COLLOQUIUM MATHEMATICUM

VOL. 71 1996 NO. 2

STEINITZ CLASSES OF A NONABELIAN EXTENSION OF DEGREE p^3

BY

JAMES E. CARTER (CHARLESTON, SOUTH CAROLINA)

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 $C(L,k)$ (see [FT]). Now let G be a finite group. As L varies over all normal extensions of k with Galois group $\mathrm{Gal}(L/k)$ isomorphic to G, $C(L,k)$ varies over a subset $R(k,G)$ of *realizable classes* of the class group $C(k)$ of k. If we consider only tamely ramified extensions of k, then we denote this set by $R_{\mathrm{t}}(k,G)$. From now on, let p be an odd prime. In [L1], $R_{\mathrm{t}}(k,G)$ is determined when G is a cyclic group of order p. In this case it is shown that $R_{\mathrm{t}}(k,G)$ is actually a subgroup of $C(k)$. This result is extended in [L2] to include cyclic groups of order p^r, where $r \ge 1$.

In the present paper we consider the following situation. With the notation as above, assume k contains the multiplicative group μ_p of pth roots of unity. Let G be the nonabelian group of order p^3 given in terms of generators and relations by

(1) $$G = \langle \eta,\tau,\xi \mid \eta^p=\tau^p=\xi^p=1,\ [\eta,\tau]=1=[\eta,\xi],\ [\tau,\xi]=\eta\rangle.$$

$A=\langle \eta,\tau\rangle$ is a normal subgroup of G and we have an exact sequence of groups

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

where B is cyclic of order p. Fix, once and for all, a tamely ramified normal extension E/k with $\mathrm{Gal}(E/k)\simeq B$. Let ζ be a primitive pth root of unity. If F is a field, denote by $F^\times$ the set of nonzero elements of F, and by F^p the multiplicative group of pth powers of elements of $F^\times$. By Kummer theory there exists an $a\in k^\times$ such that $\langle ak^p\rangle$ is a cyclic subgroup of $k^\times/k^p$ of order p, and $E=k(\alpha)$, where $\alpha^p=a$. Furthermore, $\mathrm{Gal}(E/k)=\langle\varrho\rangle$, where $\varrho(\alpha)=\zeta\alpha$.

Define the elements N and θ of the group ring $\mathbb{Z}[\langle\varrho\rangle]$ by $N=\sum_{i=0}^{p-1}\varrho^i$ and $\theta=\sum_{i=0}^{p-1} i\varrho^i$. Let G be given by (1). If L is a field on which a group H

1991 *Mathematics Subject Classification*: Primary 11R04.

acts, and S is a subgroup of H, denote by L^S the subfield of L fixed by S. Using exponential notation to denote the action of N and θ on elements of E, suppose there exists an $e \in E^\times$ such that the element $b = e^{-N}$ of $k^\times$ has order $p \pmod{k^p}$, $c = e^\theta$ has order $p \pmod{E^p}$, and $\langle bE^p\rangle$ and $\langle cE^p\rangle$ are distinct cyclic subgroups of $E^\times/E^p$ of order p. Let $F = k(\beta)$ and $M = E(\gamma)$, where $\beta^p = b$ and $\gamma^p = c$. By Kummer theory it follows that $K = EF$ and $L = MK$ are elementary abelian extensions of degree p^2 of k and E, respectively. Moreover, since $\varrho(c) = \varrho(e^\theta) = e^{\varrho\theta} = e^{\theta-N+p} = e^{-N}e^\theta e^p = bce^p$, we have $\varrho^i(c) \equiv c \pmod{\langle b\rangle E^p}$ for every positive integer i. Hence, $B = \langle b, c\rangle E^p = \langle b, \varrho^i(c)\rangle E^p = \varrho^i(B)$ for every positive integer i. Since $L = E(B^{1/p})$, where $B^{1/p}$ is the set of pth roots of elements of B, it follows that every k-embedding of L into an algebraic closure of k is a k-automorphism of L. Therefore L/k is a normal extension and, consequently, a Galois extension. A routine argument shows that there exists an isomorphism $\phi_L : \mathrm{Gal}(L/k) \to G$ such that $E = L^{\phi_L^{-1}(A)}$. Conversely, if L is any Galois extension of k containing E such that $\phi_L : \mathrm{Gal}(L/k) \to G$ is an isomorphism with $E = L^{\phi_L^{-1}(A)}$, it is not difficult to show that there exists subfields F, M, and K of L as described above. When an extension L/k as just characterized is tamely ramified, we will call it a *G-extension with respect to E/k and Σ*. As L varies over all such extensions of k, $C(L, k)$ varies over a subset $R_{\mathrm{t}}(E/k, \Sigma)$ of $C(k)$.

