COLLOQUIUM MATHEMATICUM

VOL. 76 1998 NO. 2

MODULE STRUCTURE OF INTEGERS IN METACYCLIC EXTENSIONS

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], Theorem 13). Now let G be a finite group containing a normal subgroup H. Then we have an exact sequence of groups

$$\Sigma: \quad 1 \to H \to G \to G/H \to 1.$$

With k as above, fix a normal extension E/k with Galois group $\mathrm{Gal}(E/k) \simeq G/H$. Suppose L/k is a normal extension such that $E \subseteq L$, and there exists an isomorphism $\phi_L : \mathrm{Gal}(L/k) \to G$. Furthermore, assume E is the subfield of L fixed by $\phi_L^{-1}(H)$. An extension L/k as just described will be called 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 $R(E/k,\Sigma)$ of the class group $C(k)$ of k. If we consider only tamely ramified extensions then we denote this set by $R_{\mathrm{t}}(E/k,\Sigma)$.

Now let p be an odd prime and assume k contains the multiplicative group μ_p of pth roots of unity. In [C1], $R_{\mathrm{t}}(E/k,\Sigma)$ is determined when L/k is a certain type of nonabelian extension of degree p^3 with $[E:k]=p$. It is shown that if $\mathfrak{O}_E$ 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 consider the following situation. Let p and q be distinct odd prime numbers and assume $\mu_{pq} \subseteq k$. Let G be the metacyclic group of order pq given in terms of generators and relations by

$$\langle \sigma, \tau \mid \sigma^p = 1,\ \tau^q = 1,\ \tau\sigma\tau^{-1} = \sigma^r \rangle$$

where r is a primitive qth root of unity mod p (and hence, $p \equiv 1 \pmod{q}$). Let s be the unique integer in $\{2,3,\ldots,p-1\}$ such that $sr \equiv 1 \pmod{p}$. Then s is also a primitive qth root of unity mod p. Hence, $s^q = 1 + tp$ for some positive integer t.

1991 *Mathematics Subject Classification*: Primary 11R04; Secondary 12F10.

The cyclic subgroup $\langle\sigma\rangle$ of G generated by σ is a normal subgroup of G and we have an exact sequence of groups

$$\Sigma: \quad 1 \to \langle\sigma\rangle \to G \to G/\langle\sigma\rangle \to 1.$$

Fix, once and for all, a tamely ramified normal extension E/k with $\mathrm{Gal}(E/k) \simeq G/\langle\sigma\rangle$. Furthermore, assume p and q are such that $t \not\equiv 0 \pmod{p}$. Then it is possible to apply the method developed in [C1] to determine $R_{\mathrm{t}}(E/k,\Sigma)$ (Theorem 10). As in [C1], we will see that if $\mathfrak{O}_E$ is free as an $\mathfrak{o}$-module, then $R_{\mathrm{t}}(E/k,\Sigma)$ is a subgroup of $C(k)$ (Corollary 11).

1. Metacyclic groups as Galois groups. Let p, q, G, s, and t be as described in the last three paragraphs of the previous section. For the moment, however, we do not require the condition $t \not\equiv 0 \pmod{p}$. Let k be an arbitrary field such that the characteristic of k is not equal to p or q, and $\mu_{pq} \subseteq k$. If K is any field and m is a positive integer then $K^{\times}$ denotes the multiplicative group of nonzero elements of K, and K^m is the multiplicative group of mth powers of elements of $K^{\times}$. If K contains the field M, then $[K : M]$ is the dimension of K as a vector space over M. If A is a group that acts on K and B is a subgroup of A then we write K^B for the subfield of K fixed by B.

