PACIFIC JOURNAL OF MATHEMATICS
Vol. 52, No. 2, 1974

ON THE DIVISIBILITY OF KNOT GROUPS

KUNIO MURASUGI

Some conditions for the knot group to be an R-group, i.e., the group in which the extraction of roots is unique, will be discussed in this paper. In particular, the group of a product knot is an R-group iff the knot group of each component is an R-group. For a fibred knot, a sufficient condition for its group to be an R-group will be given.

A group G is called an *R-group* if for every pair of elements x and y, and every natural number n, it follows from $x^n = y^n$ that $x = y$. In other words, G is an R-group if G has not more than one solution for every equation $x^n = a$. If G is an R-group, G is locally infinite. The converse, however, need not be true even if G is restricted to the group of a knot in S^3. For example, let G be the group of $K(m, n)$, the torus knot of type (m, n). G has a presentation $G = (a, b: a^m = b^n)$. Then the equation $x^m = a^m$ has infinitely many distinct solutions, $x = a, (ba)a(ba)^{-1}, (ba)^2a(ba)^{-2}, \cdots$.

This observation gives immediately a negative answer to Problem N in [3]. Neuwirth asks if a knot group can be ordered. In fact, the group of $K(m, n)(|m|, |n| \geqq 2)$ cannot be ordered, since an ordered group is always an R-group. Therefore, Problem N now leads slightly weaker problems: Can a knot group other than torus knot groups be ordered? Or, is a knot group other than torus knot groups an R-group?

The purpose of this paper is to give a sufficient condition for the group of a fibred knot to be an R-group. (See Theorem 2.) Using this condition, we can prove, for example, that the group of the figure eight knot is an R-group. (See Proposition 3 or Proposition 5.)

1. Statement of main results.

To make our statement precise, we will introduce some concepts relevant to an R-group.

DEFINITION 1. Let $n > 1$ be an integer. A group G is said to be n-divisible if for any pair of elements x and y in G it follows from $x^n = y^n$ that $x = y$.

Therefore, a group G is an R-group if G is n-divisible for every n. However, n may be restricted to a prime number. In fact, we have the following easy

PROPOSITION 1. *G is mn-divisible iff G is m- and n-divisible.*

Proposition 1 implies

PROPOSITION 2. *A group G is an R-group iff G is p-divisible for every prime p.*

The group of $K(m, n)$ is neither m-divisible nor n-divisible. However, it will be shown in § 4 that it is p-divisible iff $(n, p) = (m, p) = 1$, (see Theorem 3).

Now the following theorem shows that we need only consider the groups of prime knots.

THEOREM 1. *Let K be the product knot of two knots K_1 and K_2. Let G, G_1, and G_2 denote the groups of knots K, K_1, and K_2, respectively. Then G is an R-group iff G_1 and G_2 are R-groups.*

The proof will be given in § 2.

Finally, the main theorem of this paper is stated as follows.

THEOREM 2. *Let K be a nontrivial fibred (or Neuwirth) knot. Suppose that the Alexander polynomial $\Delta(t)$ of K has no repeated roots and let $\alpha_1, \cdots, \alpha_m$ be all the roots of $\Delta(t)$. If the group of K is not p-divisible, p a prime, then the multiplicative subgroup generated by $\alpha_1, \cdots, \alpha_m$ in the complex number field contains a nontrivial* pth *root of unity.*

The proof will be given in § 3.

2. *Proof of Theorem* 1. Since a subgroup of an R-group is an R-group, "only if" part of Theorem 1 is trivial.

To prove "if" part, we will show a slightly stronger theorem below.

Let $G = G_1 \overset{*}{_H} G_2$ denote the free product of two groups G_1 and G_2 with an amalgamated subgroup H.

Let $\mathfrak{S}_i$ $(i = 1, 2)$ be the system of right coset representatives for G_i modulo H. Then any element x of G has a unique normal form: $x = hx_1 \cdots x_k$, where $h \in H$, each $x_i (\notin H)$ belongs to only one system $\mathfrak{S}_1$ or $\mathfrak{S}_2$ and no two successive elements x_i and x_{i+1} $(i = 1, \cdots, k-1)$ belong to the same system. k is the length of x, denoted by $l(x)$. h will be called the *initial* factor of x, and is denoted by $i(x)$. If $x \in H$, or if $l(x) \geqq 1$ and if x_k and x_1 belong to different systems, x is said to be cyclically reduced.