We will determine $R_{\mathrm{t}}(E/k, \Sigma)$ (Theorem 6) in two stages. In Section 1 we obtain a description of the discriminant ideal $d_{L/E}$ for a G-extension with respect to E/k and Σ (Proposition 3). We can then use a result of [A], and the characterization of L/k indicated above, to prove our main result in Section 2. As an immediate consequence we find that if the ring of integers $\mathfrak{O}_E$ in E is free as an $\mathfrak{o}$-module, then $R_{\mathrm{t}}(E/k, \Sigma)$ is a subgroup of $C(k)$ (Corollary 7).

1. Arithmetic considerations. Standard facts from algebraic number theory used in this and the following sections can be found in [FT], [J] or [L]. If $\mathfrak{X}$ and $\mathfrak{Z}$ are ideals in an algebraic number field then $\mathfrak{X}\|\mathfrak{Z}$ means $\mathfrak{X}\mathfrak{Y} = \mathfrak{Z}$, where $\mathfrak{Y}$ is an ideal relatively prime to $\mathfrak{X}$.

LEMMA 1. *The elements e, b, and c satisfying the conditions stated above may be chosen so that $e \in \mathfrak{O}_E$ with $b = e^N$ and $c = e^\theta$.*

Proof. If e_1 is a nonzero element of $\mathfrak{O}_E$ then $(ee_1^p)^{-N} = e^{-N}(e_1^{-N})^p$ and $(ee_1^p)^\theta = e^\theta(e_1^\theta)^p$. We also have $(e^{p-1})^N = e^{-N}(e^N)^p$ and $(e^{p-1})^\theta = (e^\theta)^{p-1}$. The lemma follows from these facts and Kummer theory.

Let $\varepsilon : \mathbb{Z}[\langle\varrho\rangle] \to \mathbb{Z}$ be the augmentation homomorphism. Let (e) be the principal ideal in $\mathfrak{O}_E$ generated by e. Reordering the prime factors of (e) if necessary, we have

$$(e) = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{A_i}\Big)\mathfrak{A},$$

where the $\mathfrak{P}_i$ are distinct prime ideals in E which split completely in E/k, and such that $\mathfrak{P}_i \cap \mathfrak{o} \neq \mathfrak{P}_j \cap \mathfrak{o}$ whenever $i \neq j$; $\mathfrak{A}$ is an ideal in E divisible only by prime ideals in E which either remain prime or totally ramify in E/k; and the A_i are elements of $\mathbb{Z}[\langle\varrho\rangle]$ with nonnegative coefficients.

Let $\mathfrak{L}$ be a prime factor of $\mathfrak{A}$. Then $\mathfrak{L}^N = \mathfrak{L}^{\varepsilon(N)}$ and $\mathfrak{L}^\theta = \mathfrak{L}^{\varepsilon(\theta)}$. Therefore, since $\varepsilon(N) = p$, $\varepsilon(\theta) = p(p-1)/2$, and $A_iN = \varepsilon(A_i)N$ for each i, we have

$$(e^N) = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{\varepsilon(A_i)N}\Big)\mathfrak{B}^p \tag{2}$$

and

$$(e^\theta) = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{A_i\theta}\Big)\mathfrak{C}^p, \tag{3}$$

where $\mathfrak{B}$ and $\mathfrak{C}$ are ideals in E.

