means of Gauss's theory of genera. A generalization of this result can be found in [1], where A. Fröhlich has obtained upper and lower bounds for $\text{rank } A_M$ when M is a cyclic extension of $\mathbb{Q}$ of degree l . His methods also show how to compute $\text{rank } A_M$ exactly when $l = 3$. In [4], G. Gras has described a procedure for analyzing the l -class groups of relatively cyclic extensions of degree l . However when $l > 3$, the computations can be very difficult.

In previous papers (see [2] and [3]) we have obtained algorithms for finding $\text{rank } A_M$ when M is a non-Galois cubic extension of $\mathbb{Q}$ and $l = 3$. In this paper we analyze the following more general situation. We let l be an odd prime, J an algebraic number field with $A_J = \{1\}$, and L a nonabelian Galois extension of J satisfying the following conditions.

- (i) $[L : J] = nl$ with $1 < n \leq l - 1$ and $n|(l - 1)$.
- (ii) $\text{Gal}(L/J)$ is generated by $\{\sigma, \tau\}$ with relations $\sigma^l = 1, \tau^n = 1, \tau\sigma = \sigma^r\tau$, where $1 < r \leq l - 1, r^n \equiv 1 \pmod{l}$, and $r^i \not\equiv 1 \pmod{l}$ for $1 \leq i < n$.

We let $\langle \tau \rangle$ (resp. $\langle \sigma \rangle$) denote the subgroup of $\text{Gal}(L/J)$ generated by τ (resp. σ), and we let K (resp. F) be the fixed field of $\langle \tau \rangle$ (resp. $\langle \sigma \rangle$). From condition (ii) we see that $\langle \sigma \rangle$ is a normal subgroup of $\text{Gal}(L/J)$, and hence F is Galois over J (in fact, $\text{Gal}(F/J)$ is cyclic of order n generated by $\tau|_F$). Also K is a non-Galois extension of J with $[K : J] = l$. An important example of this situation is $J = \mathbb{Q}$, $F = \mathbb{Q}(\zeta)$, $K = \mathbb{Q}(x^{1/l})$, and $L = K \cdot F$, where ζ is a primitive l -th root of unity, and x belongs to $\mathbb{Q}$ but is not an l -th power in $\mathbb{Q}$.

Our primary goal in this paper is to obtain information about A_K . We shall provide upper and lower bounds for $\text{rank } A_K$ as well as additional information about the structure of A_K . Furthermore we shall obtain information about the structure of A_M for each field M such that $K \subseteq M \subseteq L$. We remark that some of the results in [5] are special cases of our results, and several of our results are generalizations of results in [8].

We conclude this section with a remark on notations. In general we use multiplicative notation for groups and modules, and the action of a group or ring on a module is expressed by exponentiation. Furthermore we adopt the convention $(x^\sigma)^\tau = x^{\sigma\tau}$.

2. *Action of Galois group on l -class groups.* We let notations be the same as in §1.

We shall analyze the action of $\text{Gal}(L/J)$ on A_L . We first note that $\mathbb{Z}_l$ contains the n -th roots of unity since $n|(l-1)$. For $j = 0, 1, \dots, n-1$, we define ψ_j to be the l -adic character of $\langle \tau \rangle$ (i.e., of $\text{Gal}(L/K)$) such that

$$\psi_j(\tau) = \mu^j, \quad (2.1)$$

where μ is the n -th root of unity in $\mathbb{Z}_l$ such that $\mu \equiv r \pmod{l}$. We define

$$\varepsilon_j = \frac{1}{n} \sum_{i=0}^{n-1} \psi_j(\tau^{-i}) \tau^i, \quad 0 \leq j \leq n-1. \quad (2.2)$$

Then $\{\varepsilon_j\}_{j=0}^{n-1}$ is a set of mutually orthogonal idempotents of $\mathbb{Z}_l[\langle \tau \rangle]$. We let $A_L^{(j)} = A_L \varepsilon_j = \{a^{\varepsilon_j} | a \in A_L\}$. Then $A_L \cong \prod_{j=0}^{n-1} A_L^{(j)}$. Similarly if we restrict τ to F and let $A_F^{(j)} = A_F \varepsilon_j$, then $A_F \cong \prod_{j=0}^{n-1} A_F^{(j)}$. For each positive rational integer m which divides n , we let K_m be the fixed field of $\langle \tau^m \rangle$. Then $K \subseteq K_m \subseteq L$; in particular, $K_1 = K$ and $K_n = L$.