In this section we will give a characterization of Galois extensions L/k with $\mathrm{Gal}(L/k)=G$ (Theorems 4 and 6). Our immediate goal is to describe generators for L/k and the action of σ and τ on these generators. To this end let $E=L^{\langle\sigma\rangle}$ and $F=L^{\langle\tau\rangle}$. By Galois theory L/E is a Galois extension of degree p with Galois group $\mathrm{Gal}(L/E) = \langle\sigma\rangle$, and L/F is a Galois extension of degree q with Galois group $\mathrm{Gal}(L/F) = \langle\tau\rangle$. As $[L : k] = pq$ we have $[E : k] = q$, and $[F : k] = p$. From this it follows easily that $E\cap F = k$ and $EF = L$. Also, by Galois theory, E/k is a Galois extension. We have $\mathrm{Gal}(E/k) = \langle\varrho\rangle$ where ϱ is the restriction $\tau|E$ of τ to E. By Kummer theory $E = k(\alpha)$ and $L = E(\beta)$ with $\alpha^q = a$ and $\beta^p = b$ for some $a \in k^{\times}$ and $b \in E^{\times}$ such that $\langle ak^q\rangle$ has order q in $k^{\times}/k^q$, and $\langle bE^p\rangle$ has order p in $E^{\times}/E^p$. Moreover, we may assume α and β chosen so that $\varrho(\alpha) = \zeta_q\alpha$ and $\sigma(\beta) = \zeta_p\beta$.

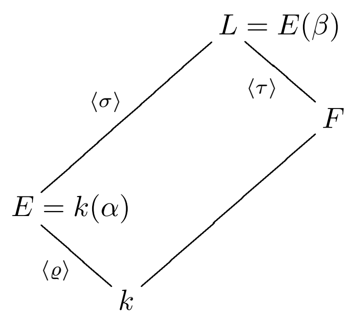


Fig. 1

Since $L = k(\alpha, \beta)$, the action of any element of $\mathrm{Gal}(L/k)$ on L is completely determined by its action on the elements α and β. Thus far we know σ fixes α and $\sigma(\beta) = \zeta_p \beta$. Also, $\tau(\alpha) = \zeta_q \alpha$. It remains to determine $\tau(\beta)$. Let $\mathbb{Z}\langle\varrho\rangle$ be the group ring and denote the action of $\mathbb{Z}\langle\varrho\rangle$ on E by exponentiation. Define $\theta \in \mathbb{Z}\langle\varrho\rangle$ by

$$\theta = \sum_{i=0}^{q-1} s^{q-1-i} \varrho^i.$$

Lemma 1. *$\varrho\theta = s\theta - tp$.*

P r o o f. This follows from the fact that $(s-\varrho)\theta = s^q - \varrho^q = 1 + tp - 1 = tp$.

Lemma 2. *$\sum_{i=0}^{q-1} s^{q-1-i} \equiv 0 \pmod p$.*

P r o o f. We have

$$(s-1) \sum_{i=0}^{q-1} s^{q-1-i} = s^q - 1 = tp.$$

Since p does not divde $s-1$ the result follows.

Now we prove

Proposition 3. *$\tau(\beta) = \beta^s e$ for some $e \in E^\times$. Consequently, $b^t = e^{-\theta}$.*

P r o o f. We will show that $\tau(\beta)/\beta^s \in L^{\langle\sigma^r\rangle} = E$. Then the first statement follows from this since $\tau(\beta)$ is nonzero. From (1) we have $\sigma^r\tau = \tau\sigma$. Hence,

$$\begin{aligned}\sigma^r(\tau(\beta)/\beta^s) &= (\tau\sigma)(\beta)/\sigma^r(\beta^s) = \tau(\zeta_p\beta)/(\zeta_p^{rs}\beta^s) \\ &= \tau(\zeta_p\beta)/(\zeta_p\beta^s) = \tau(\beta)/\beta^s.\end{aligned}$$

Therefore, $\tau(\beta) = \beta^s e$ for some $e \in E^\times$. By successively applying τ to both sides of this equation one obtains

$$\beta = \tau^q(\beta) = \beta^{s^q} \varrho^0(e)^{s^{q-1}} \varrho(e)^{s^{q-2}} \varrho^2(e)^{s^{q-3}} \ldots \varrho^{q-1}(e)^{s^0}.$$

