PACIFIC JOURNAL OF MATHEMATICS
Vol. 105, No. 2, 1983

LIFTING GROUP HOMOMORPHISMS

RICHARD HARTLEY

If a knot K has Alexander polynomial different from 1, then its knot group, G maps onto some metacyclic group, $Z_r \tilde{\otimes} Z_p$. We show that in that case, it also has a homomorphism onto a split extension of a free abelian group of rank $p-1$ by $Z_r \tilde{\otimes} Z_p$, and hence also onto a split extension of a direct sum of $p-1$ cyclic groups of order s by the metacyclic group. In many cases, (such as if s is coprime with p), this group can be specified exactly. Otherwise there are a finite number of possibilities. A special case is Perko's result that a homomorphism of a knot group onto $S_3 = Z_2 \tilde{\otimes} Z_3$ lifts to $S_4 = Z_2 \tilde{\otimes} Z_3 \tilde{\otimes} (Z_2 \oplus Z_2)$.

As an application we obtain information about the derived series of G.

In a final section it is shown how to associate a rational polynomial invariant to every metacyclic representation.

1. Lifting metacyclic representations. Let p be a prime, r a divisor of $p-1$ and β a primitive rth root modulo p. Let $E = Z_r \tilde{\otimes} Z_p = \langle Y, S: Y^r = S^p = 1, Y^{-1}SY = S^\beta \rangle$. Up to isomorphism, the group is independent of β. Let G be the knot group of a knot, K, in the 3-sphere, S^3, and let ϕ be a homomorphism of G onto E which takes a meridian, m, of K to $Y^a S^b$. Then g.c.d. $(a, r) = 1$, since G is generated by conjugates of m. Setting $X = Y^a S^b$ and eliminating Y, we obtain a presentation

$$E = \langle X, S: X^r = S^p = 1, X^{-1}SX = S^\alpha \rangle,$$

where $\alpha = \beta^a$ and $m\phi = X$. We describe this situation by saying that ϕ *maps G onto $E(\alpha)$*, meaning that $(m\phi)^{-1}Sm\phi = S^\alpha$. The following condition is well known: **[6, 3]**

(1.1) *G maps onto $E(\alpha)$ if and only if p divides* $\Delta(\alpha)$ where Δ is the Alexander polynomial of K.

We assume throughout this paper that ϕ maps G onto $E(\alpha)$.

Let η be a primitive pth root of unity, and Q the rational numbers. Then $Q(\eta)$ can be given the structure of an E-module by

$$V^S = V.\eta \quad \textit{and} \quad V^X = V\sigma \tag{1.2}$$

for $V \in Q(\eta)$, where σ is the Galois automorphism of $Q(\eta)$ determined by $\eta\sigma = \eta^\alpha$. (Module action is denoted by writing the element of E as a superscript.)

Let $(E, Q(\eta))$ denote the corresponding split extension of $Q(\eta)$ by E. This is the set $\{(x, V)\colon x \in E, V \in Q(\eta)\}$ with multiplication given by $(x, U)\cdot(y, V) = (xy, U^y + V)$. Via the module action, E permutes the pth roots of unity, and in fact this affords a faithful transitive permutation representation, θ, of E on the set $\{0, 1, \ldots, p-1\}$ given by $i(x\theta) = j$ where $(\eta^i)^x = \eta^j$. Then $\phi\theta$ is a transitive permutation representation of G and there is a corresponding p-sheeted covering, $\tilde{M}$, of S^3 branched over K. This covered space is characterised as follows. Above the base point b in S^3 lie p points, $\tilde{b}_0, \tilde{b}_1, \ldots, \tilde{b}_{p-1}$. If x is an element of G, that is, a path in $S^3 - N(K)$, (where $N(K)$ is a regular neighbourhood of K), and if $\tilde{x}_i$ is the lifting of x to a path in $\tilde{M}$ starting at the point $\tilde{b}_i$, then the end point of $\tilde{x}_i$ is $\tilde{b}_{i(x\phi\theta)}$.

Now, suppose that u_2 is a rational 2-chain in $\tilde{M} - N(\tilde{K})$ with boundary in $\partial(\tilde{M} - N(\tilde{K}))$ and assume that for all i, $\tilde{b}_i$ does not lie in $|u_2|$. Define a map $\phi'\colon G \to (E, Q(\eta))$ by

$$\phi'\colon x \mapsto \left(x\phi, \sum_{i=0}^{p-1} \mathrm{Int}(u_2, \tilde{x}_i)\cdot\eta^{i(x\phi\theta)}\right) \tag{1.3}$$

where Int is the algebraic intersection number. Then, using the fact that $(xy)_i = \tilde{x}_i + \tilde{y}_{i(x\phi\theta)}$, one easily verifies that ϕ' is a homomorphism.