PROPOSITION 2.1.

$$A_{K_m} \cong \prod_{s=0}^{m-1} A_L^{(ns/m)}.$$

Proof. Since $[L : K_m]$ is relatively prime to l , it is easy to see that

$$A_{K_m} = \{a \in A_L | a^{\tau^m} = a\}.$$

For $a \in A_L$ and $0 \leq j \leq n-1$, a straightforward calculation shows that

$$a \in A_L^{(j)} \Leftrightarrow a^\tau = a^{\mu^j}. \text{ So if } a \in A_L^{(j)}, \text{ then } a^{\tau^m} = a^{\mu^{mj}}. \text{ Hence for } a \in A_L^{(j)},$$

$$a^{\tau^m} = a \Leftrightarrow \mu^{mj} = 1 \Leftrightarrow n|mj \Leftrightarrow j = \frac{ns}{m}$$

for $s = 0, 1, \dots, m-1$. It then follows that $A_{K_m} \cong \prod_{s=0}^{m-1} A_L^{(ns/m)}$.

Remark. By restricting τ to F , we get $A_{J_m} \cong \prod_{s=0}^{m-1} A_F^{(ns/m)}$, where J_m is the fixed field of $\langle \tau^m | F \rangle$. We also note that $A_L^{(j)} = \{a \in A_L | a^\tau = a^{\mu^j}\}$ and

$$A_F^{(j)} = \{a \in A_F | a^\tau = a^{\mu^j}\}.$$

Next we note that

$$\begin{aligned} \tau(1 + \sigma + \dots + \sigma^{l-1}) &= \tau + \tau\sigma + \dots + \tau\sigma^{l-1} = \tau + \sigma^r \tau + \dots + \sigma^{(l-1)r} \tau \\ &= (1 + \sigma^r + \dots + \sigma^{(l-1)r})\tau. \end{aligned}$$

Since r is relatively prime to l , then $\{0, r, 2r, \dots, (l-1)r\}$ is a complete residue system modulo l . Hence we conclude that $1 + \sigma^r + \dots + \sigma^{(l-1)r}$ is the same as $1 + \sigma + \dots + \sigma^{l-1}$ since $\sigma^l = 1$. So $\tau(1 + \sigma + \dots + \sigma^{l-1}) = (1 + \sigma + \dots + \sigma^{l-1})\tau$. Then $\tau^m(1 + \sigma + \dots + \sigma^{l-1}) = (1 + \sigma + \dots + \sigma^{l-1})\tau^m$ for each positive integer m . We let $N_\sigma : A_L \rightarrow A_F$ be the map induced by the norm map from ideals of L to ideals of F . If $a \in A_L^{(j)}$, where $0 \leq j \leq n-1$, then $N_\sigma a \in A_F^{(j)}$; i.e.,

$$\begin{aligned} (N_\sigma a)^\tau &= a^{(1+\sigma+\dots+\sigma^{l-1})\tau} = (a^\tau)^{1+\sigma+\dots+\sigma^{l-1}} = (a^{\mu^j})^{1+\sigma+\dots+\sigma^{l-1}} \\ &= (a^{1+\sigma+\dots+\sigma^{l-1}})^{\mu^j} = (N_\sigma a)^{\mu^j}, \end{aligned}$$

which implies $N_\sigma a \in A_F^{(j)}$. So for each j , $N_\sigma A_L^{(j)} \subseteq A_F^{(j)}$. Moreover, if L is ramified over F , then by class field theory $N_\sigma A_L = A_F$ and hence $N_\sigma A_L^{(j)} = A_F^{(j)}$. If L is unramified over F , then $N_\sigma A_L$ is a subgroup of A_F of index l . Hence when L/F is unramified, $N_\sigma A_L^{(j)} = A_F^{(j)}$ for all but one value of j , and for that value of j , $N_\sigma A_L^{(j)}$ is a subgroup of $A_F^{(j)}$ of index l .