THEOREM 1A. $G = G_1 \overset{*}{_H} G_2$ *is an R-group if the following condition* (1)–(3) *are satisfied:*

(2.1) (1) *G_1 and G_2 are R-groups,*

(2) *H is an isolated subgroup of G_1 and G_2. In other words, if $l(x) \leqq 1$ and $l(x^n) = 0$ for some natural number n, then $l(x) = 0$.*

(3) *$x^n = y^n$ for some natural number n yields $i(x) = i(y)$.*

Theorem 1A implies immediately

COROLLARY. *$G = G_1 * G_2$ is an R-group iff G_1 and G_2 are groups.*

The proof of Theorem 1A will follow from Lemmas 1–6 below.

LEMMA 1. *Let y be a noncyclically reduced element of $G = G_1 \overset{*}{_H} G_2$ and $y \notin H$. Then y can be written as*

$$y = u^{-1} y_0 u ,$$

where

(2.2) (1) *y_0 is a cyclically reduced element of G. Let $y_0 = hz_1 \cdots z_k$, $h \in H$, be the normal form of y_0. Then $l(y_0) = k \geqq 1$.*

(2) *u has the normal form, $u = \tilde{h} u_1 \cdots u_\lambda$, where $\tilde{h} \in H$, $\lambda = l(u) \geqq 1$, and $u_i \in \mathfrak{G}_1$ or $\mathfrak{G}_2$.*

(3) (i) *If $k \geqq 2$, then k is even, and z_k and u_1 are not in the same system, and $u_1^{-1} \tilde{h}^{-1} h z_1 \notin H$. Therefore, $l(y) = k + 2\lambda - 1$.*

(ii) *If $k = 1$, then z_1 and u_1 are not in the same system and $l(y) = 2\lambda + 1$.*

Since the proof is straightforward, it will be omitted, or see [2, § 4.2]. Denote $k = \tilde{l}(y)$.

In the following lemmas, we assume that the group $G = G_1 \overset{*}{_H} G_2$ satisfies (2.1) (1)–(3).

LEMMA 2. *Let y be a noncyclically reduced element of $G = G_1 \overset{*}{_H} G_2$ and $y \notin H$. Then for any positive integer n, $l(y^n)$ is given as follows:*

(2.3) (1) *If $\tilde{l}(y) = k \geqq 2$ and $l(u) = \lambda (\geqq 1)$, then $l(y^n) = nk + 2\lambda - 1 \geqq 2$.*

(2) *If $\tilde{l}(y) = 1$, then $l(y^n) = 2\lambda + 1 \geqq 3$.*

Proof. (1) is obvious.

To prove (2), let $y = u^{-1} y_0 u$ be the form obtained in Lemma 1. Since $\tilde{l}(y) = 1$, we see that $y_0 = hz$, $z \in G_1 - H$ or $G_2 - H$. Since z and u_1 are not in the same factor, it follows that

$$l(y^n) = l(u^{-1}(hz)^n u) \leqq 2\lambda + 1 . \tag{2.4}$$

An inequality in (2.4) holds only when $(hz)^n$ and u_1 belong to the same factor, i.e., $(hz)^n \in H$. Then by (2.1) (2) $hz \in H$, and hence, $z \in H$. This is a contradiction. Therefore, $l(y^n) = 2\lambda + 1$.

LEMMA 3. *Let x and y be cyclically reduced elements of G. If $x^n = y^n$, then $l(x) = l(y)$.*

Proof. First we note that for any cyclically reduced element z

$$l(z^n) \leqq 1 \quad \text{iff} \quad l(z) \leqq 1 . \tag{2.5}$$

Now the proof will be divided into the following three cases.

Case 1. $l(x) \geqq 2$.

Then $l(x^n) = nl(x) \geqq 2$. Since $x^n = y^n$, $l(y^n) = l(x^n) = nl(x) \geqq 2$ and hence $l(y) \geqq 2$. Therefore, $l(y^n) = nl(y)$. Now, the conclusion of Lemma 3 is immediate.

Case 2. $l(x) = 1$.

Then $l(x^n) = 1$, and hence, $l(y^n) = 1$, since $x^n = y^n$. Therefore, it follows from (2.5) that $l(y) \leqq 1$. $l(y)$ cannot be 0, otherwise $l(y^n)$ would be 0. Therefore, $l(y) = 1 = l(x)$.

Case 3. $l(x) = 0$.

Then $l(x^n) = 0$ and hence $l(y^n) = 0$. Then it follows from (2.1) (2) that $l(y) = 0$.

LEMMA 4. *Let x and y be cyclically reduced elements of G. Then $x^n = y^n$ yields $x = y$.*

Proof. By Lemma 3, we know that $l(x) = l(y)$. Let $x = hx_1 \cdots x_k$ and $y = gy_1 \cdots y_k$ be the normal forms of x and y.

