Journal of Pure and Applied Algebra 51 (1988) 217–229
North-Holland

ON PROPER POWERS IN FREE PRODUCTS AND DEHN SURGERY

Steven BOYER*
Department of Mathematics, University of Toronto, Toronto, Canada, M5S 1A1

Communicated by C.A. Weibel
Received 13 May 1986

We prove that for any triple (p, q, r) of integers, each greater than or equal to 2, and word $w \in \mathbb{Z}/p * \mathbb{Z}/q$, the group $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle$ is nontrivial. Conditions on the triple (p, q, r) are found under which this quotient group is infinite. We then apply these results to provide the last piece of evidence needed to show that nonintegral Dehn surgery on a knot in S^3 cannot yield a reducible 3-manifold.

Introduction

The main result of this paper is the following theorem:

Theorem 1. *Let p, q and r be integers greater than or equal to 2. Then for any word $w \in \mathbb{Z}/p * \mathbb{Z}/q$,*

$$(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle \not\cong \{e\} .$$

Here the symbol '$*$' denotes the free product operation between groups and '$\langle w^r \rangle$' denotes the normal closure of w^r in $\mathbb{Z}/p * \mathbb{Z}/q$.

Theorem 1 has been discovered independently by Baumslag, Morgan and Shalen [1]. We direct the reader to this paper for an alternate approach to the theorem.

Our proof involves the construction of a nontrivial representation

$$\rho : \mathbb{Z}/p * \mathbb{Z}/q \to \mathrm{SO}(3)$$

for which $\rho(w)^r = e$ (e will always be used to denote the identity elements of the groups appearing in this paper). Consideration of the image of ρ allows us to deduce

* Partially supported by NSERC Grant A4034. Current address: Département de mathématiques et d'informatique, Université du Québec à Montréal, C.P. 8888, Succursale "A" Montréal, Canada, H3C 3P8.

Theorem 2. *Suppose $w \in \mathbb{Z}/p * \mathbb{Z}/q$ projects to nontrivial elements of $\mathbb{Z}/p$ and $\mathbb{Z}/q$ and that $r \geq 2$ is such that*

(i) *no two of p, q and r are 2,*

(ii) $\max\{p, q, r\} \geq 6$.

Further, if (p, q, r) is a permutation of either $(2, 3, 6)$, $(2, 4, 4)$ or $(2, 6, 6)$ assume

(iii) *w does not project to generators of both $\mathbb{Z}/p$ and $\mathbb{Z}/q$.*

Then the quotient $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle$ is infinite.

Using the techniques developed in this paper we can show that if w projects nontrivially to both $\mathbb{Z}/p$ and $\mathbb{Z}/q$, then excluding some 32 exceptional triples (p, q, r), $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle$ will be infinite when the classical criterion $1/p + 1/q + 1/r \leq 1$ holds. The exceptions reflect the fact that certain infinite triangle groups

$$\Delta(p, q, r) = \langle x, y \mid x^p = y^q = (xy)^r = e \rangle$$

admit no representations in SO(3) with infinite image.

In the previously mentioned paper [1], the authors use the larger group $PSL_2(\mathbb{C})$ as a universal target, and the extra room afforded by this noncompact group allows them to show $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle$ is infinite whenever $1/p + 1/q + 1/r \leq 1$. The main difference in the two approaches is that in [1], representations are constructed which inject the factors $\mathbb{Z}/p$ and $\mathbb{Z}/q$ and which send w to an element of order r. We can do this in most, but not all cases (see the addendum in Section 2).

Similar techniques to those used in proving Theorem 1 yield

Theorem 3. *Let $A_1, A_2, \ldots, A_n$ be an arbitrary collection of nontrivial abelian groups, where $n \geq 2$. Then for any $w \in P = A_1 * A_2 * \cdots * A_n$ and $r \geq 2$, at least $n - 1$ of the natural homomorphisms*

$$A_i \to P/\langle w^r \rangle$$

are injections. If we assume further that w projects nontrivially to each A_i, then all n of these homomorphisms are injections.

Theorem 3 has also been discovered by Fine, Howie and Rosenberger [4].