We let $B = \ker(N_\sigma : A_L \rightarrow A_F)$. It is easy to see that B is a $\mathbb{Z}_l[\text{Gal}(L/J)]$ module since τ computes with $1 + \sigma + \dots + \sigma^{l-1}$. In particular B is a $\mathbb{Z}_l[\langle \tau \rangle]$ module, and we can define $B^{(j)} = B^{\epsilon_j}$ for $0 \leq j \leq n-1$. Then

$$B^{(j)} = \ker(N_\sigma|_{A_L^{(j)}} : A_L^{(j)} \rightarrow A_F^{(j)}).$$

We summarize our results as follows.

PROPOSITION 2.2. *If L/F is ramified, there are exact sequences*

$$1 \rightarrow B^{(j)} \rightarrow A_L^{(j)} \rightarrow A_F^{(j)} \rightarrow 1, \quad 0 \leq j \leq n-1.$$

If L/F is unramified, the same exact sequences exist for all but one value of j . For that value of j , there is an exact sequence

$$1 \rightarrow B^{(j)} \rightarrow A_L^{(j)} \rightarrow \Lambda^{(j)} \rightarrow 1$$

where $\Lambda^{(j)}$ is a subgroup of $A_F^{(j)}$ of index l .

COROLLARY 2.3. $A_K \cong B^{(0)}$.

Proof. Since $K = K_1$, Proposition 2.1 implies $A_K \cong A_L^{(0)}$. Also $A_F^{(0)} \cong A_J$, which is trivial by assumption. So the exact sequence of Proposition 2.2 with $j = 0$ implies that $A_K \cong A_L^{(0)} \cong B^{(0)}$.

We now focus our attention on $B = \ker(N_\sigma : A_L \rightarrow A_F)$. We shall analyze B as a module over $\mathbb{Z}_l[\langle \sigma \rangle]$ and as a module over $\mathbb{Z}_l[\langle \tau \rangle]$. Our methods involve module theory rather than number theory. Since $B^{1+\sigma+\dots+\sigma^{l-1}} = N_\sigma B = \{1\}$, then B is a $\mathbb{Z}_l[\langle \sigma \rangle]/(1 + \sigma + \dots + \sigma^{l-1})$ module. If ζ denotes a primitive l -th root of unity, then

$$\mathbb{Z}_l[\langle \sigma \rangle]/(1 + \sigma + \dots + \sigma^{l-1}) \cong \mathbb{Z}_l[\zeta]$$

by means of $\sigma \mapsto \zeta$. We note that $\mathbb{Z}_l[\zeta]$ is a principal ideal domain, and B is a finitely generated torsion module over $\mathbb{Z}_l[\zeta]$. The following proposition is now easy to prove.

PROPOSITION 2.4. *Let R denote $\mathbb{Z}_l[\zeta]$. Then*

$$B \cong R/(1 - \zeta)^{i_1} R \oplus \dots \oplus R/(1 - \zeta)^{i_w} R$$

(in additive notation) for some positive integers $i_1 \leq i_2 \leq \dots \leq i_w$, where $w = \text{rank } B_1$ and $B_1 = \{a \in B | a^\sigma = a\}$.

