ACTA ARITHMETICA
LXXVIII.3 (1997)

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 $\mathfrak{O}_L$ and $\mathfrak{o}$ denote the rings of integers in L and k, respectively. As an $\mathfrak{o}$-module, $\mathfrak{O}_L$ 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 $\mathrm{Gal}(L/k) \simeq G$, $C(L,k)$ varies over a subset $R(k,G)$ of $C(k)$. If we consider only tamely ramified such extensions, then this set is denoted by $R_{\mathrm{t}}(k,G)$. An interesting problem is to determine $R(k,G)$ or $R_{\mathrm{t}}(k,G)$ 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 μ_n of nth roots of unity, then $R(k,G) = R_{\mathrm{t}}(k,G) = C(k)^d$ (the subgroup of $C(k)$ consisting of dth 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 $R_{\mathrm{t}}(k,G)$ 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 μ_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 $\mathrm{Gal}(E/k) \simeq B$. As L varies over all tamely ramified normal extensions of k of a particular type which contain E, and such that $\mathrm{Gal}(L/k) \simeq G$, $C(L,k)$ varies over a subset $R_{\mathrm{t}}(E/k,\Sigma)$ of $C(k)$. It is shown that when the ring of integers in E is free as an $\mathfrak{o}$-module, then $R_{\mathrm{t}}(E/k,\Sigma)$ 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 $R_{\mathrm{t}}(k,G)$. Making essential use of results of [1] and [2], we will show that $R_{\mathrm{t}}(k,G)$ 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 nonabelian group of order $p^3 = mn$ where n is the exponent of G. If $\mu_n \subseteq k$ then*

$$R_{\mathrm{t}}(k, G) = C(k)^{m(p-1)/2}.$$

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*

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

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

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

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

$$\mathfrak{p}^{fg(e-1)} \parallel N_{L/k}(\mathfrak{D}) = d_{L/k}.$$

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

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

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

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

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*

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

Proof. There are two cases to consider.

Case 1. Suppose $n = p$. Let $\mathfrak{c}$ be any class in $C(k)$. We construct a tamely ramified normal extension L/k such that $\mathrm{Gal}(L/k) \simeq G$ and

$C(L,k) = \mathfrak{c}^{m(p-1)/2}$: by Theorem 2 of [7] there exists a tamely ramified normal extension E/k of degree p such that $C(E,k) = \mathfrak{c}^{(p-1)/2}$. 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 $\mathrm{Gal}(L/k) \simeq G$ and $C(L,k) = (\mathfrak{c}X)^{m(p-1)/2} = \mathfrak{c}^{m(p-1)/2}$. Therefore

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

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 $\mathfrak{c}$ 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 $\mathrm{Gal}(L/k) \simeq G$. We then show in the remaining two steps that L/k is tamely ramified and $C(L,k) = \mathfrak{c}^{m(p-1)/2}$.

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

Let $\mathfrak{m} = (1-\zeta)^{p^2}$. Choose an odd integer $s > 3$ such that $\mathfrak{c}^s = \mathfrak{c}$. Let $\mathfrak{l}$ be a prime ideal in $\mathfrak{c}$ such that $\mathfrak{l}$ is not a factor of (p). Let $C_k(\mathfrak{m})$ be the ray class group modulo $\mathfrak{m}$ of k, and let $\mathfrak{c}_{\mathfrak{m}}$ be the element of $C_k(\mathfrak{m})$ which contains $\mathfrak{l}$. Choose distinct prime ideals $\mathfrak{l}_1,\ldots,\mathfrak{l}_s$ in $\mathfrak{c}_{\mathfrak{m}}$. Choose positive integers u_i, $1 \le i \le s$, such that $(u_i,p) = 1$ for each i and $\sum_{i=1}^{s} u_i = p^2 s$ (e.g. $u_i = p^2-1$ for $1 \le i \le (s+1)/2$, $u_i = p^2+1$ for $(s+3)/2 \le i \le s-1$, and $u_s = p^2+2$). Let $\mathfrak{l}_{s+1}$ be a prime ideal in $\mathfrak{c}^{-1}$. Then

$$(a) = \Big(\prod_{i=1}^{s} \mathfrak{l}_i^{u_i}\Big)\mathfrak{l}_{s+1}^{p^2 s} \tag{2.1}$$

where $a \in \mathfrak{o}$ and $a \equiv 1 \pmod{\mathfrak{m}}$. Let $E = k(\alpha)$ where $\alpha^p = a$. Let ζ be a primitive pth root of unity. By Kummer theory E/k is cyclic of degree p with, say, $\mathrm{Gal}(E/k) \simeq \langle \varrho \rangle$ 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 $\mathfrak{l}_1,\ldots,\mathfrak{l}_s$. 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

$$d_{E/k} = \Big(\prod_{i=1}^{s} \mathfrak{l}_i\Big)^{p-1}.$$

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

$$C(E,k) = \mathrm{cl}(d_{E/k}^{1/2}) = \mathrm{cl}\Big(\prod_{i=1}^{s} \mathfrak{l}_i\Big)^{(p-1)/2} = \mathfrak{c}^{s(p-1)/2} = \mathfrak{c}^{(p-1)/2}.$$