Case 1. $l(x) = k \geqq 2$.

The normal forms of x^n and y^n can be written as

$$x^n = h'x_1^{(n-1)}x_2^{(n-1)} \cdots x_k^{(n-1)} \cdots x_1'x_2' \cdots x_k'x_1 \cdots x_k$$

and

$$y^n = g'y_1^{(n-1)}y_2^{(n-1)} \cdots y_k^{(n-1)} \cdots y_1'y_2' \cdots y_k'y_1 \cdots y_k .$$

Since $x^n = y^n$, we obtain that $x_1 = y_1, \cdots, x_k = y_k$. Moreover, it follows from (2.1) (3) that $i(x) = h = i(y) = g$. Therefore, $x = hx_1 \cdots x_k = gy_1 \cdots y_k = y$.

Case 2. $l(x) = k = 1$.

Then $x = hx_1$ and $y = gy_1$. Suppose that x_1 and y_1 are not in the same *system*. Then $x^n = (hx_1)^n = (gy_1)^n = y^n$ must belong to $H = G_1 \cap G_2$, and hence, x belongs to H by (2.1) (2). It contradicts our assumption. Therefore, x_1 and y_1 belong to the same system. Since G_1 and G_2 are R-groups, $x = y$ follows.

Case 3. $l(x) = l(y) = 0$.
Then $x = y$, since H is an R-group as a subgroup of G_i.

LEMMA 5. *Let x and y be elements of G. Suppose that only one of x and y, x say, is cyclically reduced, but y is not, and hence $y \notin H$. Then $x^n \neq y^n$.*

Proof. Case 1. $l(x) \geqq 2$.

It follows from Lemma 2 that $l(x^n) \equiv 0 \pmod 2$, while $l(y^n) \equiv 1 \pmod 2$. Therefore, $x^n \neq y^n$.

Case 2. $l(x) = 1$.

Since x belongs to one factor, we see that $l(x^n) = 1$. On the other hand, $l(y^n) \geqq 2$ by Lemma 2. Therefore, $x^n \neq y^n$.

Case 3. $l(x) = 0$. Suppose $x^n = y^n$.

Then x^n belongs to H and so does y^n. Therefore, y belongs to H by (2.1) (2). It contradicts our assumption.

LEMMA 6. *Suppose that neither x nor y is cyclically reduced. Then $x^n = y^n$ yields $x = y$.*

Proof. By Lemma 1, we can write

$$x = u^{-1}x_0u \quad \text{and} \quad y = v^{-1}y_0v ,$$

where x_0 and y_0 are cyclically reduced. Then $x^n = y^n$ yields $u^{-1}x_0^nu = v^{-1}y_0^nv$ and hence,

$$x_0^n = uv^{-1}y_0^nvu^{-1} = (uv^{-1}y_0vu^{-1})^n .$$

Since x_0 is cyclically reduced, it follows from Lemmas 4 and 5 that $x_0 = uv^{-1}y_0vu^{-1}$. It implies that $x = y$.

Theorem 1A follows immediately from these lemmas.

Now what it remains to show is that the group of the product knot $K_1 \# K_2$ satisfies (2.1) (1)–(3).

Let $G_i = G(K_i)$ be the knot group of K_i. Then it is well known that $G = G_1 \ast_H G_2$, where $G = G(K_1 \# K_2)$ and H is the infinite cyclic group generated by t that is represented by a meridian. Denote P' the commutator subgroup of a group P.

Now (2.1) (1) is exactly the assumption of Theorem 1.

To prove (2.1) (2), take an element x from G_1, say. x is written as $x = t^k x_1$, where $x_1 \in G_1'$. Then $x^n = t^{kn} x_1'$ for some $x_1' \in G_1'$. Therefore $x^n = t^{kn} x_1' = t^m$, for some m, yields $kn = m$, and hence, $t^{kn} x_1' = t^{kn}$. Since G_1 is an R-group, it follows that $(t^k x_1)^n = (t^k)^n$ yields $t^k x_1 = t^k$. Therefore, $x_1 = 1$, and hence, $x \in H$.

To prove (2.1) (3), let $x = t^q x_1 \cdots x_k$ and $y = t^r y_1 \cdots y_l$ be the normal forms of x and y. Then $x^n = t^{qn} g$ and $y^n = t^{rn} h$ for some $g, h \in G'$. Thus $x^n = y^n$ implies that $t^{qn} = t^{rn}$ in G/G', and hence, $q = r$. This proves (2.1) (3).