To further investigate B , we let $B_i = \{a \in B | a^{(1-\sigma)^i} = 1\}$ for $i = 0, 1, 2, \dots$. Then $\{1\} = B_0 \subseteq B_1 \subseteq B_2 \subseteq \dots \subseteq B_{i_w} = B$. (We note that this definition of B_1 agrees with the definition of B_1 in Proposition 2.4.) Also B_{i+1}/B_i is an elementary abelian l -group since

$$B_{i+1} \supseteq B_i \supseteq B_{i+1}^{1-\sigma} \supseteq B_{i+1}^{(1-\sigma)^{l-1}} = B_{i+1}^l$$

(the last step follows from $(1 - \zeta)^{l-1} R = (l)R$). Next we claim that each B_i is a

$\mathbb{Z}_l[\langle \tau \rangle]$ module. Indeed, if $a^{(1-\sigma)^l} = 1$, then

$$(a^\tau)^{(1-\sigma)^l} = a^{(1-\sigma^r)^l \tau} = a^{(1-\sigma)^l(1+\sigma+\dots+\sigma^{r-1})^l \tau} = 1.$$

So $a^\tau \in B_i$, and B_i is a $\mathbb{Z}_l[\langle \tau \rangle]$ module. Then B_{i+j}/B_i is a $\mathbb{Z}_l[\langle \tau \rangle]$ module for each integer $i \geq 0$ and $j \geq 0$. Hence $B_i \cong \prod_{s=0}^{n-1} B_i^{(s)}$ and

$$B_{i+j}/B_i \cong \prod_{s=0}^{n-1} (B_{i+j}/B_i)^{(s)} \cong \prod_{s=0}^{n-1} (B_{i+j}^{(s)} \cdot B_i)/B_i,$$

where $B_i^{(s)} = B_i^{\varepsilon_s}$, $(B_{i+j}/B_i)^{(s)} = (B_{i+j}/B_i)^{\varepsilon_s}$, and $\{\varepsilon_s\}_{s=0}^{n-1}$ is the set of mutually orthogonal idempotents defined by equation (2.2). Next we note that $B_{l-1} = \{a \in B | a^l = 1\}$ since $(1-\zeta)^{l-1} R = (l)R$. So $\text{rank } B = \text{rank } B_{l-1}$, and

$$\text{rank } B^{(s)} = \text{rank } B_{l-1}^{(s)} \quad (2.3)$$

for each s , where $B^{(s)} = B^{\varepsilon_s}$. Also

$$\text{rank } B_{l-1}^{(s)} = \sum_{i=1}^{l-1} \text{rank } (B_i/B_{i-1})^{(s)} \quad (2.4)$$

since $B_{l-1}^{(s)}$ and each $(B_i/B_{i-1})^{(s)}$ are elementary abelian l -groups and $B_0 = \{1\}$.

LEMMA 2.5. *Let i be an integer such that $1 < i \leq l-1$, and let q be an integer which satisfies $1 \leq q < i$. Let s be an integer such that $0 \leq s \leq n-1$. Then $(1-\sigma)^q$ maps $(B_i/B_{i-1})^{(s)}$ into $(B_{i-q}/B_{i-q-1})^{(v)}$, where $0 \leq v \leq n-1$ and $v \equiv s-q \pmod{n}$.*

Proof. Let $b \in (B_i/B_{i-1})^{(s)} = (B_i^{(s)} \cdot B_{i-1})/B_{i-1}$. Then there exists an element $a \in B_i^{(s)}$ such that b is the image of a in $(B_i^{(s)} \cdot B_{i-1})/B_{i-1}$. We note that $a^l = 1$ since $a \in B_i \subseteq B_{l-1} = \{a \in B | a^l = 1\}$, and hence $a^\tau = a^{\mu^s} = a^{r^s}$ (see the remark following Proposition 2.1, the definition of μ following equation 2.1, and condition (ii) in §1). Now clearly $a^{(1-\sigma)^q} \in B_{i-q}$. We shall show that

$$(a^{(1-\sigma)^q})^\tau \equiv (a^{(1-\sigma)^q})^{r^v} \pmod{B_{i-q-1}},$$

which will complete the proof since it implies that $(1-\sigma)^q$ maps $(B_i/B_{i-1})^{(s)}$ into $(B_{i-q}/B_{i-q-1})^{(v)}$. Now