It has been conjectured that for any nontrivial groups G_1, G_2, $w \in G_1 * G_2$ and $r \geq 2$, $(G_1 * G_2)/\langle w^r \rangle \not\cong \{e\}$ (see [7, §9]). When $r \geq 4$ this is known to be true [6, §4; 11]. An immediate corollary of Theorem 3 is

Corollary 4. *If G_1, G_2 are nonperfect groups, $w \in G_1 * G_2$ and $r \geq 2$, $G_1 * G_2/\langle w^r \rangle \not\cong \{e\}$.* □

We close the introduction by describing some applications of Theorem 1 to the topology of 3-manifolds. It was these connections which originally motivated our studies.

The Dehn surgery operation, performed on a smooth knot in a 3-manifold, is one of the most important constructions in 3-manifold theory. Of particular interest is when the knot, K, lies in the 3-sphere, S^3. For a reduced fraction $a/b \in \mathbb{Q} \cup \{1/0\}$ we shall let $M(K, a/b)$ denote the 3-manifold resulting from the (a/b)-Dehn surgery along K (see [13, §9.G]). Using the work of González-Acuña and Short [6], Theorem 1 may be shown to imply

Corollary 5. *If $M(K, a/b) \cong M_1 \# M_2$, where $H_1(M_i) \not\cong \{0\}$ $(i = 1, 2)$, then $b = \pm 1$. In particular, the connected sum of two lens spaces can so arise only as an integral surgery on S^3.*

Gordon and Luecke have observed that through their joint work with Culler and Shalen [3], Corollary 5 is the last piece of evidence needed to deduce,

Theorem (Gordon and Luecke [9]). *If $M(K, a/b)$ is reducible, then $b = \pm 1$.* □

There are many well-known instances of when an integral Dehn surgery on a knot in S^3 yields a reducible 3-manifold. For instance, for any relatively prime pair $p, q \geq 2$, the connected sums $L(p, q)\#L(q, p)$ can so occur (see [5, 7, 12] for these and other examples). Using the relationship between the surgery coefficient (a/b) and the link pairing on $M(K, a/b)$ we shall show

Proposition 6. *Suppose $L(p, s)\#L(q, t)$ occurs as a Dehn surgery on a knot in S^3. Then there is an integer u, relatively prime to pq, and an $\varepsilon = \pm 1$ so that*

$$L(p, s) = \varepsilon L(p, u^2 q) \quad \textit{and} \quad L(q, t) = \varepsilon L(q, u^2 p) .$$

The paper is organized in the following fashion. Section 1 contains several elementary lemmas which are used in Section 2 to prove Theorems 1–3. The reader is advised to proceed directly to Section 2 and to refer back to Section 1 when necessary. The last section, Section 3, is used to discuss the topological results referred to above.

1. Background results

Recall that $\mathrm{SO}(3) \cong \mathrm{SU}(2)/\{\pm e\}$ and let

$$\lambda : \mathrm{SU}(2) \rightarrow \mathrm{SO}(3)$$

be the quotient map. As $-e$ is the only element in SU(2) of order 2, the following is easily verified:

Lemma 1.1. *For any* $c \in \mathrm{SU}(2)$ *or order* $n > 0$, $\lambda(c) \in \mathrm{SO}(3)$ *has order* $(n/2)$ *or* n *depending on whether or not* n *is even or odd.* □

Lemma 1.2. *Suppose numbers* α_1, α_2 *are given where* $0 \leq \alpha_1 \leq \alpha_2 \leq 1$. *Then for any* $n > 1$,

$$|\{m \mid \alpha_1 n \leq m \leq \alpha_2 n \text{ and } \gcd(m, n) = 1\}| > (\alpha_2 - \alpha_1)\phi(n) - 2^{\nu(n)}$$

where ϕ *is the Euler* ϕ*-function and* $\nu(n)$ *is the number of distinct prime factors of* n.