3. *Proof of Theorem* 2. Let K be a fibred knot in S^3. Then the knot group G of K is a semi-direct product of Z and F, where Z is an infinite cyclic group generated by t and F is a free group freely generated by r elements $x_1, \cdots, x_r$. The action of Z on F is given by an automorphism ϕ of F:

$$\phi: x_i \longrightarrow t x_i t^{-1} = W_i , \qquad i = 1, \cdots, r .$$

Let $\{F_n\}$ be the lower central series of F, where $F = F_1$ and $F_n = [F, F_{n-1}]$. Then ϕ induces an automorphism $\phi_n: F_n \to F_n$ for each n, since F_n is a characteristic subgroup of F. Using ϕ_n, we can construct a semi-direct product $G_n(K)$ of Z and F_n, where the action of Z on F_n is given by ϕ_n.

Now we know that F_n/F_{n+1} is a free abelian group of finite rank and ϕ_n induces an automorphism $\hat{\phi}_n$ of F_n/F_{n+1}. Let $\Delta_n(t)$ be the characteristic polynomial of the integer matrix M_n associated with $\hat{\phi}_n$. We should note here that the Alexander polynomial $\Delta_K(t)$ of K is just $\Delta_1(t)$ defined above.

First we want to know the characteristic roots of $\hat{\phi}_n$.

To do this, we use a technique given in [2, § 5.7].

Let $A_0(Z, r)$ be the graded associative Z-algebra freely generated by r elements $y_1, y_2, \cdots, y_r$. We define the bracket product in $A_0(Z, r)$ by $[u, v] = uv - vu$. Then there exists a free Lie algebra $\Lambda_0(Z, r)$ freely generated by $\xi_1, \cdots, \xi_r$ that is imbedded in $A_0(Z, r)$ equipped with the bracket product [2, Lemma 5.5]. Let Λ_n be the submodule consisting of all homogeneous elements of degree n in $\Lambda_0(Z, r)$. Then F_n/F_{n+1} is isomorphic to Λ_n, as an abelian group, under a natural mapping [2, Theorem 5.12]. Therefore, the automorphism $\hat{\phi}_n$ of F_n/F_{n+1} induces an automorphism $\tilde{\phi}_n$ of Λ_n.

Let C denote the complex number field. For $u_1, \cdots, u_k \in C - \{0\}$, we denote by $\langle u_1, \cdots, u_k \rangle$ the multiplicative subgroup in $C - \{0\}$ generated by $u_1, \cdots, u_k$.

LEMMA 7. *Suppose that $\Delta_K(t)$ has no repeated roots, and let $\alpha_1, \cdots, \alpha_r$ be all the roots of $\Delta_K(t)$. Let $\beta_1, \cdots, \beta_s$ be all the roots of $\Delta_n(t)$. Then*

$$\langle \alpha_1, \cdots, \alpha_r \rangle \supset \langle \beta_1, \cdots, \beta_s \rangle .$$

Therefore, in particular, the splitting field of $\Delta_n(t)$ is contained in that of $\Delta_K(t)$.

Proof. Since we are concerned with only the characteristic roots, we consider the vector space $V_n = F_n/F_{n+1} \otimes C$ instead of a free abelian group F_n/F_{n+1}, and the vector space $\Lambda_n \otimes C$ instead of Λ_n.

Since $\Delta_K(t)$ has no repeated roots, the characteristic polynomial coincides with the minimal polynomial and further V_1 is completely reducible. Therefore, we can choose a new basis $\{\bar{x}_1, \cdots, \bar{x}_r\}$ for V_1 so that $\hat{\phi}_1(\bar{x}_i) = \alpha_i \bar{x}_i$. The corresponding new basis of $\Lambda_1 \otimes C$ will be written as $\bar{\xi}_1, \cdots, \bar{\xi}_r$ and $\tilde{\phi}_1(\bar{\xi}_i) = \alpha_i \bar{\xi}_i$. Then $\tilde{\phi}_n$ maps a basis element $\bar{\xi}_{i,n}$ of $\Lambda_n \otimes C$ to an element of the form $\alpha_1^{k_1} \cdots \alpha_r^{k_r} \bar{\xi}_{i,n}$. Therefore, the matrix associated with $\tilde{\phi}_n$ is diagonal and each characteristic root β_i of $\tilde{\phi}_n$, and that of $\hat{\phi}_n$, is of the form $\alpha_1^{k_1} \cdots \alpha_r^{k_r}$. This proves Lemma 7.