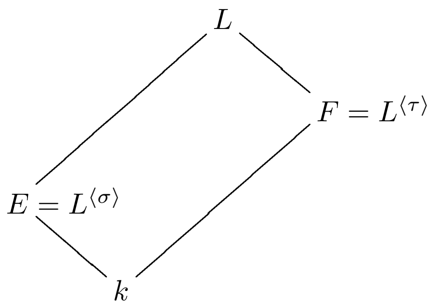
Hence,

$$\beta = \beta^{1+tp} e^\theta = \beta\beta^{tp} e^\theta = \beta b^t e^\theta.$$

Therefore, $b^t = e^{-\theta}$.

We summarize the above results in the following

Theorem 4. *Suppose L/k is a Galois extension such that $\mathrm{Gal}(L/k) = G$. If $E = L^{\langle\sigma\rangle}$ and $F = L^{\langle\tau\rangle}$ then we have the following diagram of subfields of L:*



where $E \cap F = k$ and $L = EF$, and there exist elements $\alpha \in E$ and $\beta \in L$ such that $E = k(\alpha)$ and $L = E(\beta)$, with $\tau(\alpha) = \zeta_q\alpha$ and $\sigma(\beta) = \zeta_p\beta$. Then $\alpha^q = a$ and $\beta^p = b$ where $a \in k^\times$ and $b \in E^\times$. Furthermore, $\langle ak^q\rangle$ is a cyclic subgroup of $k^\times/k^q$ of order q, and $\langle bE^p\rangle$ is a cyclic subgroup of $E^\times/E^p$ of order p. Moreover, if $\varrho = \tau|E$ then $\mathrm{Gal}(E/k) = \langle\varrho\rangle$ and we define $\theta \in \mathbb{Z}\langle\varrho\rangle$ by $\theta = \sum_{i=0}^{q-1} s^{q-1-i}\varrho^i$. Then σ and τ act as k-automorphisms of L according to the following table where $e \in E^\times$ and $b^t = e^{-\theta}$:

	α	β
σ	α	$\zeta_p\beta$
τ	$\zeta_q\alpha$	$\beta^s e$

Now assume that p and q are such that $t \not\equiv 0 \pmod p$. Under this condition we will construct a Galois extension L/k with $\mathrm{Gal}(L/k) \simeq G$.

Keeping the results of Theorem 4 in mind, let $a \in k^\times$ such that $\langle ak^q\rangle$ is a cyclic subgroup of $k^\times/k^q$ of order q. Let $E = k(\alpha)$ where $\alpha^q = a$. Then E/k is a Galois extension of degree q with $\mathrm{Gal}(E/k) = \langle\varrho\rangle$, where $\varrho(\alpha) = \zeta_q\alpha$. By assumption we may choose r such that $t \not\equiv 0 \pmod p$. Now define $\theta \in \mathbb{Z}\langle\varrho\rangle$ by $\theta = \sum_{i=0}^{q-1} s^{q-1-i}\varrho^i$. Suppose there exists an $\varepsilon \in E^\times$ such that $b^t \equiv \varepsilon^{-\theta} \pmod{E^p}$ for some $b \in E^\times$ of order $p \pmod{E^p}$. Since $t \not\equiv 0 \pmod p$ there exists an integer $u \in \{1, \ldots, p-1\}$ such that $ut \equiv 1 \pmod p$. Hence, $ut = 1 + mp$ for some nonnegative integer m. It follows that $b \equiv \varepsilon^{-u\theta}b^{-mp} \equiv \varepsilon^{-u\theta} \pmod{E^p}$. Let $L = E(\beta)$ with $\beta^p = b$ where we may assume $b = \varepsilon^{-u\theta}$. Then L/E is a Galois extension of degree p with $\mathrm{Gal}(L/E) = \langle\sigma\rangle$ where $\sigma(\beta) = \zeta_p\beta$.