Step 2. In this step we construct the element κ. Let $\mathfrak{q}$ be a prime ideal in $\mathfrak{c}^{-1}$ such that $\mathfrak{q}$ is not a factor of (p). Note that $(\mathfrak{c}^{-1})^s = (\mathfrak{c}^s)^{-1} = \mathfrak{c}^{-1}$

where s is the integer of Step 1. Let $\mathfrak{c}'_{\mathfrak{m}}$ be the class in $C_k(\mathfrak{m})$ which contains $\mathfrak{q}$ and choose distinct prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ in $\mathfrak{c}'_{\mathfrak{m}}$ such that $(\mathfrak{q}_i, \mathfrak{l}_j) = 1$ for $1 \le i \le s$ and $1 \le j \le s+1$ where the $\mathfrak{l}_j$ are the prime ideals of Step 1. Choose positive integers v_i for $1 \le i \le s$ such that $(v_i, p) = 1$ and $\sum_{i=1}^{s} v_i = ps$. Let $\mathfrak{q}_{s+1}$ be a prime ideal in $(\mathfrak{c}'_{\mathfrak{m}})^{-1}$ such that $(\mathfrak{q}_{s+1}, \mathfrak{l}_j) = 1$ for $1 \le j \le s+1$. We have

$$(\kappa) = \Big(\prod_{i=1}^{s} \mathfrak{q}_i^{v_i}\Big)\mathfrak{q}_{s+1}^{ps} \tag{2.2}$$

where $\kappa \in \mathfrak{o}$ and $\kappa \equiv 1 \pmod{\mathfrak{m}}$. Since $((\kappa), d_{E/k}) = 1$ each $\mathfrak{q}_i$ 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, $\mathfrak{b} = (\alpha\kappa)$, and $\mathfrak{m} = (1-\zeta)^{p^2}$. Construct e as outlined in that proof. Then

$$(e) = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{b_i}\Big)\mathfrak{Q}^{pt} \tag{2.3}$$

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 $\mathrm{Gal}(L/k) \simeq G$.

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

$$(1-\zeta) = \prod_{i=1}^{g} \mathfrak{p}_i^{w_i} \tag{2.4}$$

where the $\mathfrak{p}_i$ are distinct prime ideals in k and the w_i are positive integers. Let $\mathfrak{p} = \mathfrak{p}_1$ and $w = w_1$. Thus

$$v_{\mathfrak{p}}(1-\zeta) = w. \tag{2.5}$$

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

$$\mathfrak{p}^{wp+x} \mid (a-1) = (\alpha^p - 1) = \prod_{k=0}^{p-1} (\alpha - \zeta^k)$$

where $x = wp(p-1)$. It follows that

$$\mathfrak{P}^{wp+x} \mid \prod_{k=0}^{p-1} (\alpha - \zeta^k) \tag{2.6}$$

and therefore

$$\mathfrak{P}^{w+1} \mid (\alpha - \zeta^i) \tag{2.7}$$

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),

$$\mathfrak{P}^{w} \parallel (\alpha - \zeta^i) - (\alpha - \zeta^j). \tag{2.8}$$

Thus, by (2.7) and (2.8), $\mathfrak{P}^w \parallel (\alpha - \zeta^j)$ whenever $j \neq i$. Therefore,

$$v_{\mathfrak{P}}\Big(\prod_{j \neq i} (\alpha - \zeta^j)\Big) = (p-1)w.$$

By (2.6) we have

$$v_{\mathfrak{P}}\Big(\prod_{k=0}^{p-1} (\alpha - \zeta^k)\Big) \geq wp + x.$$

Hence

$$\begin{aligned} v_{\mathfrak{P}}\Big(\prod_{k=0}^{p-1} (\alpha - \zeta^k)\Big) &= v_{\mathfrak{P}}\Big(\prod_{j \neq i} (\alpha - \zeta^j)\Big) + v_{\mathfrak{P}}(\alpha - \zeta^i) \\ &= (p-1)w + v_{\mathfrak{P}}(\alpha - \zeta^i) \geq wp + x. \end{aligned}$$