This gives a homomorphism of G onto a subgroup, H of $(E, Q(\eta))$ and there is an exact sequence $0 \to \mathfrak{J} \to H \to E \to 0$, where $\mathfrak{J}$ is a subgroup of $Q(\eta)$. Since H and E are finitely generated, so is $\mathfrak{J}$. Furthermore, $\mathfrak{J}$ inherits an E-module structure from $Q(\eta)$. In particular, $\mathfrak{J}$ is invariant under multiplication by η, so it is a fractional ideal of $Q(\eta)$. It is also invariant under the Galois automorphism, σ. Such an ideal will be called *symmetric*. Denote H by $(E, \mathfrak{J})$. I claim:

(1.4) *If ϕ is a homomorphism of G onto $E(\alpha)$, then ϕ lifts to a homomorphism of G onto an extension of $\mathfrak{J}$ by E, where $\mathfrak{J}$ is a non-zero symmetric fractional ideal of $Q(\eta)$.*

It will be shown later, in §2, that this extension splits.

To prove (1.4), it remains only to show that u_2 can be chosen in such a way that $\mathfrak{J}$ is non-zero. We examine the covering space in more detail. Let b, the base point in S^3, lie in $\partial N(K)$. If m is a meridian of K, then $m\phi\theta$ consists of $n = (p-1)/r$ cycles $\mathcal{C}_1, \ldots, \mathcal{C}_n$ of length r, and one cycle $\mathcal{C}_0 = (0)$ of length one. A longitude is sent to the identity, since it lies in the second derived subgroup of G. In the covering space, therefore, K is covered by a link, $\tilde{K}$, of $n+1$ components, $\tilde{K}_0$ of branching index one,

and $\tilde{K}_i$; $i = 1,\ldots,n$ of branching index r. Point $\tilde{b}_i$ lies in $\partial(\tilde{K}_j)$ if and only if $i \in \mathcal{C}_j$ [**4**, §3].

Let $\tilde{\mu}_i$ and $\tilde{\lambda}_i$ be the homology classes represented by meridian and longitude of $\tilde{K}_i$.

All homology groups referred to in the following are rational homology groups and as such, vector spaces over Q. Consider the homomorphism i_*: $H_1(\tilde{K}) \to H_1(\tilde{M})$ induced by inclusion. Its kernel contains the element $\gamma = \tilde{K}_0 + r\Sigma_{i=1}^n \tilde{K}_i$, as can be seen from "lifting" the relation $K \sim 0$ in $H_1(S^3)$ [**4**, Proposition 4.4]. If $\ker(i_*)$ contains an element $\beta = \Sigma_{i=0}^n b_i \tilde{K}_i$, then there exists a 2-chain, u_2, in $\tilde{M} - N(\tilde{K})$ with boundary $\Sigma_{i=0}^n b_i \tilde{\lambda}_i + a_i \tilde{\nu}_i$. This gives rise to a homomorphism ϕ': $G \to (E, Q(\eta))$. If $x = m^r$, then $\tilde{x}_0 = r\tilde{\mu}_0$ and $\tilde{x}_i = \tilde{\mu}_j$ if $i \in \mathcal{C}_j$ for $i \neq 0$, so it is easily seen that $m^r\phi' = (1, rb_0 + \Sigma_{i=1}^{p-1} b_i' \eta^i)$ where $b_i' = b_j$ if i is in the cycle $\mathcal{C}_j$. This is a non-zero element of $\mathcal{G}$ as long as β is chosen not to be a multiple of γ.

If this cannot be done, then $\ker(i_*)$ is generated by γ over Q, and by [**4**, Proposition 1.3], $\dim H_1(\tilde{M} - \tilde{K}) = \dim(H_1(\tilde{M})) + 1$. Since $H_1(\tilde{M})$ is obtained from $H_1(\tilde{M} - \tilde{K})$ by killing the meridians, it follows that the meridians of the $\tilde{K}_i$ generate a dimension one subspace of $H_1(\tilde{M} - \tilde{K})$. Thus, $\tilde{\mu}_0 \sim q\tilde{\mu}_1$ in $H_1(\tilde{M} - \tilde{K})$. Since $\tilde{\mu}_0$ covers m once, and $\tilde{\mu}_1$ covers m r times, we have $m \sim qrm$ in $H_1(S^3 - K)$, whence $q = 1/r$, since $m \nsim 0$. This shows $r\tilde{\mu}_0 - \tilde{\mu}_1 \sim 0$, and so there is a rational 2-chain, u_2, with this boundary. Since $\tilde{l}_i = \tilde{\lambda}_j$ for $i \in \mathcal{C}_j$, the corresponding homomorphism, ϕ', sends l to $(1, r - \eta - \eta^\alpha - \cdots - \eta^{\alpha^{r-1}})$ which is a non-zero element of $\mathcal{G}$. In all cases, therefore, u_2 can be chosen so that $\mathcal{G}$ is non-zero. □