PROPOSITION 5. *Let L/k be the extension described in the preceding paragraph. Then L/k is a Galois extension.*

Proof. Let $\langle b\rangle$ be the cyclic subgroup of $E^\times$ generated by b. Let $B = \langle b\rangle E^p$ be the set of all products xy such that $x \in \langle b\rangle$ and $y \in E^p$. Applying Lemma 1 to obtain the following second equality we have $\varrho(b) = \varepsilon^{-u\varrho\theta} = \varepsilon^{-u(s\theta - tp)} = \varepsilon^{(-u\theta)s}\varepsilon^{utp} \equiv b^s \pmod{E^p}$. It follows that $\varrho^i(b) \equiv b^{s^i} \pmod{E^p}$ for each $i \in \{0, 1, \ldots, q-1\}$. Also, for each such i we have $(b^{s^i})^{s^{q-i}} = b^{s^q} = b^{1+tp} \equiv b \pmod{E^p}$. Therefore, $\varrho^i(B) = \langle\varrho^i(b)\rangle E^p = \langle b\rangle E^p = B$ for each

$i \in \{0, 1, \ldots, q-1\}$. Hence, by Lemma 5 of [C2], L/k is a normal extension. Since L/k is a separable extension, it follows that L/k is a Galois extension.

In view of Proposition 5, we have the following exact sequence of groups:

$$1 \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(L/k) \to \mathrm{Gal}(E/k) \to 1$$

where the second arrow from the left is inclusion, and the third is restriction to E. Hence, there exists $\tau \in \mathrm{Gal}(L/k)$ such that $\tau|E = \varrho$. Let $F = L^{\langle\tau\rangle}$. By Galois theory L/F is a Galois extension and $\mathrm{Gal}(L/F) = \langle\tau\rangle$. It is not difficult to show that $E \cap F = k$ and $EF = L$.

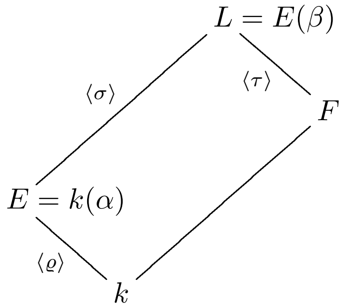


Fig. 2

From the latter fact it follows that the surjective homomorphism

$$\mathrm{Gal}(L/F) \to \mathrm{Gal}(E/k)$$

defined by restriction to E is also injective. Therefore, the order $|\langle\tau\rangle|$ of $\langle\tau\rangle$ is q. Hence, $\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$. Since $\langle\sigma\rangle$ is a normal subgroup of $\mathrm{Gal}(L/k)$, $\langle\sigma\rangle\langle\tau\rangle$ is a subgroup of $\mathrm{Gal}(L/k)$. Furthermore, $|\langle\sigma\rangle\langle\tau\rangle| = |\langle\sigma\rangle||\langle\tau\rangle|/|\langle\sigma\rangle \cap \langle\tau\rangle| = pq$. Therefore, $\mathrm{Gal}(L/k) = \langle\sigma\rangle\langle\tau\rangle$.

THEOREM 6. *Let L/k be the extension shown in Figure* 2. *Then L/k is a Galois extension with* $\mathrm{Gal}(L/k) \simeq G$. *Moreover*, *the action of* $\mathrm{Gal}(L/k)$ *on L is given by the following table where $e \in E^{\times}$ and $b^t = e^{-\theta}$*:

	α	β
σ	α	$\zeta_p\beta$
τ	$\zeta_q\alpha$	$\beta^s e$

Proof. It remains to prove that $\mathrm{Gal}(L/k)$ acts on L as stated, and $\mathrm{Gal}(L/k) \simeq G$.