LEMMA 2. *Let $A = \sum a_j\varrho^i \in \mathbb{Z}[\langle\varrho\rangle]$. Then $A\theta \equiv \varepsilon(A)\theta + dN \pmod p$, where $d = -\sum ja_j$. In particular, if $\varepsilon(A) \equiv 0 \pmod p$ then $A\theta \equiv dN \pmod p$.*

Proof. We have $(1-\varrho)\theta = N-p$. Hence, $\varrho\theta \equiv \theta - N \pmod p$. Applying ϱ repeatedly to this congruence we find that $\varrho^r\theta \equiv \theta - rN \pmod p$, where r is any nonnegative integer. Hence $A\theta \equiv \varepsilon(A)\theta + dN \pmod p$, where $d = -\sum ja_j$.

PROPOSITION 3. *Let L/k be a G-extension with respect to E/k and Σ. Then*

$$(e) = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{A_i}\Big)\mathfrak{A}$$

as described in the paragraph following Lemma 1, and we have

$$d_{L/E} = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{n_iN}\Big)^{p(p-1)},$$

where $n_i \in \{0,1\}$. Moreover,

(i) *if $\varepsilon(A_i) \not\equiv 0 \pmod p$ then $n_i = 1$;*

(ii) *if $\varepsilon(A_i) \equiv 0 \pmod p$ then $A_i\theta \equiv d_iN \pmod p$, where $d_i \in \mathbb{Z}$. We then have $n_i = 1$ if and only if $d_i \not\equiv 0 \pmod p$.*

Proof. Suppose $\mathfrak{P}$ is a prime ideal in E and $\mathfrak{P}$ ramifies in L/E. Since L/E is tamely ramified, $\mathfrak{P}$ is not a factor of (p), and the inertia group $T_{\mathfrak{P}}$

of $\mathfrak{P}$ in $\mathrm{Gal}(L/E)$ is cyclic. Since $\mathrm{Gal}(L/E)$ is elementary abelian of type (p,p) it follows that $T_{\mathfrak{P}}$ has order p. Hence, the ramification index of $\mathfrak{P}$ in L/E is p. Furthermore, either $\mathfrak{P}$ ramifies in M/E or $\mathfrak{P}$ ramifies in K/E. Assume the latter. Since K/E is tamely ramified, $\mathfrak{P}$ occurs as a factor of $d_{K/E}$ exactly $p-1$ times, i.e.,

$$v_{\mathfrak{P}}(d_{K/E}) = p-1.$$

Let $N_{K/E}$ denote the ideal norm from K to E. From

$$d_{L/E} = d_{K/E}^{[L:K]} N_{K/E}(d_{L/K})$$

we have

$$v_{\mathfrak{P}}(d_{L/E}) = p(p-1). \tag{4}$$

Since $K = E(\beta)$, where $\beta^p = e^N$, it follows from (2), the proof of Theorem 118 of [H], and (4) that

$$\Big(\prod_{\varepsilon(A_i)\not\equiv 0\,(p)} \mathfrak{P}_i^N\Big)^{p(p-1)} \Big\| d_{L/E}. \tag{5}$$

The remaining prime factors of $d_{L/E}$ are the prime ideals in E which ramify in M/E. We have $M = E(\gamma)$, where $\gamma^p = e^\theta$. Consider (3). If $\varepsilon(A_i) \not\equiv 0 \pmod p$ then the contribution made to $d_{L/E}$ from the ideal $\mathfrak{P}_i^{A_i\theta}$ is already apparent in (5) since the prime factors of $\mathfrak{P}_i^{A_i\theta}$ are among those of $\mathfrak{P}_i^{\varepsilon(A_i)N}$. Suppose $\varepsilon(A_i) \equiv 0 \pmod p$. By Lemma 2 this implies $A_i\theta \equiv d_iN \pmod p$, where $d_i \in \mathbb{Z}$. By an argument similar to that which produced (5) we obtain

$$\Big(\prod_{\substack{\varepsilon(A_i)\equiv 0\,(p)\\ d_i\not\equiv 0\,(p)}} \mathfrak{P}_i^N\Big)^{p(p-1)} \Big\| d_{L/E}.$$

2. Realizable classes. Let $\delta = (p-1)/2$. By Section 2 of [L1] we have $C(E,k) = \mathfrak{c}^\delta$ for some $\mathfrak{c} \in C(k)$. Let $W_{E/k}$ be the subgroup of $C(k)$ generated by the classes in $C(k)$ which contain at least one prime ideal in k which splits completely in E/k. In this section we will show that

$$R_{\mathrm{t}}(E/k, \Sigma) = (\mathfrak{c}W_{E/k})^{p^2\delta},$$

where $(\mathfrak{c}W_{E/k})^{p^2\delta}$ is the set of $(p^2\delta)$th powers of elements of the coset $\mathfrak{c}W_{E/k}$. In particular, if $C(E,k) = 1$ then we have

$$R_{\mathrm{t}}(E/k, \Sigma) = (W_{E/k})^{p^2\delta}.$$

By replacing the extension F/k in the proof of Lemma 2.5 of [L1] with our extension E/k, we obtain a proof of the following lemma.