Proof. Recall the Möbius function $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ given by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1\,, \\ (-1)^{\nu(d)} & \text{if } d \text{ is square free}\,, \\ 0 & \text{if } d \text{ is not square free}\,. \end{cases}$$

It is easy to show that for any $m > 0$,

$$\sum_{d \mid m} \mu(d) = \begin{cases} 1 & \text{if } m = 1\,, \\ 0 & \text{if } m > 1\,. \end{cases}$$

Thus

$$\begin{aligned}
&|\{m \mid \alpha_1 n \leq m \leq \alpha_2 n \text{ and } \gcd(m, n) = 1\}| \\
&\quad = \sum_{\alpha_1 n \leq m \leq \alpha_2 n} \; \sum_{d \mid \gcd(m, n)} \mu(d) \\
&\quad = \sum_{d \mid n} \left[\frac{(\alpha_2 - \alpha_1)n}{d}\right] \mu(d) \\
&\quad = (\alpha_2 - \alpha_1)n \sum_{d \mid n} \frac{\mu(d)}{d} + \varepsilon \\
&\quad = (\alpha_2 - \alpha_1)n\left(\frac{\phi(n)}{n}\right) + \varepsilon \quad \text{(see [10, §16.3])} \\
&\quad = (\alpha_2 - \alpha_1)\phi(n) + \varepsilon
\end{aligned}$$

where

$$\begin{aligned}
|\varepsilon| &= \left|\sum_{d \mid n} \left\{\left[\frac{(\alpha_2 - \alpha_1)n}{d}\right] - \frac{(\alpha_2 - \alpha_1)n}{d}\right\} \mu(d)\right| \\
&< \sum_{d \mid n} |\mu(d)| \\
&= 2^{\nu(n)}\,.
\end{aligned}$$

Clearly this completes the proof. □

Lemma 1.3. *Suppose n is a positive integer other than* $1, 2$ *or* 12. *Then there is a primitive nth root of unity u with* $\mathrm{Im}(u) \geq 1/\sqrt{2}$.

Proof. It suffices to find an integer m, relatively prime to n, with $\frac{1}{8}n \leq m \leq \frac{3}{8}n$. By applying Lemma 1.2 with $\alpha_1 = \frac{1}{8}$ and $\alpha_2 = \frac{3}{8}$ we are ensured of such an m as long as $\phi(n)/2^{\nu(n)} \geq 4$. This inequality is readily checked for $\nu(n) \geq 5$. Assume then that $1 \leq \nu(n) \leq 4$.

Now for an integer n with $\nu(n) = 4$, any sequence of 10 consecutive integers contains at least one relatively prime to n. Hence if $n > 40$, there will always be an m with $\frac{1}{8}n < m < \frac{3}{8}n$ and $\gcd(n, m) = 1$. But for $\nu(n) = 4$, $n \geq 210$ and thus the lemma holds for this case.

For $\nu(n) = 3, 2$ or 1, any sequence of respectively $6, 4$ or 2 consecutive integers contains at least one relatively prime to n. Hence if $n > 24$, 16 or 8 respectively we are done. The finite number of cases which remain may be checked by hand. □

A similar analysis proves the next lemma.

Lemma 1.4. *Suppose n is a positive integer other than* 1, 2, 3, 4, 6, 8 *or* 12. *Then there is a primitive nth root of unity contained in the interior of any subsector of the upper half circle of angle* $\frac{1}{2}\pi$. □

Lemma 1.5. *Let positive integers s, n be given and set* $d = \gcd(s, n)$. *Then if u_1 is any primitive (n/d)th root of unity, there is a primitive nth root of unity u such that* $u^s = u_1$.

Proof. Set $u_1 = \exp(2\pi \mathrm{i} td/n)$ where $\gcd(t, n/d) = 1$. By Dirichlet's theorem on primes in arithmetic progression we may assume that t is a prime larger than n. In particular we may suppose $\gcd(t, n) = 1$.

Next choose integers a, b such that $as + bn = d$. Evidently $\gcd(a, n/d) = 1$ and note that for any $k \in \mathbb{Z}$, $(a + k(n/d))s + (b - k(s/d))n = d$. Hence by another application of Dirichlet's theorem we may assume that $\gcd(a, n) = 1$.