By definition we have $\sigma(\alpha) = \alpha$, and $\sigma(\beta) = \zeta_p\beta$. Also, since $\tau|E = \varrho$, we get $\tau(\alpha) = \varrho(\alpha) = \zeta_q\alpha$. Applying Lemma 1 to obtain the following fifth equality we have $\tau(\beta)^p = \tau(b) = \varrho(b) = \varrho(\varepsilon^{-u\theta}) = \varepsilon^{-u\varrho\theta} = \varepsilon^{-u(s\theta-tp)} = \varepsilon^{(-u\theta)s}\varepsilon^{utp}$. Therefore, $\tau(\beta) = \beta^s\zeta_p^v\varepsilon^{ut}$ for some integer v. Let $e = \zeta_p^v\varepsilon^{ut}$. Then $e \in E^{\times}$ and, applying Lemma 2 to obtain the following second equality, we have $e^{-\theta} = (\zeta_p^v\varepsilon^{ut})^{-\theta} = (\varepsilon^{ut})^{-\theta} = (\varepsilon^{-u\theta})^t = b^t$.

We have already shown that $\mathrm{Gal}(L/k) = \langle \sigma, \tau \rangle$ where $\sigma^p = 1$ and $\tau^q = 1$. Hence, to complete the proof we need to show that $\tau\sigma\tau^{-1} = \sigma^r$. We have $(\tau\sigma)(\alpha) = \tau(\alpha) = \zeta_q \alpha$, and $(\sigma^r \tau)(\alpha) = \sigma^r(\zeta_q \alpha) = \zeta_q \alpha$. Also, $(\tau\sigma)(\beta) = \tau(\zeta_p \beta) = \zeta_p \beta^s e$, and $(\sigma^r \tau)(\beta) = \sigma^r(\beta^s e) = (\zeta_p^r \beta)^s e = \zeta_p \beta^s e$. It follows that $\tau\sigma = \sigma^r \tau$. Therefore, $\tau\sigma\tau^{-1} = \sigma^r$.

REMARK. For p and q such that $t \not\equiv 0 \pmod p$, Theorem 4 together with Theorem 6 provide a complete characterizaton of Galois extensions L/k with $\mathrm{Gal}(L/k) \simeq G$, provided such extensions of k exist.

For the remainder of the paper, we assume the notation and assumptions introduced in the last three paragraphs of Section 0.

2. Arithmetic considerations. Suppose L/k is a tamely ramified G-extension with respect to E/k and Σ. In this section we will determine the discriminant ideal $d_{L/E}$ of L/E. Standard facts from algebraic number theory used in this and the remaining sections can be found in [FT], [J], or [L].

Let $\mathrm{Gal}(E/k) = \langle \varrho \rangle$. Let $\mathbb{Z}\langle \varrho \rangle$ be the group ring and define $\theta \in \mathbb{Z}\langle \varrho \rangle$ by $\theta = \sum_{i=0}^{q-1} s^{q-1-i} \varrho^i$. Denote the action of $\mathbb{Z}\langle \varrho \rangle$ on E by exponentiation. By Theorem 4 there exist elements b and e in $E^\times$ such that $L = E(\beta)$ where $\beta^p = b$ with $b^t = e^{-\theta}$. Since $t \not\equiv 0 \pmod p$ there is an integer $u \in \{1, \ldots, p-1\}$ such that $ut = 1 + np$ for some nonnegative integer n. Then $b = e^{-u\theta} b^{-np}$. By Kummer theory $E(\beta) = E(\beta_1)$ where $\beta_1^p = e^{-u\theta}$. Hence, for the purpose of determining $d_{L/E}$, we may assume $b = e^{-u\theta}$. Furthermore, we have the following lemma.

LEMMA 7. *We may assume* $e \in \mathfrak{O}_E$ *and* $b = e^{u\theta}$.

Proof. If e_1 is any element of $\mathfrak{O}_E$ then $(e e_1^p)^{-u\theta} = e^{-u\theta}(e_1^{-u\theta})^p$. Also, $(e^{p-1})^{u\theta} = e^{-u\theta}(e^{u\theta})^p$. The lemma follows from these facts and Kummer theory.