Note that in the case where E is just the dihedral group, D_p, $(E, Q(\eta))$ can be embedded in the group of motions of the complex plane. Representations of G by motions of the complex plane have been studied by Burde [**1**, **2**] and his existence theorem for such representations is a special case of 1.4.

2. Structure of $(E, \mathcal{G})$. In order to understand the group $(E, \mathcal{G})$ better we have two goals: to prove that the extension splits and to enumerate the possible symmetric ideals of $Q(\eta)$, thus determining the structure of $\mathcal{G}$ as an E-module, and determining the group.

To prove that the extension splits, we show that $H^2(E, \mathcal{G}) = 0$ using the Lyndon-Hochschild-Serre spectral sequence [**12**, Theorem 11.45]. Given $0 \to Z_p \to E \to Z_r \to 0$, there is a spectral sequence $H^i(Z_r, H^j(Z_p, \mathcal{G})) \Rightarrow H^{i+j}(E, \mathcal{G})$. The action of the generator, S, of Z_p on $\mathcal{G}$ is multiplication by η. Thus,

$$\ker(S - 1) = 0 = \mathrm{Im}(1 + S + S^2 + \cdots + S^{p-1}).$$

It follows that $H^j(Z_p, \mathfrak{J}) = 0$ for $j = 0, 2$, and so $H^{2-j}(Z_r, H^j(Z_p, \mathfrak{J})) = 0$ for $j = 0, 2$. Now $p \cdot H^1(Z_p, \mathfrak{J}) = 0$, [**12**, Theorem 10.26] and so Z_r and $H^1(Z_p, \mathfrak{J})$ have coprime orders as groups. It follows that $H^1(Z_r, H^1(Z_p, \mathfrak{J})) = 0$ as well (see proof of [**12**, Theorem 10.27]) and so, $H^2(E, \mathfrak{J}) = 0$.

Our next task is to classify symmetric ideals of $Q(\eta)$ up to isomorphism as E-modules. The ring $Z[\eta]$ will be denoted by R, the fixed field of σ by L and its ring of integers by R_0. First remark:

(2.1) *If $\mathfrak{J}^*$ is any E-module of $Q(\eta)$ and $q \in L$, then $q\mathfrak{J}^*$ is E-isomorphic to $\mathfrak{J}^*$. The isomorphism is given by multiplication by q.*

In particular, we may assume that $\mathfrak{J}$ is an ideal of R.

LEMMA. *Let $\mathfrak{J}$ be a symmetric ideal in R. Then $\mathfrak{J} = (1 - \eta)^\varepsilon JR$, where $0 \leq \varepsilon < r$ and J is an ideal of R_0.*

Proof. The proof is based on the proof of Lemma 1.2 in [**7**]. Let $\mathfrak{J} = (1 - \eta)^\varepsilon \mathfrak{J}'$, where $\mathfrak{J}'$ is an integral ideal not divisible by $(1 - \eta)$. Let P be a prime factor of $\mathfrak{J}'$ and $P_0 = P \cap R_0$. Now P_0 does not ramify, since the only Z-prime to ramify is (p), and this factors into $(1 - \eta)^p$ in R. Furthermore, σ acts transitively on the prime factors of P_0R in R ([**11**], p. 163). Thus, for some i, $P_0R = P \cdot P\sigma \cdots P\sigma^i$, where the ideals on the right are all distinct and divide $\mathfrak{J}$, since $\mathfrak{J}$ is symmetric. By induction, therefore, $\mathfrak{J} = (1 - \eta)^\varepsilon JR$, with J an ideal of R_0. Finally, note that the ideal generated by $(1 - \eta)^r$ is generated by the element $\prod_{i=0}^{r-1}(1 - \eta)\sigma^i$ of R_0. □

The ideal $(1 - \eta)^\varepsilon JR$ depends only on ε and the ideal class of J in R_0, as can be seen from (2.1). There are, therefore, only a finite number of non-isomorphic $\mathfrak{J}$'s. In particular, when R_0 is a principal ideal domain, which is the case at least when $r = 2$ and $p \leq 47$ (and possibly when $p < 97$ [**8**]), it may be taken that $\mathfrak{J} = (1 - \eta)^\varepsilon R$.