Set

$$u = \exp\left(\frac{2\pi \mathrm{i} ta}{n}\right).$$

Then u is a primitive nth root of unity for which

$$u^s = \exp\left(\frac{2\pi \mathrm{i} tas}{n}\right) = \exp\left(\frac{2\pi \mathrm{i}(td - tbn)}{n}\right) = u_1 .$$

Thus we are done. □

Remark 1.6. It is not hard to combine Lemmas 1.3 and 1.5 to show that given nonzero integers s and n, $s \not\equiv 0 \pmod n$, there is an nth root of unity u such that $\mathrm{Im}(u^s) \geq 1/\sqrt{2}$. Further, if $(n/\gcd(n, s)) \neq 2$ or 12, u may be assumed to be primitive.

We close this section by stating three elementary lemmas.

Lemma 1.7. *The function* trace : $\mathrm{SU}(2) \to [-2, 2]$ *faithfully distinguishes conjugacy classes. In particular, each element $c \in \mathrm{SU}(2)$ is conjugate to its adjoint c^*.* □

Lemma 1.8. *Each $c \in \mathrm{SU}(2)$ is conjugate to a diagonal matrix. Hence, by Lemma 1.7, c has order n in* SU(2) *if and only if* $\mathrm{trace}(c) = 2\cos(2\pi j/n)$ *for some integer j relatively prime to n.* □

Lemma 1.9. *Let a and b be noncommuting elements of a dihedral group such that a has order 2 and b has order greater than 2. Then any element $a^{m_1}b^{n_1}a^{m_2}b^{n_2} \cdots a^{m_l}b^{n_l}$ has order 2 as long as $\sum_{i=1}^{l} m_i$ is odd.* □

2. Proofs of the main theorems

In this section we prove Theorems 1–3. First though we must generate some notation.

The groups $\mathbb{Z}/p$, $\mathbb{Z}/q$ will be written multiplicatively as

$$\mathbb{Z}/p = \{e, x, \ldots, x^{p-1}\},$$
$$\mathbb{Z}/q = \{e, y, \ldots, y^{q-1}\}.$$

For the purposes of Theorem 1 we may assume that w projects nontrivially to each of the factor groups $\mathbb{Z}/p$ and $\mathbb{Z}/q$, as otherwise the result is obvious. Suppose then that,

$$w \to (x^s, y^t) \in \mathbb{Z}/p \oplus \mathbb{Z}/q$$

upon abelianization, where $s \not\equiv 0 \pmod p$ and $t \not\equiv 0 \pmod q$.

Let $F(\tilde{x}, \tilde{y})$ be a free group on symbols $\tilde{x}$, $\tilde{y}$ and choose $\tilde{w} \in F(\tilde{x}, \tilde{y})$ which maps to w under the obvious epimorphism $F(\tilde{x}, \tilde{y}) \to \mathbb{Z}/p * \mathbb{Z}/q$. We may and do assume that the exponent sums of $\tilde{w}$ in $\tilde{x}$ and $\tilde{y}$ are s and t respectively.

Note that for any group G, there is a function

$$\tilde{w} : G \times G \to G$$

where $\tilde{w}(a, b)$ is the result of formally replacing $\tilde{x}$ and $\tilde{y}$ in $\tilde{w}$ by a and b respectively. If G happens to be a topological group, then $\tilde{w}$ will be continuous.

Proof of Theorem 1. It evidently suffices to construct a nontrivial representation $\rho : \mathbb{Z}/p * \mathbb{Z}/q \to \mathrm{SO}(3)$ for which $\rho(w)^r = e$.

Lemma 2.1. *To produce such a ρ, we need only find elements $a, b \in \mathrm{SU}(2)$ with*
(i) $\lambda(a) \neq e$ *and* $\lambda(b) \neq e$,
(ii) $a^{2p} = b^{2q} = \tilde{w}(a, b)^{2r} = e$.