Lemma 4. *Every class in $W_{E/k}$ contains infinitely many prime ideals in k which split completely in E/k.*

If F is an arbitrary algebraic number field and $\mathfrak{I}$ is an ideal in F, then $\mathrm{cl}(\mathfrak{I})$ denotes the class of $\mathfrak{I}$ in $C(F)$. Suppose L/k is a G-extension with respect to E/k and Σ. By Proposition 3,

$$d_{L/E} = \Big(\prod_{i=1}^{s} \mathfrak{P}_i^N\Big)^{p(p-1)},$$

where $s \le t$, with t and the $\mathfrak{P}_i$ as indicated in the statement of Proposition 3 (the latter after a possible relabelling of subscripts). From the theorem of [A], and the fact that $[L:E]$ is odd, it follows that $C(L,E) = \mathrm{cl}(d_{L/E}^{1/2})$. Let $\mathfrak{p}_i$ be the prime ideal in k such that $\mathfrak{p}_i\mathfrak{O}_E = \mathfrak{P}_i^N$ (hence $N_{E/k}(\mathfrak{P}_i^N) = \mathfrak{p}_i^p$, where $N_{E/k}$ is the ideal norm from E to k). Let $\mathfrak{N}_{E/k}$ denote the norm from $C(E)$ to $C(k)$. Since

$$C(L,k) = C(E,k)^{[L:E]}\mathfrak{N}_{E/k}(C(L,E))$$

we have

$$\begin{aligned} C(L,k) &= \mathfrak{c}^{p^2\delta}\mathfrak{N}_{E/k}\Big(\mathrm{cl}\Big(\prod_{i=1}^{s}\mathfrak{P}_i^N\Big)\Big)^{p\delta} \\ &= \mathfrak{c}^{p^2\delta}\,\mathrm{cl}\Big(N_{E/k}\Big(\prod_{i=1}^{s}\mathfrak{P}_i^N\Big)\Big)^{p\delta} = \mathfrak{c}^{p^2\delta}\Big(\prod_{i=1}^{s}\mathrm{cl}(\mathfrak{p}_i)\Big)^{p^2\delta} \in (\mathfrak{c}W_{E/k})^{p^2\delta}. \end{aligned}$$

Hence,

$$R_{\mathrm{t}}(E/k,\Sigma) \subseteq (W_{E/k})^{p^2\delta}. \tag{6}$$

We now show that the reverse inclusion holds. For a modulus $\mathfrak{m}$ of an algebraic number field F, let $C_F(\mathfrak{m})$ denote the ray class group modulo $\mathfrak{m}$ (see [J]).

Proposition 5. *Let $X \in W_{E/k}$ and let $\mathfrak{b}$ be a fractional ideal in k. Then there exists a G-extension with respect to E/k and Σ such that $C(L,k) = (\mathfrak{c}X)^{p^2\delta}$ and $(d_{L/E},\mathfrak{B}) = 1$, where $\mathfrak{B} = \mathfrak{b}\mathfrak{O}_E$.*

Proof (cf. the proof of Theorem 2.6 in [L1]). Recall that $E = k(\alpha)$, where $\alpha^p = a$ for some $a \in k^\times$ and a is not a pth power of an element of k. Choose an odd integer $t > 3$ such that $X^t = X$, and choose positive integers b_i, $1 \le i \le t$, such that $(b_i,p) = 1$ for each i and $\sum_{i=1}^t b_i = pt$ (e.g. $b_i = p-1$ for $1 \le i \le (t+1)/2$, $b_i = p+1$ for $(t+3)/2 \le i \le t-1$, and $b_t = p+2$). Let $\mathfrak{m}$ be the modulus $(1-\zeta)^{p^2}$ of k. By Lemma 4, X contains infinitely many prime ideals which split completely in E. Since $C_E(\mathfrak{m})$ is finite, there exists a class $\mathfrak{c}_\mathfrak{m} \in C_E(\mathfrak{m})$ containing infinitely many prime ideals $\mathfrak{P}$ which split completely in E/k, and such that $\mathfrak{P}\cap k$ is a prime in X. Choose prime ideals $\mathfrak{P}_1,\ldots,\mathfrak{P}_t \in \mathfrak{c}_{\mathfrak{m}}$ such that