3. Finite Quotients. We now turn our attention to finite quotients of $(E, \mathfrak{J})$. The group $(E, \mathfrak{J})$ has a homomorphism onto the split extension $(E, \mathfrak{J}/s\mathfrak{J})$, where s is any integer, and the structure of $\mathfrak{J}/s\mathfrak{J}$ as an E-module is inherited from $\mathfrak{J}$.

(3.1) LEMMA. *If $\mathfrak{J} = (1 - \eta)^\varepsilon JR$ with J an ideal of R_0, then $\mathfrak{J}/s\mathfrak{J}$ is E-isomorphic to $\mathfrak{J}'/s\mathfrak{J}'$ with $\mathfrak{J}' = (1 - \eta)^\varepsilon R$. If p does not divide s, then $\mathfrak{J}/s\mathfrak{J}$ is E-isomorphic to R/sR.*

Proof. Let Q_s be the ring $\{a/b \in Q;\ \text{g.c.d. } (b, s) = 1\}$ and let $\mathfrak{J}_s = Q_s\mathfrak{J}$. Then $\mathfrak{J}_s$ is a symmetric ideal of $R_s = RQ_s$, and there is an E-module isomorphism $\mathfrak{J}/s\mathfrak{J} \cong \mathfrak{J}_s/s\mathfrak{J}_s$ given by $a + s\mathfrak{J} \to a + s\mathfrak{J}_s$ for $a \in \mathfrak{J}$. Let $\mathfrak{J} = (1 - \eta)^\varepsilon JR$. Then $\mathfrak{J}_s = (1 - \eta)^\varepsilon JQ_sR_s$, and JQ_s is an ideal of R_0Q_s. Now, R_0 is a Dedekind domain, and unique factorisation of ideals in R_0 implies unique factorisation in R_0Q_s, so R_0Q_s is a Dedekind domain. If P_s is a prime ideal in R_0Q_s, then P_s divides PR_0 for some prime ideal, P of Q_s, namely, $P = P_s \cap Q_s$. However, Q_s has only finitely many prime ideals, and each PR_0 has only finitely many divisors in R_0Q_s. So, R_0Q_s has only finitely many prime ideals, and so it is a principal ideal domain [**11**, p. 112]. Therefore, for some $q \in R_0Q_s \subset L$, we have $\mathfrak{J}_s = (1 - \eta)^\varepsilon qR_s$ which is isomorphic to $\mathfrak{J}_s' = (1 - \eta)^\varepsilon R_s$ as an E-module by (2.1). Setting $\mathfrak{J}' = (1 - \eta)^\varepsilon R$, we have $\mathfrak{J}/s\mathfrak{J} \cong \mathfrak{J}_s/s\mathfrak{J}_s \cong \mathfrak{J}_s'/s\mathfrak{J}_s' \cong \mathfrak{J}'/s\mathfrak{J}'$.

Now, $(1 - \eta)$ divides p in R, and so in R_s. But, if g.c.d. $(s, p) = 1$, then p is a unit of R_s, and so, therefore, is $(1 - \eta)^\varepsilon$. Then $\mathfrak{J}_s' = R_s$, and we may taken $\mathfrak{J}' = R$. □

4. Restrictions on the value of ε. We have shown that if $\Delta(a) \equiv 0 \bmod p$ then G maps onto $(E, \mathfrak{J})$ where $\mathfrak{J} = (1 - \eta)^\varepsilon JR$ for some ε. We now investigate what values of ε may occur. Lemma 3.1 shows that G maps onto $(E, \mathfrak{J}'/p\mathfrak{J}')$ where $\mathfrak{J}' = (1 - \eta)^\varepsilon R$. As an abelian group, $\mathfrak{J}'$ has a basis $T_i = (1 - \eta)^\varepsilon\eta^i$; $i = 1, \ldots, p - 1$. The action of E is given by

$$T_i^S = (1 - \eta)^\varepsilon\eta^{i+1} = \sum_{j=1}^{p-1} a_{ij}(1 - \eta)^\varepsilon\eta^j = \sum_{j=1}^{p-1} a_{ij}T_j$$