$$\begin{aligned} (a^{(1-\sigma)^q})^\tau &= a^{\tau(1-\sigma)^q} = a^{r^s(1-\sigma^{\bar{r}})^q} \\ &= a^{(1-\sigma)^q(1+\sigma+\dots+\sigma^{\bar{r}-1})^q r^s} \end{aligned}$$

where $\bar{r}$ satisfies $1 < \bar{r} \leq l-1$ and $\bar{r}r \equiv 1 \pmod{l}$. Note that

$$1 + \sigma + \dots + \sigma^{\bar{r}-1} \equiv \bar{r} \pmod{(1-\sigma)}.$$

So

$$\begin{aligned} a^{(1-\sigma)^q(1+\sigma+\dots+\sigma^{\bar{r}-1})^q r^s} &\equiv a^{(1-\sigma)^q \bar{r}^q r^s} \\ &\equiv (a^{(1-\sigma)^q})^{r^v} \pmod{B_{i-q-1}^{1-\sigma}}. \end{aligned}$$

Hence $(a^{(1-\sigma)^q})^\tau \equiv (a^{(1-\sigma)^q})^{r^v} \pmod{B_{i-q-1}}$ since $B_{i-q-1}^{1-\sigma} \subseteq B_{i-q-1}$.

Remark. From the definition of each B_i , we see that $(1-\sigma)^q$ maps B_i/B_{i-1} injectively into B_{i-q}/B_{i-q-1} . Then Lemma 2.5 implies that $(1-\sigma)^q$ maps $(B_i/B_{i-1})^{(s)}$

injectively into $(B_{i-q}/B_{i-q-1})^{(v)}$. We remark that the map is surjective if there is no exponent i_j in Proposition 2.4 such that $i_j < i$.

COROLLARY 2.6. Rank $B^{(s)} \leq (l-1)w/n$ for $0 \leq s \leq n-1$, where w is given in Proposition 2.4.

Proof. Let s be fixed. For each $i = 1, 2, \dots, l-1$, the above remark implies that $(1-\sigma)^{i-1}$ maps $(B_i/B_{i-1})^{(s)}$ injectively into $(B_1/B_0)^{(v_i)} = B_1^{(v_i)}$, where $v_i \equiv s-i+1 \pmod{n}$. So rank $(B_i/B_{i-1})^{(s)} \leq \text{rank } B_1^{(v_i)}$. Then from equations 2.3 and 2.4

$$\begin{aligned} \text{rank } B^{(s)} &= \text{rank } B_{l-1}^{(s)} = \sum_{i=1}^{l-1} \text{rank } (B_i/B_{i-1})^{(s)} \\ &\leq \sum_{i=1}^{l-1} \text{rank } B_1^{(v_i)} = \frac{l-1}{n} \sum_{j=0}^{n-1} \text{rank } B_1^{(j)}, \end{aligned}$$

since v_i takes on each value from 0 to $n-1$ exactly $(l-1)/n$ times as i goes from 1 to $l-1$. Since $\sum_{j=0}^{n-1} \text{rank } B_1^{(j)} = \text{rank } B_1 = w$, the proof is complete.

Remark. If each exponent i_j in Proposition 2.4 is greater than or equal to $l-1$, then rank $B^{(s)} = (l-1)w/n$ for each s .

COROLLARY 2.7. Rank $A_K \leq (l-1)w/n$. More generally

$$\text{rank } A_{K_m} \leq \frac{m(l-1)w}{n} + \text{rank } A_{J_m},$$

where K_m (resp. J_m) is defined immediately before (resp. after) Proposition 2.1.

Proof. The first part follows immediately from Corollaries 2.3 and 2.6. The second part follows from Propositions 2.1 and 2.2 and from Corollary 2.6.