Proof. Tentatively define ρ by $\rho(x) = \lambda(a)$ and $\rho(y) = \lambda(b)$. According to Lemma 1.1, this does define a homomorphism which by (i) is nontrivial. Further,

$$\rho(w)^r = \tilde{w}(\lambda(a), \lambda(b))^r = \lambda(\tilde{w}(a, b)^r) = \lambda(\pm e) = e .$$

Thus the lemma is proved. □

To find a and b we proceed as follows. By Remark 1.6 we may choose $(2p)$th and $(2q)$th roots of unity u and v with $\mathrm{Im}(u^s) \geq 1/\sqrt{2}$, $\mathrm{Im}(v^t) \geq 1/\sqrt{2}$. Define elements a_0 and b_0 of SU(2) by

$$a_0 = \begin{bmatrix} u & 0 \\ 0 & \bar{u} \end{bmatrix}, \qquad b_0 = \begin{bmatrix} v & 0 \\ 0 & \bar{v} \end{bmatrix}.$$

Evidently neither $\lambda(a_0) = e$ nor $\lambda(b_0) = e$.

If

$$\mathcal{O}(b_0) = \{ c b_0 c^{-1} \mid c \in \mathrm{SU}(2) \} ,$$

then $\mathcal{O}(b_0)$ is a connected subspace of SU(2). Indeed $\mathcal{O}(b_0) \cong S^2$. According to Lemma 1.7, $b_0^* \in \mathcal{O}(b_0)$.

Consider the continuous function

$$f : \mathcal{O}(b_0) \to [-2, 2] , \qquad b \to \mathrm{trace}(\tilde{w}(a_0, b)) .$$

Now as $\tilde{w}$ was chosen to have exponent sums s and t in $\tilde{x}$ and $\tilde{y}$, and as a_0 commutes with both b_0 and b_0^*,

$$f(b_0) = \mathrm{trace}\left(\begin{bmatrix} u^s v^t & 0 \\ 0 & \bar{u}^s \bar{v}^t \end{bmatrix}\right) = (u^s v^t + \bar{u}^s \bar{v}^t) ,$$

$$f(b_0^*) = \mathrm{trace}\left(\begin{bmatrix} u^s \bar{v}^t & 0 \\ 0 & \bar{u}^s v^t \end{bmatrix}\right) = (u^s \bar{v}^t + \bar{u}^s v^t) .$$

It follows that the connected set $f(\mathcal{O}(b_0))$ contains an interval of length at least

$$\begin{aligned} |f(b_0^*) - f(b_0)| &= |(u^s\bar{v}^t + \bar{u}^s v^t) - (u^s v^t + \bar{u}^s \bar{v}^t)| \\ &= |(\bar{u}^s - u^s)(v^t - \bar{v}^t)| \\ &= 4\,\mathrm{Im}(u^s)\,\mathrm{Im}(v^t) \\ &\geq 2\,, \end{aligned}$$

as $\mathrm{Im}(u^s) \geq 1/\sqrt{2}$ and $\mathrm{Im}(v^t) \geq 1/\sqrt{2}$.

But for any $j \in \mathbb{Z}$,

$$\left| 2\cos\left(\frac{2\pi(j+1)}{2r}\right) - 2\cos\left(\frac{2\pi j}{2r}\right) \right| \leq 2\,.$$

Then we may find $b \in \mathcal{O}(b_0)$ and $j \in \mathbb{Z}$ with

$$\mathrm{trace}(\tilde{w}(a_0, b)) = 2\cos\left(\frac{2\pi j}{2r}\right).$$

By Lemma 1.8, $\tilde{w}(a_0, b)^{2r} = e$ and so the elements $a_0, b \in \mathrm{SU}(2)$ satisfy the hypotheses of Lemma 2.1. The proof of Theorem 1 is therefore completed. □

Remark 2.2. It can be shown that in most cases, the groups from Theorem 1 admit nontrivial representations to SU(2). Consideration of the icosahedral group $\Delta(2,3,5)$ [16, §2.6], shows that this is false in general.

We must sharpen Theorem 1 in preparation for the proof of Theorem 2.