If $\mathfrak{O}$ is an arbitrary ring of algebraic integers containing the element x let $\langle x \rangle$ denote the principal ideal in $\mathfrak{O}$ generated by x. In view of Lemma 7 above and Theorem 117 of [H] we have

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

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 which is 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 $\mathfrak{L}^{u\theta} = \mathfrak{L}^{uS}$ where $S = \sum_{i=0}^{q-1} s^{q-1-i}$. Since $(s-1)S = s^q - 1 = tp$ and p does not divide $s-1$, it follows that

$S \equiv 0 \pmod p$. Hence,

$$\langle e^{u\theta}\rangle = \Big(\prod_{i=1}^{n} \mathfrak{P}_i^{uA_i\theta}\Big)\mathfrak{B}^p \tag{1}$$

where $\mathfrak{B}$ is an ideal in E.

Let $N = \sum_{j=0}^{q-1} \varrho^j$. Also, for $A = \sum_{j=0}^{q-1} a_j\varrho^j \in \mathbb{Z}\langle\varrho\rangle$, let $\bar{A} = \sum_{j=0}^{q-1} a_j s^j$.

LEMMA 8. *Suppose* $A = \sum_{j=0}^{q-1} a_j\varrho^j \in \mathbb{Z}\langle\varrho\rangle$. *Then* $A\theta \equiv \bar{A}\theta \pmod p$.

Proof. Since $(s-\varrho)\theta = s^q - \varrho^q = 1 + tp - 1 = tp$ we have $\varrho\theta = s\theta - tp$. Suppose $2 \le j \le q$. By successively applying ϱ to both sides of the last equation $j-1$ times we obtain $\varrho^j\theta = s^j\theta - tp\sum_{k=0}^{j-1} s^{j-1-k}\varrho^k$. It follows that $\varrho^j\theta \equiv s^j\theta \pmod p$ for $0 \le j \le q-1$. Hence, $\sum_{j=0}^{q-1} a_j\varrho^j\theta \equiv \sum_{j=0}^{q-1} a_j s^j\theta \pmod p$.

If $\mathfrak{I}$ is any ideal in E and $\mathfrak{P}$ is a prime ideal in E, let $v_{\mathfrak{P}}(\mathfrak{I})$ denote the exact power to which $\mathfrak{P}$ divides $\mathfrak{I}$.

PROPOSITION 9. *Suppose L/k is a tamely ramified G-extension with respect to E/k and Σ. Then*

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

as described in the paragraph following the proof of Lemma 7 and we have

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

where $n_i \in \{0,1\}$. Moreover, $n_i = 1$ if and only if $\bar{A}_i \not\equiv 0 \pmod p$.

Proof. Suppose $\mathfrak{P}$ is a prime ideal in E which ramifies in L/E. Then the ramification index of $\mathfrak{P}$ in L/E is p. Since L/E is tamely ramified $\mathfrak{P}$ is not a divisor of $\langle p\rangle$ and

$$v_{\mathfrak{P}}(d_{L/E}) = p-1. \tag{2}$$

Since $L = E(\beta)$ where $\beta^p = e^{u\theta}$, the proposition follows easily from (1), Lemma 8, the proof of Theorem 118 of [H], and (2).

3. Realizable classes. If l is an odd prime let $d(l) = (l-1)/2$. Then by Section 2 of [Lo] we have $C(E,k) = \mathfrak{c}^{d(q)}$ 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. If H is a multiplicative group and m is a positive integer, let H^m denote the subgroup of H consisting of mth powers of elements of H. In this section we will prove the following theorem.

THEOREM 10. $R_{\mathrm{t}}(E/k, \Sigma) = \mathfrak{c}^{pd(q)} W_{E/k}^{qd(p)}$.