3. Calculation of w . We let notations be the same as in §§1 and 2. In this section we describe how to compute w . From Proposition 2.4, $w = \text{rank } B_1$, where $B_1 = \{a \in B | a^\sigma = a\}$. Let $D = \{a \in A_L | a^\sigma = a\}$. From [6, Theorem 13] or [4, Theorem IV.1]

$$|D| = \frac{|A_F|^{l-1}}{[E_F : E_F \cap N_{L/F} L^*]}, \quad (3.1)$$

where:

l is the number of ramified primes in L/F ;

E_F is the group of units of F ;

$N_{L/F}$ is the norm map from L to F ;

$L^* = L - \{0\}$.

Next we let D' be the subgroup of D generated by the image of A_F in A_L and by the ideal classes of $\mathfrak{P}_1^h, \dots, \mathfrak{P}_t^h$, where $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ are the prime ideals of L which are

ramified over F , and $h = |C_F/A_F|$, where C_F is the ideal class group of F . Then by [6, §13]

$$|D'| = \frac{|A_F|^{l^{t-1}}}{[E_F : N_{L/F} E_L]},$$

where E_L is the group of units of L . Furthermore

$$D/D' \cong (E_F \cap N_{L/F} L^*)/N_{L/F} E_L. \quad (3.2)$$

In fact the isomorphism is given as follows. Let $a \in D$, and let $\mathfrak{a}$ be an ideal of L such that $\text{cl}_L(\mathfrak{a}) = a$, where $\text{cl}_L(\mathfrak{a})$ denotes the ideal class of $\mathfrak{a}$ in the ideal class group of L . Then by definition of D , $\mathfrak{a}^{1-\sigma} = (x)$ for some $x \in L^*$. We note that $x \notin E_L$ if $a \notin D'$. We now apply $N_{L/F}$ to $\mathfrak{a}^{1-\sigma} = (x)$ to obtain $(1) = (N_{L/F} x)$. So $N_{L/F} x = e$ for some $e \in E_F$. The isomorphism (3.2) is then given by

$$a \bmod D' \mapsto e \bmod N_{L/F} E_L.$$

If $|D/D'| = l^v$, we let $\mathfrak{a}_1, \dots, \mathfrak{a}_v$ be ideals of L such that $\text{cl}_L(\mathfrak{a}_1), \dots, \text{cl}_L(\mathfrak{a}_v)$ generate D/D' .

We are interested in $B_1 = \{a \in B | a^\sigma = a\} = \{a \in A_L | N_\sigma a = 1 \text{ and } a^\sigma = a\} = \{a \in D | N_\sigma a = 1\}$, where $N_\sigma : A_L \rightarrow A_F$ is the map induced by the norm map from ideals of L to ideals of F . To study B_1 , we first define ${}_l A_F = \{a \in A_F | a^l = 1\}$. If $a \in A_F$, then $N_\sigma \text{im}_L(a) = a^l$, where im_L denotes the map from A_F to A_L induced by the inclusion map of ideals of F to ideals of L . So if $a \in A_F$, then

$$\text{im}_L(a) \in B_1 \Leftrightarrow N_\sigma \text{im}_L(a) = 1 \Leftrightarrow a^l = 1 \Leftrightarrow a \in {}_l A_F.$$

We define D'' to be the subgroup of D generated by

$$\text{cl}_L(\mathfrak{a}_1), \dots, \text{cl}_L(\mathfrak{a}_v), \text{cl}_L(\mathfrak{P}_1^h), \dots, \text{cl}_L(\mathfrak{P}_t^h).$$

Then $D = D'' \cdot (\text{im}_L A_F)$. Now the exact sequence

$$1 \rightarrow B_1 \rightarrow D \rightarrow N_\sigma D \rightarrow 1$$

shows that

$$|B_1| = |D|/|N_\sigma D|. \quad (3.3)$$

Since $N_\sigma \text{im}_L A_F = A_F^l$ and $D = D'' \cdot (\text{im}_L A_F)$, then $N_\sigma D = N_\sigma D'' \cdot A_F^l$ and $A_F^l \subseteq N_\sigma D \subseteq A_F$. Hence

$$|N_\sigma D| = |(N_\sigma D'' \cdot A_F^l)/A_F^l| \cdot |A_F^l|.$$

The exact sequence $1 \rightarrow {}_l A_F \rightarrow A_F \rightarrow A_F^l \rightarrow 1$ implies

$$|N_\sigma D| = |(N_\sigma D'' \cdot A_F^l)/A_F^l| \cdot |A_F|/|{}_l A_F|. \quad (3.4)$$

