Steinitz classes of nonabelian extensions of degree $p^3$

by

JAMES E. CARTER (Charleston, S.C.)

0. Introduction. Let $L/k$ be a finite extension of algebraic number fields. Let $O_L$ and $o$ denote the rings of integers in $L$ and $k$, respectively. As an $o$-module, $O_L$ is completely determined by $[L:k]$ and its Steinitz class $C(L,k)$ in the class group $C(k)$ of $k$ (see [3], Theorem 13). Now let $G$ be a finite group. As $L$ varies over all normal extensions of $k$ with $\text{Gal}(L/k) \simeq G$, $C(L,k)$ varies over a subset $R(k,G)$ of $C(k)$. If we consider only tamely ramified such extensions, then this set is denoted by $R_t(k,G)$. An interesting problem is to determine $R(k,G)$ or $R_t(k,G)$ for various $k$ and $G$. In [7] McCulloh shows that if $G$ is a cyclic group of order $n$, and $k$ contains the multiplicative group $\mu_n$ of $n$th roots of unity, then $R(k,G) = R_t(k,G) = C(k)^d$ (the subgroup of $C(k)$ consisting of $d$th powers of elements of $C(k)$ where $d$ is a positive rational integer which depends on $n$).

From now on, unless otherwise stated, $p$ will denote an odd prime. In [5] it is shown that when $k$ is any algebraic number field and $G$ is cyclic of order $p$, then $R_t(k,G)$ is again a subgroup of $C(k)$. This result is extended in [6] to include cyclic groups of order $p^r$, where $r \geq 1$. In [1] we assume $k$ contains $\mu_p$ and $G$ is the nonabelian group of order $p^3$ with exponent $p$. There is an exact sequence of groups

$$\Sigma : 1 \to A \to G \to B \to 1$$

where $B$ is cyclic of order $p$. We fix, once and for all, a tamely ramified normal extension $E/k$ with $\text{Gal}(E/k) \simeq B$. As $L$ varies over all tamely ramified normal extensions of $k$ of a particular type which contain $E$, and such that $\text{Gal}(L/k) \simeq G$, $C(L,k)$ varies over a subset $R_t(E/k,\Sigma)$ of $C(k)$. It is shown that when the ring of integers in $E$ is free as an $o$-module, then $R_t(E/k,\Sigma)$ is a subgroup of $C(k)$. In the present paper, we continue to assume $k$ contains the appropriate roots of unity, and we return to our consideration of the set $R_t(k,G)$. Making essential use of results of [1] and [2], we will show that $R_t(k,G)$ is always a subgroup of $C(k)$ when $G$ is either of the two nonabelian groups of order $p^3$. More specifically, we prove
the following theorem:

**Theorem 0.1.** Let $k$ be an algebraic number field and let $G$ be a non-abelian group of order $p^3 = mn$ where $n$ is the exponent of $G$. If $\mu_n \subseteq k$ then

$$R_t(k, G) = C(k)^{m(p-1)/2}.$$ 

For the remainder of the paper, the notation will be as introduced above and in [1] and [2].

1. **First inclusion.** In this section we prove the following proposition:

**Proposition 1.1.** Let $k$ be any algebraic number field and let $G$ be a nonabelian group of order $p^3 = mn$ where $n$ is the exponent of $G$. Then

$$R_t(k, G) \subseteq C(k)^{m(p-1)/2}.$$ 

**Proof.** Let $L/k$ be a tamely ramified normal extension with $\text{Gal}(L/k) \cong G$. Suppose $p$ is a prime ideal in $k$ which ramifies in $L/k$, say

$$p = \left( \prod_{i=1}^g \mathfrak{P}_i \right)^e$$

where the ramification index $e = e(\mathfrak{P}_i, p) > 1$. Let $f = f(\mathfrak{P}_i, p)$ be the residue class degree and let $\mathfrak{D}$ be the different of $L/k$. Since $p$ is tamely ramified in $L/k$, $v_{\mathfrak{P}_i}(\mathfrak{D}) = e - 1$ for each $i$. Therefore

