COLLOQUIUM MATHEMATICUM

VOL. 81 | 1999 | NO. 1

A GENERALIZATION OF A RESULT ON INTEGERS IN METACYCLIC EXTENSIONS

BY

JAMES E. CARTER (CHARLESTON, SC)

Abstract. Let p be an odd prime and let c be an integer such that $c>1$ and c divides $p-1$. Let G be a metacyclic group of order pc and let k be a field such that pc is prime to the characteristic of k. Assume that k contains a primitive pcth root of unity. We first characterize the normal extensions L/k with Galois group isomorphic to G when p and c satisfy a certain condition. Then we apply our characterization to the case in which k is an algebraic number field with ring of integers $\mathfrak{o}$, and, assuming some additional conditions on such extensions, study the ring of integers $\mathfrak{O}_L$ in L as a module over $\mathfrak{o}$.

0. Introduction. The present paper extends results obtained in [1]. Let p be an odd prime and let c be an integer such that $c > 1$, and c divides $p-1$. Let G be the metacyclic group of order pc given in terms of generators and relations by

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

where r is a primitive cth root of unity mod p. Let s be the unique integer in $\{2, \ldots, p-1\}$ such that $sr \equiv 1 \pmod{p}$. Then s is also a primitive cth root of unity mod p. Hence, $s^c = 1 + tp$ for some positive integer t, and we assume p and c are such that $t \not\equiv 0 \pmod{p}$. Furthermore, we have the following exact sequence of groups:

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

Now let k be an algebraic number field and assume k contains the multiplicative group μ_{pc} of pcth roots of unity. Fix, once and for all, a tamely ramified normal extension E/k with $\mathrm{Gal}(E/k) \simeq G/\langle \sigma \rangle$. Let $\mathfrak{O}_E$ and $\mathfrak{o}$ denote the rings of integers in E and k, respectively. 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 $\phi_L^{-1}(\langle \sigma \rangle)$. 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, the Steinitz class $C(L, k)$ of the extension L/k (see [2], p. 95, Theorem 13, for instance) varies over a subset

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

$R(E/k, \Sigma)$ 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 assume that l is an odd prime, and let n be any integer greater than 1. As in [3], define $d(2) = 1$, $d(l) = (l-1)/2$, and $d(n) = \text{g.c.d.}\{d(\pi) \mid \pi$ is a prime divisor of $n\}$. For $x \in C(k)$, H a subgroup of $C(k)$, and m a positive integer, let xH be the left coset of H in $C(k)$ which contains x, and let H^m denote the multiplicative group of mth powers of elements of H. In [1], Theorem 10, we showed that when $c = q$, an odd prime number, then

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

where $\mathfrak{c} = C(E, k)$ and $W_{E/k}$ is the subgroup of $C(k)$ generated by classes which contain at least one prime ideal that splits completely in E/k. Consequently, when $\mathfrak{O}_E$ is free as an $\mathfrak{o}$-module, $R_{\mathrm{t}}(E/k, \Sigma)$ is a subgroup of the class group of k ([1], Corollary 11).

A key arithmetic feature of the extensions $k \subseteq E \subseteq L$ which are considered in Theorem 10 of [1] is that the prime ideals in E which ramify in L/E, necessarily split completely in E/k ([1], Proposition 9). In the present paper we show that this is the case for any possible value of c (Proposition 3 below). This fact and a result of McCulloh in [3] enable us to generalize Theorem 10 and Corollary 11 of [1] to include all possible values of c (Theorem 6 and Corollary 7 below).

1. More metacyclic groups as Galois groups. Let p, c, G, s, and t be as described in the first paragraph of the previous section. Let k be an arbitrary field such that pc is prime to the characteristic of k, and $\mu_{pc} \subseteq k$. Now, beginning with the second paragraph of Section 1 of [1], if we replace "q" with "c" throughout that section, then it is straightforward to verify that we obtain a complete characterization of Galois extensions L/k with $\mathrm{Gal}(L/k) \simeq G$, provided such extensions of k exist.

2. Arithmetic considerations. We now assume that E/k is the extension of algebraic number fields as described in Section 0 above. In view of Section 1, we can replace "q" with "c" in the discussion in Section 2 of [1], up to, and including, Lemma 7 and its proof. We then obtain the following description of the principal ideal $\langle e\rangle$ in the present case:

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

where the $\mathfrak{P}_i$ are distinct prime ideals in E which split completely in E/k and satisfy $\mathfrak{P}_i \cap \mathfrak{o} \neq \mathfrak{P}_j \cap \mathfrak{o}$ whenever $i \neq j$; $\mathfrak{A}$ is an ideal in E which is divisible only by prime ideals in E which do not split completely in E/k; and the A_i are elements of $\mathbb{Z}\langle\varrho\rangle$ with nonnegative coefficients.