Addendum. *Suppose that $w \in \mathbb{Z}/p * \mathbb{Z}/q$ projects to elements of order $\bar{p}$, $\bar{q}$ in $\mathbb{Z}/p$ and $\mathbb{Z}/q$ and that the triple $(\bar{p}, \bar{q}, r)$ is not a permutation of either* $(2,2,2)$, $(2,3,6)$, $(2,4,4)$, $(2,4,6)$, $(2,6,6)$, $(3,6,6)$ *or* $(4,6,12)$. *Then the representation ρ may be constructed so as to have nonabelian image in* SO(3) *and so that $\rho(x)$, $\rho(y)$ and $\rho(w)$ have orders p, q and r respectively.*

Proof. We shall continue to use the notation developed in the proof of Theorem 1. Note $p = \bar{p}\gcd(p, s)$ and $q = \bar{q}\gcd(q, t)$.

Assume first of all that neither $\bar{p}$, $\bar{q}$ nor r is 6. After possibly replacing s by $s + p$ and t by $t + q$, we may suppose that $2p = (2\bar{p})\gcd(2p, s)$ and $2q = (2\bar{q})\gcd(2q, t)$. Then by Remark 1.6, u and v may be chosen to be primitive $(2p)$th and $(2q)$th roots of unity and therefore $\rho(x)$ and $\rho(y)$ will have orders p and q (Lemma 1.1). It is not hard to show that the proof of the addendum will be complete if we can find $b \in \mathcal{O}(b_0)$ satisfying

(i) $f(b) = 2\cos\theta$, where $e^{i\theta}$ is a primitive $(2r)$th (or possibly rth if r is odd) root of unity;

(ii) $\lambda(a_0)\lambda(b) \neq \lambda(b)\lambda(a_0)$.

To that end let $g: S^1 \to [-2, 2]$ be the function $g(e^{i\theta}) = 2\cos\theta$ and recall that image(f) contains the interval $[2\,\mathrm{Re}(u^s v^t),\ 2\,\mathrm{Re}(u^s \bar{v}^t)]$. As $\mathrm{Im}(u^s)$, $\mathrm{Im}(v^t) \geq 1/\sqrt{2}$

$$g^{-1}([2\,\mathrm{Re}(u^s v^t), 2\,\mathrm{Re}(u^s \bar{v}^t)]) \cap S^1_+$$

(S^1_+ being the upper half circle) contains a sector of angle $\pi/2$. According to Lemma 1.4, this sector contains at least one primitive $(2r)$th root of unity *in its interior*, as long as $r \neq 2$, 3, 4 or 6. It is easy to see that the same is true when $r = 2$ or 4 unless $(\bar{p}, \bar{q}, r)$ is a permutation of $(2, 4, 4)$. In the case $r = 3$, we may find either a primitive 3rd or a primitive 6th root of unity in the interior of the sector.

Thus, other than in the cases excepted, we may find a $b \in \mathcal{O}(b_0)$ so that $f(b) = 2\cos\theta$ where $e^{i\theta}$ is a primitive $(2r)$th (or possibly rth if $r = 3$) root of unity. This shows condition (i), stated above, holds. Further note that $e^{i\theta}$ was in the interior of the sector and so

$$f(b_0) = 2\,\mathrm{Re}(u^s v^t) < f(b) < 2\,\mathrm{Re}(u^s \bar{v}^t) = f(b_0^*)\,.$$

Evidently then $b \not\in \{b_0, b_0^*\}$ and as such, does not commute with a_0.

Now suppose that condition (ii) above fails, that is, suppose $\lambda(a_0)$ commutes with $\lambda(b)$. By construction, we must have $a_0 b = -b a_0$. But then a simple calculation shows that both a_0 and b have order 4 and generate a quaternion group of order 8 in SU(2). It follows that the image of ρ (ρ being defined by $\rho(x) = \lambda(a_0)$, $\rho(y) = \lambda(b)$) is $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. Hence $p = q = r = 2$. But as we have excluded this possibility, condition (ii) must hold.

This addendum has now been shown to be true when none of $\bar{p}$, $\bar{q}$ and r are 6. We leave the cases when one of $\bar{p}$, $\bar{q}$ or r is 6 to the reader. They follow much as above, but it is necessary to prove a version of Lemma 1.4 for sectors subtending an angle of $\pi/3$. $\square$

Remark 2.3. If $(\bar{p}, \bar{q}, r)$ is a permutation of $(2,2,2)$, $(2,3,6)$, $(2,4,4)$, $(3,6,6)$ or $(4,6,12)$, then there is a representation ρ so that $\rho(x)$, $\rho(y)$ and $\rho(w)$ have orders p, q and r respectively, though its image may be abelian.