Now we proceed to the proof of Theorem 2.

Suppose that G is not p-divisible, $p > 1$. Then there exist x and y in G such that $x \neq y$ but $x^p = y^p$. Since G is a semi-direct product of Z and F, x and y can be written as $x = gt^k$ and $y = ht^k$ for some integer k and for some elements g and h in $F = F_1 = G'$. $g \neq h$, since $x \neq y$. Therefore, there is an element $u \neq 1$ in $F_n - F_{n+1}$, $n \geqq 1$, such that $h = ug$. Then it follows from $x^p = x^p$ that

$$(3.1) \qquad (gt^k)^p = (ugt^k)^p .$$

By induction on p, it is easy to show that

$$(3.2) \quad (ugt^k)^p \equiv u(t^k u t^{-k})(t^{2k} u t^{-2k}) \cdots (t^{(p-1)k} u t^{-(p-1)k})(gt^k)^p (\mathrm{mod}\, F_{n+1}) .$$

Compare (3.1) and (3.2) to obtain

$$(3.3) \qquad u(t^k u t^{-k})(t^{2k} u t^{-2k}) \cdots (t^{(p-1)k} u t^{-(p-1)k}) \equiv 1 \,(\mathrm{mod}\, F_{n+1}) .$$

Consider the semi-direct product $\tilde{G}_n$ of Z and F_n/F_{n+1}, where the action of Z on F_n/F_{n+1} is given by an induced automorphism $\hat{\phi}_n$.

Introduce a new multiplication $mt \cdot g = tg^m t^{-1}$ for $t \in Z$ and $g \in F_n/F_{n+1}$ so that $\widetilde{G}_n$ becomes an R-module, where R is the group ring of the infinite cyclic group Z. This R-module $\widetilde{G}_n$ is finitely presented and its relation matrix is $\| M_n - tI \|$.

Then equation (3.3) is interpreted as a relation (3.4) below, which holds in $\widetilde{G}_n$:

$$(3.4) \qquad (1 + t^k + t^{2k} + \cdots + t^{(p-1)k})u = 0 .$$

Since $\| M_n - tI \|$ is a relation matrix of the R-module $\widetilde{G}_n$, some factor of the characteristic polynomial $\Delta_n(t)$ of M_n must divide $f(t) = 1 + t^k + \cdots + t^{(p-1)k} = (1 - t^{pk})/(1 - t^k)$. Since p is prime, it follows that the set of roots of $\Delta_n(t)$ contains a mpth root of unity, $m \mid k$, and hence, it contains a pth root of unity. Theorem 2 now follows form Lemma 7.

COROLLARY 1. *Under the hypothesis of Theorem 2, if the group of a knot K is not p-divisible, then the splitting field of $\Delta_K(t)$ contains a pth root of unity.*

4. Divisibility of the groups of torus knots.

THEOREM 3. *The group G of the torus knot $K(m, n)$ is p-divisible, p a prime, iff $(n, p) = (m, p) = 1$. In any case, any two solutions of the equation $x^p = y^p$ are conjugate.*

Proof. Suppose that G is not p-divisible. We want to show that $p \mid n$ or $p \mid m$.

Sincc $\Delta(t) = (1 - t)(1 - t^{mn})/(1 - t^m)(1 - t^n)$, all the roots $\alpha_1, \cdots, \alpha_{(m-1)(n-1)}$ of $\Delta(t)$ are distinct and they are mnth root of unity. Therefore, $\langle \alpha_1, \cdots, \alpha_{(m-1)(n-1)} \rangle$ contains only mnth roots of unity. On the other hand, it follows from Theorem 2 that $\langle \alpha_1, \cdots, \alpha_{(m-1)(n-1)} \rangle$ must contain a pth root of unity. Therefore, p must be a divisor of mn, and hence, $p \mid m$ or $p \mid n$. To prove the converse, let G have a presentation $(a, b \colon a^m = b^n)$. If $p \mid m$, then $m = pq$, and $ba^q b^{-1} \neq a^q$, since a^m generates the center of G. However, $(ba^q b^{-1})^p = a^{pq}$. Therefore, G is not p-divisible.

To prove the last part[1], first we should note that $G = G_1 \mathop{*}_H G_2$, where G_1, G_2, and H are infinite cyclic groups generated by a, b, and $c = a^m (= b^n)$, respectively, and H is the center of G, but H is not an isolated subgroup of G_i, $i = 1, 2$.

Now, suppose $x^p = y^p$. We may assume without loss of generality that $p \mid m$ and hence, $p \nmid n$, since $(m, n) = 1$.