As in the paragraph following the description of $\langle e\rangle$ on p. 196 of [1], one shows in the present case that if $\mathfrak{L}$ is a prime factor of $\mathfrak{A}$ which either remains prime or totally ramifies in E/k, then $\mathfrak{L}^{u\theta}$ is a pth power in E, where $\theta = \sum_{i=0}^{c-1} s^{c-1-i}\varrho^i$, and c is any integer satisfying the stated conditions. In the case in which c is not prime, there may also be prime factors of $\mathfrak{A}$ which neither remain prime nor totally ramify in E/k. In that case we have

LEMMA 1. *If $\mathfrak{L}$ is a prime factor of $\mathfrak{A}$ which neither remains prime nor totally ramifies in E/k, then $\mathfrak{L}^{u\theta}$ is a pth power in E.*

Proof. Let g and h be integers such that $g, h > 1$, and $gh = c$. Let $\mathfrak{L}_1$ be a prime factor of $\mathfrak{A}$ such that $\mathfrak{l}\mathfrak{O}_E = (\prod_{i=1}^{g} \mathfrak{L}_i)^{e(\mathfrak{L}_1/l)}$, where $\mathfrak{l}$ is a prime ideal in $\mathfrak{o}$, $e(\mathfrak{L}_1/l)$ is the ramification index of $\mathfrak{L}_1$ over $\mathfrak{l}$, and $\mathfrak{L}_{j+1} = \varrho^j(\mathfrak{L}_1)$ for $j = 0, 1, \ldots, g-1$. If x is a real number, let $\lfloor x\rfloor$ denote the greatest integer less than or equal to x. Then $\lfloor (c-1)/g\rfloor = h-1$, and we have $\mathfrak{L}_1^{u\theta} = \prod_{i=1}^{g} \mathfrak{L}_i^{uA_i}$, where $A_i = \sum_{j=0}^{h-1} s^{c-i-gj}$ for $i = 1, \ldots, g$. Since $(\sum_{j=0}^{g-1} s^j)A_g = \sum_{j=0}^{c-1} s^j \equiv 0 \pmod p$, and s is a primitive cth root of unity mod p, it follows that $A_g \equiv 0 \pmod p$. Since $A_{g-j} = s^j A_g$ for $j = 1, \ldots, g-1$, we have $A_i \equiv 0 \pmod p$ for each $i = 1, \ldots, g$, which proves the lemma.

By Lemma 1 and the paragraph preceding it, we obtain, as in (1) of [1],

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

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

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

LEMMA 2. *Suppose $A = \sum_{j=0}^{c-1} a_j\varrho^j \in \mathbb{Z}\langle\varrho\rangle$. Then $A\theta \equiv \overline{A}\theta \pmod p$.*

Proof. In the proof of Lemma 8 of [1], replace "q" with "c" to obtain a proof of the present lemma.

We now have

PROPOSITION 3. *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 first paragraph of the present section, 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 $\overline{A}_i \not\equiv 0 \pmod p$.

Proof. In the proof of Proposition 9 of [1], replace "Lemma 8" of that paper with "Lemma 2" of the present paper to obtain a proof of the present proposition (of course, "(1)" which appears in the proof of Proposition 9 of [1] now refers to (1) of the present paper).

3. Realizable classes. We continue to assume that E/k is the extension of algebraic number fields of Section 2 above. Then, by [3], Theorem 1, we have $C(E,k) = \mathfrak{c}^{d(c)}$ for some $\mathfrak{c} \in C(k)$.

Proposition 4. $R_{\mathrm{t}}(E/k,\Sigma) \subseteq \mathfrak{c}^{pd(c)} W_{E/k}^{cd(p)}$.

Proof. In the proof of Proposition 12 of [1], replace "Proposition 9" of that paper with "Proposition 3" of the present paper to obtain a proof of the present proposition.

Proposition 5. $R_{\mathrm{t}}(E/k,\Sigma) \supseteq \mathfrak{c}^{pd(c)} W_{E/k}^{cd(p)}$.

Proof. In the last paragraph of the proof of Proposition 13 of [1], replace "q" with "c", "Proposition 9" of that paper with "Proposition 3" of the present paper, and "Proposition 12" of that paper with "Proposition 4" of the present paper. Then we have a proof of the present proposition.

From Propositions 4 and 5 above, we obtain

Theorem 6. $R_{\mathrm{t}}(E/k,\Sigma) = \mathfrak{c}^{pd(c)} W_{E/k}^{cd(p)}$.

As an immediate consequence we have

Corollary 7. *If* $C(E,k) = 1$ *then* $R_{\mathrm{t}}(E/k,\Sigma) = W_{E/k}^{cd(p)}$.

Acknowledgements. The author wishes to thank Professor Władysław Narkiewicz for his question regarding the results of [1], which led the author to consider generalizing those results.

REFERENCES

[1] J. E. Carter, *Module structure of integers in metacyclic extensions*, Colloq. Math. 76 (1998), 191–199.

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

[3] L. R. McCulloh, *Cyclic extensions without relative integral bases*, Proc. Amer. Math. Soc. 17 (1966), 1191–1194.

Department of Mathematics
College of Charleston
66 George Street
Charleston, SC 29424–0001, U.S.A.
E-mail: carterje@cofc.edu

Received 11 February 1999