Then using equations 3.1 and 3.4 in equation 3.3, we get

$$|B_1| = \frac{|{}_l A_F| \cdot l^{t-1}}{[E_F : E_F \cap N_{L/F} L^*] \cdot |(N_\sigma D'' \cdot A_F^l)/A_F^l|}. \quad (3.5)$$

We note that ${}_l A_F$, $E_F/(E_F \cap N_{L/F} L^*)$, and $(N_\sigma D'' \cdot A_F^l)/A_F^l$ are elementary abelian l -groups, and we define:

$$\gamma = \text{rank } {}_l A_F = \text{rank } A_F; \quad (3.6)$$

$$\delta = \text{rank } E_F/(E_F \cap N_{L/F} L^*); \quad (3.7)$$

$$z = \text{rank } (N_\sigma D'' \cdot A_F^l)/A_F^l. \quad (3.8)$$

Since B_1 is an elementary abelian l -group and $w = \text{rank } B_1$, then equations 3.5 through 3.8 give the following result.

PROPOSITION 3.1. $w = t + \gamma - 1 - \delta - z$, where t is the number of ramified primes in L/F , and γ, δ, z are defined by equations 3.6 through 3.8.

Remark. Clearly $0 \leq \delta \leq \beta$, where $\beta = \text{rank } E_F/E_F^l$. Also equations 3.6 through 3.8, the definitions of v and D'' , and the isomorphism (3.2) show that $0 \leq z \leq \min(\gamma, t + v) \leq \min(\gamma, t + \beta - \delta)$.

The next two corollaries follow immediately from our previous results.

COROLLARY 3.2.

$$\text{Rank } A_K \leq \frac{(l-1)w}{n} = \frac{(l-1)(t + \gamma - 1 - \delta - z)}{n}.$$

COROLLARY 3.3. If $\text{rank } A_F = 0$, then $w = t - 1 - \delta$ and

$$\text{rank } A_K \leq \frac{(l-1)(t-1-\delta)}{n}.$$

We can obtain a lower bound for $\text{rank } A_K$ as follows. Let d denote the number of totally ramified primes in K/J . Then $d \leq t$. Let $P = \{\text{principal fractional ideals } a \text{ of } L \text{ such that } a^\sigma = a\}$. Let P_F be the subgroup of P generated by principal fractional ideals of F . It is known that $P/P_F \cong H^1(\langle \sigma \rangle, E_L)$, where $H^1(\langle \sigma \rangle, E_L)$ denotes the 1-dimensional cohomology of $\langle \sigma \rangle$ with coefficients in E_L (see [7]). Furthermore, since $\langle \sigma \rangle$ is a cyclic group of order l , $H^1(\langle \sigma \rangle, E_L)$ is an elementary abelian l -group. Now let $q_1, \dots, q_d$ be the prime ideals of K which are totally ramified over J , and let S be the subgroup of D generated by $\text{cl}_L(q_1^c), \dots, \text{cl}_L(q_d^c)$, where $D = \{a \in A_L | a^\sigma = a\}$ and $c = |C_J/A_J| = |C_J|$. (Recall $|A_J| = 1$ by assumption.) We note that $(q_i^c)^{t+\sigma+\dots+\sigma^{l-1}} = (q_i^c)^l$ for each i , and $N_\sigma S \subseteq C_J^c = \{1\}$. Hence $S^l = \{1\}$. So $\text{rank } A_K \geq \text{rank } S \geq d - \text{rank } (P/P_F) = d - \text{rank } H^1(\langle \sigma \rangle, E_L)$. It is known that

$$\frac{|H^2(\langle \sigma \rangle, E_L)|}{|H^1(\langle \sigma \rangle, E_L)|} = \frac{1}{l}$$