[1] I owe the proof mostly to D. Solitar.

Let $x = hx_1 \cdots x_k$ and $y = gy_1 \cdots y_l$ be the normal forms of x and y, where $h = c^r = a^{mr}$ and $g = c^s = a^{ms}$. By Lemma 6, one of x and y, x say, is assumed to be cyclically reduced. Further, if $k = 1$, we may assume that x is in G_1.

Case 1. y is cyclically reduced.

It is obvious that $k \geqq 2$ iff $l \geqq 2$ and if $k, l \geqq 2$, then $k = l$. Therefore, $x = y$ follows immediately from $x^p = y^p$.

Suppose that $k \leqq 1$ and $l \leqq 1$. There are six cases to be considered.

$$\text{(i)} \quad \begin{cases} x = c^r a^d \\ y = c^s a^e \end{cases} \qquad \text{(ii)} \quad \begin{cases} x = c^r a^d \\ y = c^s b^f \end{cases}$$

$$\text{(iii)} \quad \begin{cases} x = c^r a^d \\ y = c^s \end{cases} \qquad \text{(iv)} \quad \begin{cases} x = c^r \\ y = c^s a^e \end{cases}$$

$$\text{(v)} \quad \begin{cases} x = c^r \\ y = c^s b^f \end{cases} \qquad \text{(vi)} \quad \begin{cases} x = c^r \\ y = c^s , \end{cases}$$

where $0 < d, e < m$, and $0 < f < n$.

In Cases (i) and (vi), it is easy to see that $x = y$ follows from $x^p = y^p$. Case (ii) does not occur. In fact, $x^p = y^p$ implies that $fp \equiv 0 \pmod n$ and hence, $f \equiv 0 \pmod n$, since $(p, n) = 1$. Similarly, Case (v) does not occur. Case (iii) also does not occur. In fact, $x^p = y^p$ implies that $rmp + dp = smp$, and hence, $d \equiv 0 \pmod m$. Similarly, Case (iv) does not occur.

Case 2. y is not cyclically reduced.

Suppose that $l(x) = k \geqq 2$. Then $l(x^p)$ is always even, while $l(y)$ is odd by Lemma 2. Therefore, $x^p \neq y^p$, and hence, $l(x) \leqq 1$.

Suppose that $l(x) \leqq 1$. Since y is not cyclically reduced, $\tilde{l}(y) \neq 0$. *If* $\tilde{l}(y) \geqq 2$, then $l(y^p) \geqq 2$ by Lemma 2. This contradicts $x^p = y^p$. Therefore, $\tilde{l}(y) = 1$.

Now we have to consider the following four cases.

$$\text{(i)} \quad \begin{cases} x = c^r a^d \\ y = u^{-1} c^s a^e u \end{cases} \qquad \text{(ii)} \quad \begin{cases} x = c^r a^d \\ y = u^{-1} c^s b^f u \end{cases}$$

$$\text{(iii)} \quad \begin{cases} x = c^r \\ y = u^{-1} c^s a^e u \end{cases} \qquad \text{(iv)} \quad \begin{cases} x = c^r \\ y = u^{-1} c^s b^f u , \end{cases}$$

where $0 < d, e < m$, and $0 < f < n$.

Now Case (ii) does not occur. In fact, $x^p = y^p$ implies that $c^{rp} a^{dp} = u^{-1} c^{sp} b^{fp} u$ and hence, $b^{fp} \in H$, otherwise $l(y^p) \geqq 2$. Therefore,

$fp \equiv 0 (\mathrm{mod}\, n)$. Since $(p, n) = 1$, it follows that $f \equiv 0 \,(\mathrm{mod}\, n)$. This contradicts $0 < f < n$. By a similar argument, we can prove that Case (iv) does not occur. Case (iii) does not occur. In fact $x^p = y^p$ implies that $a^{rpm} = u^{-1} a^{spm+ep} u$ and hence, $rpm = spm + ep$. It shows that $e \equiv 0 \,(\mathrm{mod}\, m)$, which contradicts $0 < e < m$.

Now consider Case (i). If $(c^s a^e)^p \notin H$, then $l(y^p) \geqq 2$, while $l(x^p) = 1$. Therefore, $(c^s a^e)^p \in H$. Then $x^p = y^p$ implies that $a^{rmp+dp} = u^{-1} a^{smp+ep} u = a^{spm+ep}$, since $a^{spm+ep} \in H$. Therefore, $rmp + dp = spm + ep$ and hence, $rm + d = sm + e$. This shows that $y = u^{-1} x u$.