$$T_i^X = (1 - \eta^\alpha)^\varepsilon\eta^{i\alpha} = (1 - \eta)^\varepsilon\cdot(1 + \eta + \cdots + \eta^{\alpha-1})^\varepsilon\eta^{i\alpha} = \sum_{j=1}^{p-1} b_{ij}T_j$$

for certain readily calculable a_{ij} and b_{ij}. A presentation for $(E, \mathfrak{J}'/p\mathfrak{J}')$ is

$$\left\langle X, S, T_i\colon X^r = S^p = T_i^p = 1,\ X^{-1}SX = S^\alpha,\ T_i \rightleftharpoons T_j,\ X^{-1}T_iX = \prod_{j=1}^{p-1} T_j^{b_{ij}},\ S^{-1}T_iS = \prod_{j=1}^{p-1} T_j^{a_{ij}} \right\rangle.$$

Now, setting all T_i equal to a single element, T, of order p, and noticing that $\Sigma_{j=1}^{p-1} a_{ij} \equiv 1 \bmod p$, and $\Sigma_{j=1}^{p-1} b_{ij} \equiv \alpha^\varepsilon \bmod p$, we see that G maps onto the group

$$\langle X, S, T\colon X^r = S^p = T^p = 1,\ S \rightleftharpoons T,\ X^{-1}SX = S^\alpha,\ X^{-1}TX = T^{\alpha^\varepsilon}\rangle$$

and a meridian is mapped to XT^ν. Suppose $\varepsilon \neq 0$ and so $\alpha^\varepsilon \not\equiv 1 \bmod p$. The above group is then a semi-direct product, $Z_r \textcircled{\times} (Z_p \oplus Z_p)$, and using

the notation of [3], $Z_p \oplus Z_p$ has structure $X_p(t-\alpha) \oplus X_p(t-\alpha^\varepsilon)$ as a Z_p-module.

Let A_r be the (integral) homology group of the r-fold cyclic branched covering space of K. Let $A_{r,p} = A_r/pA_r$. Then $A_{r,p}$ has the structure of a Z_p-module, and $X_p(t-\alpha) \oplus X_p(t-\alpha^\varepsilon)$ must be a quotient module of $A_{r,p}$. According to [3, §2, Case1, considerations (ii) and (iii)], the modulo p reduction of $\Delta(T)$, denoted $\Delta_p(t)$, must be divisible by $t-\alpha$ and $t-\alpha^\varepsilon$ over Z_p, and if $\alpha = \alpha^\varepsilon$, then $(t-\alpha)^2$ divides $\Delta_p(t)$ over Z_p.

If $r = 2$ and $A_{2,p} \cong Z_p$ as an abelian group, then $A_{2,p}$ clearly cannot map onto $Z_p \oplus Z_p$, so we must conclude that $\varepsilon = 0$. (This is exactly the case when G has a single representation onto the dihedral group, D_p.) If $r > 2$, however, metacyclic representations occur in pairs, and G maps onto $E(\alpha)$ if and only if it maps onto $E(\beta)$ where $\alpha\beta \equiv 1 \bmod p$ [3, Proposition 1.6]. If then $A_{r,p} \cong Z_p \oplus Z_p$ as an abelian group, then as a module, $A_{r,p} = X_p(t-\alpha) \oplus X_p(t-\beta)$ with $\alpha\beta \equiv 1 \bmod p$. This means that $\beta = \alpha^\varepsilon$, and so, $\varepsilon = r-1$.

We now collect our conclusions.

(4.1)THEOREM. *Let ϕ be a homomorphism of G onto $E(\alpha) \cong Z_r \tilde{\otimes} Z_p$. Then there is an integer ε: $0 \le \varepsilon < r$ such that*

(i) *ϕ lifts to a homomorphism of G onto $(e, \mathfrak{J})$ where $\mathfrak{J}$ is the ideal $(1-\eta)^\varepsilon JR$ of $R = Z[\eta]$, and J is an ideal of R_0.*

(ii) *If $r = 2$ and $p \le 47$, then $\mathfrak{J}$ can be taken as $(1-\eta)^\varepsilon R$.*

(iii) *For any integer, s, ϕ lifts to a homomorphism of G onto $(E, \mathfrak{J}/s\mathfrak{J})$ where $\mathfrak{J} = (1-\eta)^\varepsilon R$. If g.c.d. $(s, p) = 1$, then we can take $\mathfrak{J} = R$.*

The notation $(E, -)$ denotes a split extension, and the action of E on R is given by (1.2).