$$p^f \| N_{L/k}(\mathfrak{D}) = d_{L/k}.$$ 

Now suppose $\mathfrak{P}$ is any of the prime ideals in $L$ which divides $p$. Since the tame ramification group of $\mathfrak{P}$ over $p$ is cyclic of order $e$ it follows that $G$ contains an element of order $e$. Therefore $e | n$. Since $mn = p^3 = ef g$ we have $m | fg$. Therefore

$$C(L, k) = \text{cl}(d_{L/k}^{1/2}) \in C(k)^{m(p-1)/2}.$$ 

2. **Second inclusion.** Let $k$ and $G$ be as described in the statement of Theorem 0.1. By Proposition 1.1,

$$R_t(k, G) \subseteq C(k)^{m(p-1)/2}.$$ 

We will now establish the reverse inclusion thereby proving the theorem.

**Proposition 2.1.** Let $k$ and $G$ be as described in the statement of Theorem 0.1. Then

$$R_t(k, G) \supseteq C(k)^{m(p-1)/2}.$$ 

**Proof.** There are two cases to consider.

**Case 1.** Suppose $n = p$. Let $c$ be any class in $C(k)$. We construct a tamely ramified normal extension $L/k$ such that $\text{Gal}(L/k) \cong G$ and
Therefore, as in the proof of Lemma 4 of [1], we have

\[ C(L, k) = \varepsilon^{m(p-1)/2}, \]

by Theorem 2 of [7] there exists a tamely ramified normal extension \( E/k \) of degree \( p \) such that \( C(E, k) = \varepsilon^{(p-1)/2} \). In Proposition 5 of [1] let \( X \in W_{E/k} \) be the trivial class. That proposition gives a tamely ramified normal extension \( L/k \) containing \( E \) such that \( \text{Gal}(L/k) \simeq G \) and \( C(L, k) = (\varepsilon X)^{m(p-1)/2} = \varepsilon^{m(p-1)/2} \). Therefore

\[ R_t(k, G) \supseteq C(k)^{m(p-1)/2}. \]

**Case 2.** Suppose \( n = p^2 \). In the introduction of [2], the structure of \( G \) is described in terms of generators and relations and the parameters \( s \) and \( l \). According to that description we may assume \( s = 1 \) and \( l = 1 \). Let \( c \) be any class in \( C(k) \). In the following four steps we construct a normal extension \( L/k \) as described in Theorem 6 of [2] such that \( \text{Gal}(L/k) \simeq G \). We then show in the remaining two steps that \( L/k \) is tamely ramified and \( C(L, k) = \varepsilon^{m(p-1)/2} \).

**Step 1.** In this step we construct a tamely ramified cyclic extension \( E/k \) of degree \( p \) such that \( C(E, k) = \varepsilon^{(p-1)/2} \).

Let \( m = (1 - \zeta)p^2 \). Choose an odd integer \( s \geq 3 \) such that \( \varepsilon^s = c \). Let \( l \) be a prime ideal in \( c \) such that \( l \) is not a factor of \( (p) \). Let \( C_k(m) \) be the ray class group modulo \( m \) of \( k \), and let \( c_m \) be the element of \( C_k(m) \) which contains \( l \). Choose distinct prime ideals \( l_1, \ldots, l_s \) in \( C_K(m) \). Choose positive integers \( u_i \), \( 1 \leq i \leq s \), such that \( (u_i, p) = 1 \) for each \( i \) and \( \sum_{i=1}^{s} u_i = p^2s \) (e.g. \( u_i = p^2 - 1 \) for \( 1 \leq i \leq (s + 1)/2 \), \( u_i = p^2 + 1 \) for \( (s + 3)/2 \leq i \leq s - 1 \), and \( u_s = p^2 + 2 \)).