(cf. [9, p. 192]), and furthermore $H^2(\langle \sigma \rangle, E_L) = E_F/N_{L/F} E_L$, which is an elementary abelian l -group since $\langle \sigma \rangle$ is cyclic of order l . Then

$$\text{rank } H^1(\langle \sigma \rangle, E_L) = 1 + \text{rank } H^2(\langle \sigma \rangle, E_L),$$

and hence

$$\text{rank } A_K \geq d - 1 - \text{rank } H^2(\langle \sigma \rangle, E_L) \geq d - 1 - \beta,$$

where $\beta = \text{rank } E_F/E_F^l$. (More precisely, we have proved that $\text{rank } B_1^{(0)} \geq d - 1 - \beta$, where $B_1^{(0)} = \{a \in A_L | N_\sigma a = 1, a^\sigma = a, a^\tau = a\}$.) We summarize these results in the following proposition.

PROPOSITION 3.4. $\text{Rank } A_K \geq d - 1 - \beta$, where d is the number of totally ramified primes in K/J , and $\beta = \text{rank } E_F/E_F^l$.

COROLLARY 3.5. Suppose $\text{rank } A_F = 0$ and $[F : J] = l - 1$. For each prime q of J which ramifies totally in K , we suppose that there is exactly one prime of F which divides q . Then

$$d - 1 - \beta \leq \text{rank } A_K \leq d - 1 - \delta \leq d - 1.$$

Proof. The first inequality follows from Proposition 3.4. To get the second inequality, we use Corollary 3.3 with $n = l - 1$ and $t = d$. The third inequality is obvious.

Remark. Corollary 3.5 has also been obtained by Kobayashi (see [8]).

We restrict now to the case $J = \mathbb{Q}$. If $l = 3$, then K is a non-Galois cubic extension of J ; L is the normal closure of K ; and F is the quadratic subfield of L . In this situation it is not difficult to compute $\text{rank } A_K$ exactly. Indeed by Corollary 2.3 and equations 2.3 and 2.4, only $\text{rank } B_1^{(0)}$ and $\text{rank } (B_2/B_1)^{(0)}$ are needed. For explicit calculations of these ranks, see [3]. When $l > 3$, it is usually very difficult to compute $\text{rank } A_K$ exactly.

References

1. A. Fröhlich. "The generalization of a theorem of L. Redei's," *Quart. J. Math. Oxford*, (2), 5 (1954), 130-140.
2. F. Gerth. "On 3-class groups of pure cubic fields," *J. Reine Angew. Math.*, 278/279 (1975), 52-62.
3. F. Gerth. "Ranks of 3-class groups of non-Galois cubic fields," to appear in *Acta Arithmetica*.
4. G. Gras. *Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier l* , Thesis (Grenoble, 1972).
5. G. Gras. "Sur les l -classes d'idéaux des extensions non galoisiennes de $\mathbb{Q}$ de degré premier impair l a clôture galoisiennes diédrale de degré $2l$," *J. Math. Soc. Japan*, 26(1974), 677-685.
6. H. Hasse. "Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Ia," *Jber. Deutsch. Math.-Verein.*, 36 (1927), 233-311.
7. K. Iwasawa. "A note on the group of units of an algebraic number field," *J. Math. Pures Appl.*, ser. 9, 35 (1956), 189-192.
8. S. Kobayashi. "On the l -class rank in some algebraic number fields," *J. Math. Soc. Japan*, 26 (1974), 668-676.
9. S. Lang. *Algebraic number theory* (Addison-Wesley, Reading, Mass., 1970).

Department of Mathematics,
University of Texas,
Austin, Texas 78712,
U.S.A.

12B25: ALGEBRAIC NUMBER THEORY;
Algebraic number theory, local fields:
Class field theory.

Received on the 25th of November, 1975.