The following restrictions on the value of ε apply:

(iv) *If $\varepsilon \neq 0$ then $\Delta(\alpha^\varepsilon) \equiv 0 \bmod p$.*

(v) *If $\varepsilon = 1$ then $(t-\alpha)^2$ divides $\Delta_p(t)$ over Z_p.*

(vi) *If $r = 2$ and $A_{r,p} \cong Z_p$, then $\varepsilon = 0$.*

(vii) *If $r > 2$ and $A_{r,p} = Z_p \oplus Z_p$, then $\varepsilon = 0$ or $r-1$.* □

Thus, any cycle of $\tilde{M} - N(\tilde{K})^0$ relative to its boundary gives rise to a homomorphism ϕ': $G \to (E, Q(\eta))$ which is a lifting of ϕ. It can be shown that every such ϕ' arises in this way. Namely, if ϕ' is a homomorphism from G into $(E, Q(\eta))$ which is a lifting of a homomorphism ϕ: $G \to E$, then there exists a rational 2-chain u_2 with boundary in $\partial(\tilde{M} - N(\tilde{K})^0)$ such that ϕ' is given by (1.3). The proof is not difficult, and is omitted.

The hypothesis of the theorem is true exactly when p divides $\Delta(\alpha)$. But Δ is a knot invariant which depends only on G/G''. It seems remarkable, then, that a metabelian invariant, Δ, can provide a necessary and sufficient condition for the existence of certain non-metabelian quotients of the knot group.

5. Applications. As an abelian group, $\mathfrak{J}$ is free of rank $p-1$. Therefore, $(E, \mathfrak{J})$ is a semi-direct product $Z_r \tilde{\wedge} Z_p \tilde{\wedge} (Z \oplus \cdots \oplus Z)$ and $(E, \mathfrak{J}/s\mathfrak{J})$ is $Z_r \tilde{\wedge} Z_p \tilde{\wedge} (Z_s \oplus \cdots \oplus Z_s)$ where there are $p-1$ copies of Z (respectively Z_s) in the direct sums. The special case $r=2$, $p=3$, $s=2$ gives $Z_2 \tilde{\wedge} Z_3 \tilde{\wedge} (Z_2 \oplus Z_2) \cong S_4$. According to (4.1), then, a knot group, G, maps onto S_4 if and only if it maps onto $S_3 \cong Z_2 \tilde{\wedge} Z_3$. (See also [9].)

We can use (4.1) to obtain information about the third derived quotient of G.

(5.1) *If G is a knot group for which $\Delta(t) \neq 1$, then G''/G''' has infinite rank.*

Of course, if $\Delta(t) = 1$, then $G'' = G'$, and so $G''' = G''$. Thus, the derived series either stops with $G' = G''$, or else $G > G' > G'' > G'''$ with all inclusions proper.

Proof of (5.1). Calculate the derived subgroup of $H = (E, \mathfrak{J})$. It is generated by S and an ideal $\mathfrak{J}'$ with $(1-\eta)\mathfrak{J} \subset \mathfrak{J}' \subset \mathfrak{J}$. Then H'' is $(1-\eta)\mathfrak{J}'$ and $H''' = 0$. Thus, $H''/H''' = (1-\eta)\mathfrak{J}'$ which is free abelian of rank $p-1$. Now G maps onto $(E, \mathfrak{J})$, with $E = Z_r \tilde{\wedge} Z_p$ for some r, if and only if p divides $\Delta(\alpha)$ for some α. For any polynomial Δ of degree at least one, there are an infinite number of primes occurring as divisors of $\Delta(\alpha)$ as α runs over all integers. For if $\Delta(t) = a_0 + a_1 t + \cdots + a_n t^n$ and q is any sufficiently large integer, then $\Delta(a_0^2 q)$ is divisible by a prime not occuring in $a_0 q$. Thus, for arbitrarily large p, G maps onto some $(Z_r \tilde{\wedge} Z_p, \mathfrak{J})$, and G''/G''' maps onto a free abelian group of rank $p-1$. So G''/G''' does not have finite rank. □

6. An invariant. In [1] and [2], G. Burde derived an invariant of ϕ: $G \to E$ in the case where E is dihedral from the value of $l\phi'$ in a properly normalised lifting of ϕ. This can be generalised to the case considered here. Metacyclic representations have an important property not possessed by dihedral representations, namely, the associated invariants are the only known generally applicable invariants which may be used to prove that a knot is non-invertible. In fact metacyclic invariants are sufficient to determine all non-invertible knots with 10 crossings or less.