As an immediate consequence we obtain

COROLLARY 11. *If* $C(E,k) = 1$ *then* $R_{\mathrm{t}}(E/k, \Sigma) = W_{E/k}^{qd(p)}$.

Theorem 10 follows from the following two propositions.

PROPOSITION 12. $R_{\mathrm{t}}(E/k, \Sigma) \subseteq \mathfrak{c}^{pd(q)} W_{E/k}^{qd(p)}$.

Proof. Let L/k be a G-extension with respect to E/k and Σ. By Proposition 9,

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

where $m \le n$, with n and the $\mathfrak{P}_i$ as indicated in the statement of Proposition 9 (the latter after a possible relabelling of subscripts). Now, by an argument similar to that which produced (6) of [C1], we obtain the stated result.

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 13. $R_{\mathrm{t}}(E/k, \Sigma) \supseteq \mathfrak{c}^{pd(q)} W_{E/k}^{qd(p)}$.

Proof. Let $\mathfrak{c}_1 \in W_{E/k}$ and choose an odd integer $v > 3$ such that $\mathfrak{c}_1^v = \mathfrak{c}_1$. As in the proof of Proposition 5 of [C1], choose positive integers b_i, $1 \le i \le v$, such that $(b_i, p) = 1$ for each i and $\sum_{i=1}^{v} b_i = pv$. Let $\mathfrak{m}$ be the modulus $\langle 1 - \zeta_p \rangle^{p^2}$ of k. By Lemma 4 of [C1], $\mathfrak{c}_1$ 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 ideal in $\mathfrak{c}_1$. Choose prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_v \in \mathfrak{c}_{\mathfrak{m}}$ such that

(i) each $\mathfrak{P}_i$ splits completely in E/k;
(ii) for each i, $\mathfrak{P}_i \cap k \in \mathfrak{c}_1$;
(iii) $i \ne j$ implies $\mathfrak{P}_i$ is not conjugate to $\mathfrak{P}_j$.

Let $\mathfrak{Q}$ be a prime ideal in $\mathfrak{c}_{\mathfrak{m}}^{-1}$. Then

$$\langle \varepsilon \rangle = \Big(\prod_{i=1}^{v} \mathfrak{P}_i^{b_i}\Big) \mathfrak{Q}^{pv}$$

where $\varepsilon \in E^{\times}$ and $\varepsilon \equiv 1 \pmod{\mathfrak{m}}$. Since $\mathfrak{m}$ is a modulus of k, it follows that $\varepsilon^{-u\theta} \equiv 1 \pmod{\mathfrak{m}}$. Let $b = \varepsilon^{-u\theta}$. It is easily verified that b is not a pth power in E. Let $L = E(\beta)$ where $\beta^p = b$. Then by Theorem 6, L/k is a Galois extension with $\mathrm{Gal}(L/k) \simeq G$. Furthermore, by Theorem 119 of [H], it follows that L/E is tamely ramified. Hence, L/k is a tamely ramified G-extension with respect to E/k and Σ.

We now show that $C(L,k)=\mathfrak{c}^{pd(q)}\mathfrak{c}_1^{qd(p)}$. By the proof of Lemma 7 we may replace the element ε with $\varepsilon_1=\varepsilon^{p-1}$. Then

$$\langle\varepsilon_1\rangle=\Big(\prod_{i=1}^{v}\mathfrak{P}_i^{c_i}\Big)\mathfrak{Q}^{p(p-1)v}$$

where $c_i=b_i(p-1)$. Therefore, by Proposition 9,

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

Now, computing $C(L,k)$ as in the proof of Proposition 12 gives the result.

REFERENCES

[C1] J. E. Carter, *Steinitz classes of a nonabelian extension of degree p^3*, Colloq. Math. 71 (1996), 297–303.

[C2] —, *Characterizations of Galois extensions of prime cubed degree*, Bull. Austral. Math. Soc. 55 (1997), 99–112.

[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.

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

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

Received 22 July 1997;
revised 23 February 1998