Let \( l_{s+1} \) be a prime ideal in \( c^{-1} \). Then

\[
(a) = \left( \prod_{i=1}^{s} l_i^{u_i} \right) p^2s \]

where \( a \in \mathfrak{o} \) and \( a \equiv 1 \pmod{m} \). Let \( E = k(\alpha) \) where \( \alpha^p = a \). Let \( \zeta \) be a primitive \( p \)-th root of unity. By Kummer theory \( E/k \) is cyclic of degree \( p \) with, say, \( \text{Gal}(E/k) \simeq \langle \varrho \rangle \) where \( \varrho(\alpha) = \zeta \alpha \). Furthermore, by the proof of Theorem 118 of [4], and by Theorem 119 of [4], the only ramified prime ideals in \( E/k \) are the ideals \( l_1, \ldots, l_s \). Hence, \( E/k \) is tamely ramified (in fact, by Theorem 119 of [4], the prime divisors of \( (p) \) split completely in \( E/k \)). It follows that

\[ d_{E/k} = \left( \prod_{i=1}^{s} l_i \right)^{p-1}. \]

Therefore, as in the proof of Lemma 4 of [1], we have

\[ C(E, k) = \text{cl}(d_{E/k}^{1/2}) = \text{cl} \left( \prod_{i=1}^{s} l_i \right)^{p-1}/2 = \varepsilon^{s(p-1)/2} = \varepsilon^{(p-1)/2}. \]

**Step 2.** In this step we construct the element \( \kappa \). Let \( \mathfrak{q} \) be a prime ideal in \( c^{-1} \) such that \( \mathfrak{q} \) is not a factor of \( (p) \). Note that \((\varepsilon^{-1})^s = (\varepsilon^s)^{-1} = c^{-1}\).
where \( s \) is the integer of Step 1. Let \( c'_m \) be the class in \( C_k(m) \) which contains \( q \) and choose distinct prime ideals \( q_1, \ldots, q_s \) in \( c'_m \) such that \((q_i, l_j) = 1\) for \( 1 \leq i \leq s \) and \( 1 \leq j \leq s + 1 \) where the \( l_j \) are the prime ideals of Step 1. Choose positive integers \( v_i \) for \( 1 \leq i \leq s \) such that \((v_i, p) = 1\) and \( \sum_{i=1}^{s} v_i = ps \). Let \( q_{s+1} \) be a prime ideal in \((c'_m)^{-1}\) such that \((q_{s+1}, l_j) = 1\) for \( 1 \leq j \leq s + 1 \). We have

\[
(\kappa) = \left( \prod_{i=1}^{s} q_i^{v_i} \right) q_{s+1}^{ps}
\]

where \( \kappa \in \mathfrak{o} \) and \( \kappa \equiv 1 \pmod{m} \). Since \(((\kappa), d_{E/k}) = 1\) each \( q_i \) remains prime or splits completely in \( E/k \).

**Step 3.** In this step we construct the element \( e \). In the proof of Proposition 5 of [1], let \( X \in W_{E/k} \) be the trivial class, \( b = (\alpha \kappa) \), and \( m = (1 - \zeta)^p^2 \). Construct \( e \) as outlined in that proof. Then

\[
(e) = \left( \prod_{i=1}^{t} \mathfrak{P}_i^{b_i} \right) \Omega^{pt}
\]

as described there.

**Step 4.** It is straightforward to verify that with the elements constructed in the above three steps, the conditions of Theorem 6 of [2] are satisfied (see, for instance, the paragraph preceding Example 1 of [2]). Consequently, we obtain a normal extension \( L/k \) as described in that theorem with \( \text{Gal}(L/k) \cong G \).

**Step 5.** In this step we show that no prime divisor of \((p)\) ramifies in the extension \( L/k \). Hence, \( L/k \) is tamely ramified. In fact, we will show that we can arrange for all prime divisors of \((p)\) to split completely in \( L/k \).

Assume

\[
(1 - \zeta) = \prod_{i=1}^{g} p_i^{w_i}
\]

where the \( p_i \) are distinct prime ideals in \( k \) and the \( w_i \) are positive integers. Let \( p = p_1 \) and \( w = w_1 \). Thus

\[
v_p(1 - \zeta) = w.
\]