(Details of this are to be found in my paper "Identifying Non-invertible Knots" [5].) For this reason, I feel that it is worthwhile giving the appropriate generalisation of Burde's invariant here.

Given $m\phi' = (X, U_m)$, let $\overline{U}_m = 1/r \cdot (U_m + U_m\sigma + \cdots + U_m\sigma^{r-1})$. Let $l\phi' = (\mathrm{id}, U_l)$. The case where $U_l = \overline{U}_m = 0$ is somewhat troublesome, and we exclude it from consideration, though it certainly occurs. Otherwise, we may consider the ratio $U_l/\overline{U}_m$ in $Q(\eta) \cup \{\infty\}$.

(6.1) THEOREM. *Let ϕ: $G \to E$ be a homomorphism and let $\tilde{M}$ be the covering space corresponding to ϕ. There exists a lifting ϕ': $G \to (E, Q(\eta))$ of ϕ for which not both $\overline{U}_m$ and U_l are zero.*

(i) *The value of $U_l/\overline{U}_m$ depends only on G and ϕ, and not on the particular ϕ' chosen.*

(ii) *$U_l/\overline{U}_m \neq \infty$ if and only if all linking numbers are defined in $\tilde{M}$.*

(iii) *If $U_l/\overline{U}_m \neq \infty$ and $U_l/\overline{U}_m$ is written as $\sum_{i=1}^{p} a_i\eta^i$ with $\sum_{i=1}^{p} a_i = 0$, then $a_i = \mathrm{link}(\tilde{K}_0, \tilde{K}_j)$ where $i \in \mathcal{C}_j$* (notation as in §1). □

Proof. According to the proof of (1.4), there always exists ϕ' with $\overline{U}_m \neq 0$ or $U_l \neq 0$. We prove (iii) first. As a first step, one can normalise ϕ' as follows. Consider the map $1 + \sigma + \sigma^2 + \cdots + \sigma^{r-1}$ acting on $Q(\eta)$. Now, $U_m - \overline{U}_m$ is in its kernel, and so as is easily verified, there exists V in $Q(\eta)$ such that $V(1 - \sigma) = U_m - \overline{U}_m$. Now composing ϕ' with conjugation in $(E, Q(\eta))$ by (id, V) we obtain a new homomorphism—call it ϕ' also—such that $m\phi' = (X, \overline{U}_m)$. If $\overline{U}_m \neq 0$, then we can further compose ϕ' with the map $(E, Q(\eta)) \to (E, Q(\eta))$ given by $(x, W) \to (x, W\overline{U}_m^{-1})$, which is a homomorphism since $\overline{U}_m \in L =$ fixed field of σ. This gives a new normalised ϕ' such that $m\phi' = (X, 1)$. Neither of these normalisation steps affects the ratio $U_l/\overline{U}_m$. The proof of (iii) is now a direct generalisation of Theorem 6.3 of [4], and can be adapted almost word for word. Hence, it is omitted.

To prove (i) it remains in view of (iii) just to show that the cases $\overline{U}_m = 0$ and $\overline{U}_m \neq 0$ cannot both occur for the same ϕ (but different ϕ'). Suppose, then, that there exist homomorphisms ϕ': $x \to (x\phi, U_x)$ and ϕ'': $x \to (x\phi, V_x)$, where $\overline{U}_m \neq 0$, $\overline{V}_m = 0$, $V_l \neq 0$. One can define a third homomorphism $x \to (x\phi, U_x + V_x)$. Setting $W_x = U_x + V_x$, we see that $W_l/\overline{W}_m \neq \infty$, but $W_l/\overline{W}_m \neq U_l/\overline{U}_m$ in defiance of (iii).

Finally, if $\overline{U}_m \neq 0$ then by (iii) all linking numbers exist. Conversely, if all linking numbers exist, then (by definition) for all i, $\tilde{K}_i \sim 0$ in $H_1(M; Q)$. By the proof of (1.4), then, there exists a ϕ' such that $\overline{U}_m \neq 0$. This proves (ii). □

$U_l/\overline{U}_m$ is not entirely satisfactory as an invariant of (G, ϕ) as it stands, since different, but equivalent choices of ϕ give rise to different values. In particular, for each k, there is an automorphism γ_k of E taking S to S^k and fixing X. If ϕ is a homomorphism from G to $E(\alpha)$ then so is $\phi\gamma_k$, and $\phi\gamma_k$ is equivalent to ϕ in the usual sense of differing by an automorphism of E. However, the values of $U_l/\overline{U}_m$ for these two maps differ by the Galois automorphism γ_k^* of $Q(\eta)$ taking η to η^k. Thus, in order to obtain an invariant of the equivalence class of ϕ, one must consider the set of values $\{(U_l/\overline{U}_m)\gamma_k^*\colon k = 1,\ldots,p\}$. This is a somewhat cumbersome object. Given $U_l/\overline{U}_m = \sum_{i=1}^{p} a_i\eta^i$, one can define some lexicographical ordering and obtain a "least" element of this set to serve as a "normal form" for $U_l/\overline{U}_m$. I would like to suggest a different approach which is, I believe, more natural, and more clearly shows up symmetry properties of the knot.