This proves Theorem 3.

5. Applications.

PROPOSITION 3. *The group G of the figure eight knot K is an R-group.*

Proof. Since $\Delta_K(t) = 1 - 3t + t^2$ has two real roots α and $1/\alpha$, $|\alpha| \neq 1$, it follows that $\langle \alpha \rangle$ contains only real numbers. Therefore, G is p-divisible except possibly for $p = 2$. If $\langle \alpha \rangle$ contains -1, $\alpha^n = -1$ for some integer n. Therefore $|\alpha| = 1$, a contradiction. Since $\langle \alpha \rangle$ has no nontrivial roots of unity, it follows from Theorem 2 that G is an R-group.

Note that the figure eight knot is the only fibred knot K with $\Delta_K(t) = 1 - 3t + t^2$.

Finally we consider the knots whose Alexander polynomials $\Delta(t)$ are of degree 4.[2] Such a polynomial has the form:

$$\Delta(t) = (t - \alpha)\left(t - \frac{1}{\alpha}\right)(t - \beta)\left(t - \frac{1}{\beta}\right).$$

Note that $\alpha \neq 1$ and $\beta \neq 1$.

Case 1. Both α and β are real.

Case 2. Only one of them, α say, is real.

Case 3. Neither α nor β is real.

Case 1. $\langle \alpha, \beta \rangle$ contains no nontrivial pth root of unity, except possibly for -1.

If both α and β are positive, then $\langle \alpha, \beta \rangle$ does not contain -1, and hence, G is an R-group.

Case 2. Since β and $1/\beta$ are roots of a quadratic equation $1 + at + t^2 = 0$ for some real number a, we see that $1/\beta = \bar{\beta}$ and $|\beta| = 1$. Suppose that $\xi = \alpha^m (1/\alpha)^n \beta^r \bar{\beta}^s$ is a pth root of unity. Then

[2] I am grateful to R. A. Smith for his helpful suggestion.

$|\xi| = |\alpha|^{m-n} = 1$ yields $m = n$, and hence, $\xi = \beta^{r-s}$. Therefore, β is a $p(r - s)$th root of unity. Thus the splitting field of $\Delta(t)$ must contain a $p(r - s)$th root of unity.

Case 3. If one of the roots has the absolute value 1, so do all the roots. Kronecker's theorem, then, says that all the roots are mth roots of unity for some m.

Suppose that $|\alpha| \neq 1$. Since α and β are complex roots, $\bar{\alpha}$ and $\bar{\beta}$ are also the roots of $\Delta(t)$. If $\bar{\alpha} = 1/\alpha$, then $|\alpha| = 1$, a contradiction. If $\bar{\alpha} = \beta$, then $|\alpha| = |\beta|$, and hence, $|\alpha| = |\beta| = 1$, since $|\alpha\beta| = 1$. This contradicts our assumption. Therefore, $\bar{\alpha} = 1/\beta$. Suppose that $\langle \alpha, \beta \rangle$ contains an nth root of unity ξ. We write $\xi = \alpha^k \beta^l$. Since $\bar{\alpha} = 1/\beta$, we see that $\xi = \alpha^k \bar{\alpha}^{-l}$. Then $1 = |\xi| = |\alpha|^{k-l}$ yields $k = l$. Therefore, $\xi = (\alpha/\bar{\alpha})^k$ and $\alpha/\bar{\alpha}$ is a knth root of unity. Since $\alpha/\bar{\alpha}$ is contained in the splitting field $\mathscr{F}$ of $\Delta(t)$, $\mathscr{F}$ must contain a knth root of unity.

These observations will be collected in the following

PROPOSITION 4. *Let K be a fibred knot. Suppose that $\Delta_K(t)$ is of degree less than* 5 *and has no repeated roots. Then*

(5.1) (1) *If all the roots of $\Delta_K(t)$ are positive real numbers, then G, the group of K, is an R-group.*

(2) *Suppose that $\Delta_K(t)$ has only two complex roots β and $\bar{\beta}$. If G is not p-divisible, then β is a pq*th *root of unity for some q, and therefore, the splitting field of $\Delta_K(t)$ contains a pq*th *root of unity.*

(3) *Suppose that $\Delta_K(t)$ has four complex roots α, $\bar{\alpha}$, β, $\bar{\beta}$, and that $|\alpha| \neq 1$. If G is not p-divisible, then $\alpha/\bar{\alpha}$ is a kp*th *root of unity for some k, and therefore, the splitting field of $\Delta_K(t)$ contains a kp*th *root of unity.*

This proposition will be used to prove Proposition 5 below.