It follows that $v_{\mathfrak{P}}(\alpha - \zeta^i) \geq w + x$. Therefore

$$\mathfrak{P}^{w+x} \mid (\alpha - \zeta^i).$$

Hence, $\alpha \equiv \zeta^i \pmod{\mathfrak{P}^{w+x}}$. 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 $C(L,k) = \mathfrak{c}^{m(p-1)/2}$. From Step 1 the prime factors $\mathfrak{l}_i$ of (a), $1 \leq i \leq s$, are distinct and are contained in the class $\mathfrak{c}$ of $C(k)$. Furthermore, each $\mathfrak{l}_i$ totally ramifies in E/k. Let $\mathfrak{l}_i \mathfrak{O}_E = \mathfrak{L}_i^p$ where $\mathfrak{L}_i$ is a prime ideal in E. From Step 2 the prime factors $\mathfrak{q}_i$ of (κ), $1 \leq i \leq s$, are distinct and are contained in the class $\mathfrak{c}^{-1}$ of $C(k)$. Furthermore, each $\mathfrak{q}_i$ either remains prime or splits completely in E/k. Assume $\mathfrak{q}_i$ remains prime in E/k for $1 \le i \le r \le s$, say, $\mathfrak{q}_i\mathfrak{O}_E = \mathfrak{Q}_i$, and $\mathfrak{q}_j$ splits completely in E/k for $r+1 \le j \le s$, say, $\mathfrak{q}_j\mathfrak{O}_E = \mathfrak{Q}_j^N$, where $\mathfrak{Q}_j$ 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, $\mathfrak{p}_i\mathfrak{O}_E = \mathfrak{P}_i^N$. Moreover, $\mathfrak{p}_i$ is a prime ideal in k which is contained in the trivial class $X \in W_{E/k}$, and such that $i \ne j$ implies $\mathfrak{p}_i \ne \mathfrak{p}_j$. 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 $\beta^p = b = \zeta e^{-N}$. Since

$$(b) = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{-b_i N}\Big)\mathfrak{Q}^{ptN}$$

where $(b_i, p) = 1$ for each $1 \le i \le t$, 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 $1 \le i \le t$. Therefore, by the first part of the proof of Proposition 3 of [1],

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

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 (c) where $c = \kappa\alpha e^{\theta}$. Since the prime factors of (e^{θ}) 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 (κ) and (α). Arguing as in the case of the extension K/E, we obtain

$$\Big(\prod_{i=1}^{s} \mathfrak{L}_i^{p(p-1)}\Big) \parallel d_{L/E} \tag{2.10}$$

and

$$\Big(\prod_{i=1}^{r} \mathfrak{Q}_i^{p(p-1)}\Big)\Big(\prod_{i=r+1}^{s} \mathfrak{Q}_i^{p(p-1)N}\Big) \parallel d_{L/E}. \tag{2.11}$$

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

$$\begin{aligned} C(L,k) &= C(E,k)^{[L:E]}\mathfrak{N}_{E/k}(C(L,E)) = \mathfrak{c}^{p^2\delta}\mathfrak{N}_{E/k}(\mathrm{cl}(d_{L/E}^{1/2})) \\ &= \mathfrak{c}^{p^2\delta}\,\mathrm{cl}(N_{E/k}(d_{L/E}^{1/2})) = \mathfrak{c}^{p^2\delta}\mathfrak{c}^{sp\delta}\mathfrak{c}^{-sp^2\delta}X^{tp^2\delta} \\ &= \mathfrak{c}^{p^2\delta}\mathfrak{c}^{p\delta}\mathfrak{c}^{-p^2\delta}X^{p^2\delta} = \mathfrak{c}^{p\delta} = \mathfrak{c}^{m(p-1)/2}. \end{aligned}$$

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

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

[1] J. E. Carter, *Steinitz classes of a nonabelian extension of degree* p^3, Colloq. Math. 71 (1996), 297–303.

[2] —, *Characterization of Galois extensions of prime cubed degree*, Bull. Austral. Math. Soc. 55 (1997), 99–112.

[3] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.

[4] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981.

[5] R. L. Long, *Steinitz classes of cyclic extensions of prime degree*, J. Reine Angew. Math. 250 (1971), 87–98.

[6] —, *Steinitz classes of cyclic extensions of degree* l^r, Proc. Amer. Math. Soc. 49 (1975), 297–304.

[7] L. R. McCulloh, *Cyclic extensions without integral bases*, ibid. 17 (1966), 1191–1194.

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)