DEFINITION. *Given a homomophism ϕ of G onto $E(\alpha)$, define $\Lambda_\phi(t)$ to be* $\operatorname{char}_{L/Q}(U_l/\overline{U}_m)$, *the characteristic polynomial of $U_l/\overline{U}_m$ with respect to the fixed field, L, of σ, where $U_l/\overline{U}_m$ is defined with respect to any ϕ': $G \to (E, Q(\eta))$ lifting ϕ such that not both U_l and $\overline{U}_m$ are zero. If $U_l/\overline{U}_m = \infty$, define $\Lambda_\phi(t) = 0$.*

$\Lambda_\phi(t)$ is a polynomial of degree $(p-1)/r$ with rational coefficients. Since the characteristic polynomial is invariant under Galois automorphisms, $\Lambda_\phi(t)$ depends only on the equivalence class of ϕ. Let K be a knot and K^* its mirror image. If ϕ is a representation of the knot group, G, of K, then there is a "mirror-image" representation ϕ^* of G^*, and it is easily verified that $\Lambda_{\phi^*}(t) = \Lambda_\phi(-t)$. Thus, as expected, $\Lambda_\phi(t)$ is useful in determining whether a knot is amphicheiral.

Given $\Lambda_\phi(t)$ one can regain $U_l/\overline{U}_m$ as one of its roots, and this in turn determines the values of link $(\tilde{K}_0, \tilde{K}_j)$ according to (6.1). However, all values of link $(\tilde{K}_i, \tilde{K}_j)$ can be determined from the values of link $(\tilde{K}_0, \tilde{K}_i)$. (Perko [**10**] gave a formula for the case $r = 2$, and a similar formula holds for $r > 2$). Thus, complete information about the covering linkage invariants associated with ϕ is contained in the polynomial $\Lambda_\phi(t)$. The advantage of this invariant over the set of linking numbers is that it is unnecessary to take into account the effect of a different renumbering of the components of the covering link. The disadvantage is that sometimes the coefficients of $\Lambda_\phi(t)$ become very large.

Acknowledgement. I wish to thank Professor G. Burde and Dr. J. R. J. Groves for useful conversations in connection with this paper.

REFERENCES

1. G. Burde, *Darstellungen von Knotengruppen*, Math. Annalen, **173** (1967), 24–33.
2. _____, *Darstellungen von Knotengruppen und eine Knoteninvariante*, Hamburger Abhandlungen, **35** (1970), 107–120.
3. R. Hartley, *Metabelian representations of knot groups*, Pacific J. Math., **82** (1979), 93–104.
4. R. Hartley and K. Murasugi, *Covering linkage invariants*, Canad. J. Math., **29** (1977), 1312–1339.
5. R. Hartley, *Identifying non-invertible knots*, to appear in Topology.
6. R. Fox, *Metacyclic invariants of knots and links*, Canad. J. Math., **22** (1970), 193–201.
7. M. P. Lee, *Integral representations of dihedral groups of order* $2p$, Trans. Amer. Math. Soc., **110** (1964), 213–231.
8. J. Milnor, *Introduction to algebraic K-theory*, Annals of Math. Studies No. 72, Princeton (1971).
9. K. Perko, *Octahedral Knot Covers*, pp. 47–50 in Knots, Groups and 3-manifolds (ed. Neuwirth, L. P.). Annals of Math. Studies No. 84, Princeton (1975).
10. _____, *On dihedral covering spaces of knots*, Inventiones Math., **34** (1976), 77–82.
11. P. Ribenboim, *Algebraic Numbers*, Pure and Applied Math., Vol. 27, Wiley-Interscience (1972).
12. J. J. Rotman, *An Introduction to Homological Algebra*, Academic Press (1979).

Received November 24, 1980.

UNIVERSITY OF MELBOURNE
PARKVILLE 3052
VICTORIA, AUSTRALIA

Current address: Department of Mathematics
University of Missouri
St. Louis, MO 63121