In 1961, Trotter [4] studied the splitting fields of the Alexander polynomials of certain fibred knots. Combining his results [4, p. 557] with corollary, we obtain that

(5.2) (1) The groups of 4_1, 6_2, 7_6, 8_{12}, 9_{42}, 9_{44}, 9_{45}, are p-divisible for all prime p other than 2,

(2) The groups of 3_1, 6_3, 7_7, 8_{20}, 8_{21}, 9_{48}, are p-divisible for all prime other than 2 or 3,

(3) The group of 5_1 is p-divisible for all prime p other than 2 or 5.

Since the divisibility of the groups of 3_1, 4_1, and 5_1 has already been determined, we consider the remaining eleven knots.

Now, each of the Alexander polynomials of 8_{12} and 9_{45} has four positive real roots. Therefore by (5.1) (1), their groups are R-groups.

On the other hand, each of the Alexander polynomials of 6_2, 7_6, and 9_{42} has only two complex roots. If their groups are not 2-divisible, the splitting fields of their Alexander polynomial must contain $2q$th root of unity by (5.1) (2). According to [4, p. 557] they contain only 2nd root of unity. Therefore, one of the complex roots must be -1, which cannot occur.

That the group G of 9_{48} is an R-group will be proved as follows.

Suppose that G is not p-divisible, $p = 2$ or 3. Since the splitting field of the Alexander polynomial of 9_{48} contains only 2nd, 3rd, or 6th root of unity, it follows from (5.1) (2) that one of the complex roots, β say, is either 2nd, 3rd, or 6th root of unity. However, the calculation shows that

$$\beta = \frac{7-\sqrt{13}}{4} + \frac{1}{2\sqrt{2}}\sqrt{7\sqrt{13}-23}\,i\,,$$

which is none of 2nd, 3rd and 6th root of unity.

Therefore, G is an R-group.

Finally, we consider the groups of 9_{44}, 6_3, and 7_7. Each of the Alexander polynomials of these knots has four complex roots, each of which does not lie on the unit circle. Therefore, we can apply (5.1) (3) on these groups.

Let $\mathscr{F}(K)$ denote the splitting field of $\Delta_K(t)$. Then according to [4, p. 557], we know that

(5.3) (1) $\mathscr{F}(9_{44})$ contains only the 2nd and 4th roots of unity.

(2) $\mathscr{F}(6_3)$ and $\mathscr{F}(7_7)$ contain only the 2nd 3rd, and 6th roots of unity.

Now a direct computation shows that

$$\Delta_{9_{44}}(t) \text{ has a root } \alpha_1 = \frac{1}{2}\left\{\left(2+\sqrt{\frac{\sqrt{17}-1}{2}}\right) + i\left(1+\sqrt{\frac{\sqrt{17}+1}{2}}\right)\right\},$$

$$\Delta_{6_3}(t) \text{ has a root } \alpha_2 = \frac{1}{4}\{(3-\sqrt{\sqrt{52}-5}) + i(3+\sqrt{\sqrt{52}+5})\}\,,$$

and

$$\Delta_{7_7}(t) \text{ has a root } \alpha_3 = \frac{1}{4}\{(5+\sqrt{\sqrt{84}+3}) + i(3+\sqrt{\sqrt{84}-3})\}\,.$$

Then it is easy to verify that $\alpha_1/\bar{\alpha}_1$ is none of the 2nd and 4th root of unity, and each of $\alpha_2/\bar{\alpha}_2$ and $\alpha_3/\bar{\alpha}_3$ is none of the 2nd, 3rd, and 6th root of unity.

Therefore, the groups of these three knots are R-groups.

This proves the following

PROPOSITION 5. *The groups of knots* 4_1, 6_2, 6_3, 7_6, 7_7, 8_{12}, 9_{42}, 9_{44}, 9_{45}, 9_{48} *are R-groups.*

REMARK. (2.1) (2) is not a necessary condition for G to be an R-group.

REFERENCES

1. A. G. Kurosh, *The Theory of Groups, II*, New York, Chelsea, 1957.
2. W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory*, Intersciences, New York, 1966.
3. L. Neuwirth, *Knot Groups*, Annals of Mathematical Studies 56, Princeton University Press, 1965.
4. H. F. Trotter, *Periodic automorphisms of groups and knots*, Duke Math. J., **28** (1961), 553-557.

Received February 22, 1973 and in revised form March 18, 1974. This research was supported in part by the Canada Council Leave Fellowship W710027 and NRC Grant No. A4034.

UNIVERSITY OF TORONTO