(i) each $\mathfrak{P}_i$ splits completely in E/k;
(ii) for each i, $\mathfrak{p}_i = \mathfrak{P}_i \cap k \in X$;
(iii) $i \neq j$ implies that $\mathfrak{P}_i$ is not conjugate to $\mathfrak{P}_j$;
(iv) for each i, $(\mathfrak{P}_i^N, \mathfrak{B}) = 1$;
(v) for each i, $(\mathfrak{P}_i^N, (a)) = 1$.

Choose a prime ideal $\mathfrak{Q} \in \mathfrak{c}_{\mathfrak{m}}^{-1}$ such that $\mathfrak{Q}$ and all of its conjugates are relatively prime to (a). We have

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

where $e \in E$ and $e \equiv 1 \pmod{\mathfrak{m}}$. Since $\mathfrak{m}$ is a modulus of k, it follows that $e^\theta \equiv 1 \pmod{\mathfrak{m}}$ and $e^{-N} \equiv 1 \pmod{\mathfrak{m}}$ as well. Let $b = e^{-N}$ and $c = e^\theta$. It is straightforward to verify that the elements b and c satisfy the conditions described in the introduction. Furthermore, by Theorem 119 of [H], it follows that the corresponding extensions M/E and K/E are tamely ramified. Hence, L/k is a G-extension with respect to E/k and Σ.

We now show that $C(L,k) = (\mathfrak{c}X)^{p^2\delta}$ and $(d_{L/E}, \mathfrak{B}) = 1$. By the proof of Lemma 1 we may replace the element e with $e' = e^{p-1}$. We have

$$(e') = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{c_i}\Big)\mathfrak{Q}^{p(p-1)t},$$

where $c_i = b_i(p-1)$. Therefore, by Proposition 3(i),

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

Hence, as in the proof of (6), we obtain

$$C(L,k) = \mathfrak{c}^{p^2\delta}\Big(\prod_{i=1}^{t} \mathrm{cl}(\mathfrak{p}_i)\Big)^{p^2\delta} = \mathfrak{c}^{p^2\delta}X^{tp^2\delta} = \mathfrak{c}^{p^2\delta}X^{p^2\delta} = (\mathfrak{c}X)^{p^2\delta}.$$

Finally, by (iv), it follows that $(d_{L/E}, \mathfrak{B}) = 1$.

THEOREM 6. *Let L/k be a G-extension with respect to E/k and Σ. Furthermore, assume $C(E,k) = \mathfrak{c}^\delta$ for some $\mathfrak{c} \in C(k)$. Then*

$$R_{\mathfrak{t}}(E/k,\Sigma) = (\mathfrak{c}W_{E/k})^{p^2\delta}.$$

Proof. (6) and Proposition 5.

Corollary 7. *If L/k is a G-extension with respect to E/k and Σ and $C(E,k)=1$, then*

$$R_{\mathrm{t}}(E/k,\Sigma)=(W_{E/k})^{p^2\delta}.$$

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. He also wishes to thank the anonymous referee for helping to clarify parts of the above presentation.

REFERENCES

[A] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, in: Colloq. Internat. CNRS 24, Paris, 1950, 19–20.

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

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

[J] G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

[L] S. Lang, *Algebraic Number Theory*, Springer, 1986.

[L1] R. L. Long, *Steinitz classes of cyclic extensions of prime degree*, J. Reine Angew. Math. 250 (1971), 87–98.

[L2] —, *Steinitz classes of cyclic extensions of degree l^r*, Proc. Amer. Math. Soc. 49 (1975), 297–304.

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

Received 3 November 1995;
revised 29 February 1996