Recall from Step 1 that the prime divisors of \((p)\) split completely in \( E/k \). Hence \( p \mathfrak{O}_E = \mathfrak{P}^N \) where \( \mathfrak{P} \) is a prime ideal in \( E \). Since \( a \equiv 1 \pmod{m} \), (2.5) implies that \( a \equiv 1 \pmod{p^{w p^2}} \). Hence

\[
p^{w p^2} | (a - 1) = (\alpha^p - 1) = \prod_{k=0}^{p-1} (\alpha - \zeta^k)
\]
where \( x = wp(p - 1) \). It follows that
\[
(2.6) \quad \mathfrak{P}^{wp+x} \mid \prod_{k=0}^{p-1} (\alpha - \zeta^k)
\]
and therefore
\[
(2.7) \quad \mathfrak{P}^{wp+1} \mid (\alpha - \zeta^i)
\]
for some \( i \). For \( i \neq j \) we have \((\alpha - \zeta^i) - (\alpha - \zeta^j) = \zeta^j(1 - \zeta^{i-j})\). Therefore, by (2.5),
\[
(2.8) \quad \mathfrak{P}^w \parallel (\alpha - \zeta^i) - (\alpha - \zeta^j).
\]
Thus, by (2.7) and (2.8), \( \mathfrak{P}^w \parallel (\alpha - \zeta^j) \) whenever \( j \neq i \). Therefore,
\[
(2.9) \quad \mathfrak{P}^w \mid (\alpha - \zeta^i).
\]
By (2.6) we have
\[
\nu_{\mathfrak{p}} \left( \prod_{k=0}^{p-1} (\alpha - \zeta^k) \right) \geq wp + x.
\]
Hence
\[
\nu_{\mathfrak{p}} \left( \prod_{k=0}^{p-1} (\alpha - \zeta^k) \right) = \nu_{\mathfrak{p}} \left( \prod_{j \neq i} (\alpha - \zeta^j) \right) + \nu_{\mathfrak{p}} (\alpha - \zeta^i)
\]
\[
= (p - 1)w + \nu_{\mathfrak{p}} (\alpha - \zeta^i) \geq wp + x.
\]
It follows that \( \nu_{\mathfrak{p}} (\alpha - \zeta^i) \geq w + x \). Therefore
\[
\mathfrak{P}^{wp+x} \mid (\alpha - \zeta^i).
\]
Hence, \( \alpha \equiv \zeta^i \pmod{\mathfrak{P}^{wp+x}} \). Since \( \kappa \equiv 1 \pmod{\mathfrak{m}} \), \( e^{-N} \equiv 1 \pmod{\mathfrak{m}} \), and \( e^\theta \equiv 1 \pmod{\mathfrak{m}} \), (2.4) implies that \( \kappa \equiv 1 \pmod{\mathfrak{P}^{wp^2}} \), \( e^{-N} \equiv 1 \pmod{\mathfrak{P}^{wp^2}} \), and \( e^\theta \equiv 1 \pmod{\mathfrak{P}^{wp^2}} \). Since \( wp^2 \geq wp + 1 \) and \( w + x = w + wp(p - 1) \geq wp + 1 \), we obtain \( c \equiv \zeta^i \pmod{\mathfrak{P}^{wp+1}} \) and \( b \equiv \zeta \pmod{\mathfrak{P}^{wp+1}} \). Since \( \zeta \equiv 1 \pmod{E^p} \), \( \mathfrak{P} \) splits completely in \( M/E \) and \( K/E \) by Theorem 119 of [4]. By the Galois theory of prime decomposition in algebraic number fields, it follows that \( \mathfrak{p} \) splits completely in \( L/k \). Therefore, every prime divisor of \( (p) \) splits completely in \( L/k \). In particular, no prime divisor of \( (p) \) ramifies in \( L/k \). Therefore \( L/k \) is tamely ramified.

**Step 6.** We now show that \( C(L,k) = c^{m(p-1)/2} \). From Step 1 the prime factors \( l_i \) of \( (a) \), \( 1 \leq i \leq s \), are distinct and are contained in the class \( c \) of \( C(k) \). Furthermore, each \( l_i \) totally ramifies in \( E/k \). Let \( l_i \mathcal{O}_E = \mathcal{L}_i^p \) where \( \mathcal{L}_i \) is a prime ideal in \( E \). From Step 2 the prime factors \( q_i \) of \( (\kappa) \), \( 1 \leq i \leq s \), are distinct and are contained in the class \( c^{-1} \) of \( C(k) \). Furthermore, each \( q_i \) either remains prime or splits completely in \( E/k \). Assume \( q_i \) remains prime.
in $E/k$ for $1 \leq i \leq r$, say, $q_i \mathcal{O}_E = \mathfrak{P}_i$, and $q_j$ splits completely in $E/k$ for $r + 1 \leq j \leq s$, say, $q_j \mathcal{O}_E = \mathcal{O}_E^N$, where $\mathcal{O}_E$ is some prime ideal in $E$. From Step 3 the prime factors $\mathfrak{P}_i$ of $(e)$ are distinct and split completely in $E/k$, say, $p_i \mathcal{O}_E = \mathfrak{P}_i^N$. Moreover, $p_i$ is a prime ideal in $k$ which is contained in the trivial class $X \in \mathcal{W}_{E/k}$, and such that $i \neq j$ implies $p_i \neq p_j$. Finally, by construction, the ideals $(a), (\kappa)$, and $(e)$ are pairwise relatively prime, and they are each prime to $(p)$. We can now describe $d_{L/E}$. We have $K = E(\beta)$ where $\beta = b = \zeta e^{-N}$. Since

$$(b) = \left( \prod_{i=1}^t \mathfrak{P}_i^{-b_i,N} \right) \mathcal{O}_E^{p^N}$$

where $(b_i, p) = 1$ for each $1 \leq i \leq t$, it follows by the proof of Theorem 118 of [4] that the prime ideals in $E$ which ramify in $K/E$ are precisely the prime factors of the ideals $\mathfrak{P}_i^N$ for $1 \leq i \leq t$. Therefore, by the first part of the proof of Proposition 3 of [1],

$$(2.9) \quad \left( \prod_{i=1}^t \mathfrak{P}_i^{p(p-1)N} \right) \parallel d_{L/E}.$$  

Furthermore, the only other possible prime factors of $d_{L/E}$ are prime ideals in $E$ which ramify in $M/E$. By Theorem 118 of [4] these will be among the prime factors of $(e)$ where $c = \kappa \alpha e^0$. Since the prime factors of $(e^0)$ are included in the set of prime factors of $(b) = (e^{-N})$, which all ramify in $L/E$, their contribution to $d_{L/E}$ is given by (2.9). It remains to determine the contribution made to $d_{L/E}$ from $(\kappa)$ and $(\alpha)$. Arguing as in the case of the extension $K/E$, we obtain

$$(2.10) \quad \left( \prod_{i=1}^s \mathfrak{P}_i^{p(p-1)} \right) \parallel d_{L/E}$$

and

$$(2.11) \quad \left( \prod_{i=1}^r \mathfrak{P}_i^{p(p-1)} \right) \left( \prod_{i=r+1}^s \mathfrak{P}_i^{p(p-1)N} \right) \parallel d_{L/E}.$$  

Taking the product of the factors appearing in (2.9)–(2.11) we obtain $d_{L/E}$. Since $N_{E/k}(\mathfrak{P}_i) = 1$, $N_{E/k}(\mathfrak{P}_i^N) = q_i^p$ for $1 \leq i \leq r$, $N_{E/k}(\mathfrak{P}_i^N) = q_i^p$ for $r + 1 \leq i \leq s$, and $N_{E/k}(\mathfrak{P}_i) = p_i^p$, we have, letting $\delta = (p-1)/2$,

$$C(L, k) = C(E, k)^{[L:E]}(\mathfrak{P}_E/k(C(L, E)) = \kappa p^2 \delta \mathfrak{M}_{E/k}(\text{cl}(d_{L/E}^{1/2}))$$

$$= \kappa p^2 \delta \text{cl}(N_{E/k}(d_{L/E}^{1/2})) = \kappa p^2 \delta \zeta^{p^2 \delta} X^{p^2 \delta}$$

$$= \kappa p^2 \delta \zeta^{-p^2 \delta} X^{p^2 \delta} = \kappa p^2 \delta = \kappa^{m(p-1)/2}.$$  

Hence, $R_4(k, G) \supseteq C(k)^{m(p-1)/2}$. 

Acknowledgements. This work appears as part of the author’s Ph.D. thesis. He would like to thank Professors Leon R. McCulloh and Stephen V. Ullom for their comments and suggestions.

References


Department of Mathematics
College of Charleston
66 George Street
Charleston, South Carolina 29424-0001
U.S.A.
E-mail: carter@math.cofc.edu

Received on 5.6.1996 (2997)