Proof of Theorem 2. Let (p, q, r) be a triple such that no two of p, q and r are 2 and $\max\{p, q, r\} \geq 6$. Let $w \in \mathbb{Z}/p * \mathbb{Z}/q$ project to nontrivial elements of order $\bar{p}$ and $\bar{q}$ in $\mathbb{Z}/p$ and $\mathbb{Z}/q$ respectively.

The proof will involve several steps. For the first one, assume that $(\bar{p}, \bar{q}, r)$ is a triple to which the addendum to Theorem 1 applies. Then there is a representation $\rho : (\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle \to \mathrm{SO}(3)$ with nonabelian image and for which $\rho(x)$, $\rho(y)$ and $\rho(w)$ have orders p, q and r respectively. Our work shall be done if we can prove that $\pi = \mathrm{image}(\rho)$ is an infinite subgroup of SO(3). If π is finite, then by the classification of finite subgroups of SO(3) [16, Theorem 2.6.5] π is either dihedral or polyhedral. We shall exclude these two possibilities.

Suppose π is dihedral. Then as $\rho(x)$ and $\rho(y)$ do not commute, while any two elements of order greater than 2 in a dihedral group do commute, we see that one of $\rho(x)$ and $\rho(y)$ has order ≥ 2. Without loss of generality we may suppose $\rho(x)^2 = e$. Then $p = 2$ and therefore $q, r \geq 3$. In particular, $\rho(w)$ has order ≥ 3. But by hypothesis, w projects nontrivially to $\mathbb{Z}/p \cong \mathbb{Z}/2$ and thus x occurs an odd number of times in any expansion of w in powers of x and y. Applying ρ to such an expansion and appealing to Lemma 1.9 shows that $\rho(w)^2 = e$. This contradiction implies that π is not dihedral.

Next consider the polyhedral groups. These consist of the alternating groups A_4 and A_5 and the symmetric group S_4. As π contains an element of order $\max\{p, q, r\} \geq 6$, π is not polyhedral. We conclude then that π is an infinite subgroup of SO(3). This gives Theorem 2 for those triples $(\bar{p}, \bar{q}, r)$ to which the addendum applies. We deal with the rest now.

First suppose that $(\bar{p}, \bar{q}, r)$ is a permutation of either $(3,6,6)$ or $(4,6,12)$. These cases will be done if we can construct a surjection of $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle$ onto one of the groups we have just shown to be infinite. When $r = 6$, simply project to $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^3 \rangle$. When one of $\bar{p}$ or $\bar{q}$ is 6, say $\bar{q} = 6$, project to $(\mathbb{Z}/p * \mathbb{Z}/(\frac{1}{2}q))/\langle w_1^r \rangle$. Here w_1 is the image of w under the natural homomorphism $\mathbb{Z}/p * \mathbb{Z}/q \to \mathbb{Z}/p * \mathbb{Z}/(\frac{1}{2}q)$. It is not hard to show that w_1 projects to an element of order 3 in $\mathbb{Z}/(\frac{1}{2}q)$. Thus this image group is indeed one of those previously considered.

Next suppose $(\bar{p}, \bar{q}, r) = (2,2,2)$. We may construct a representation $\rho : (\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle \to \mathrm{SO}(3)$ with noncyclic image such that $\rho(x)$, $\rho(y)$, and $\rho(w)$ have orders p, q and r respectively. Now as $r = 2$, both $p \geq 3$ and $q \geq 3$. Thus π, the image of ρ, is not dihedral. But $\max\{p, q, r\} \geq 6$ so that π is not polyhedral either. It follows that π is infinite and therefore this case is done.

To complete the proof it suffices to show that if $(\bar{p}, \bar{q}, r)$ is a permutation of $(2,4,4)$, then the quotient $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle$ is infinite, while if $(\bar{p}, \bar{q}, r)$ is a permutation of either $(2,3,6)$, $(2,4,6)$ or $(2,6,6)$, then $(p, q, r) = (\bar{p}, \bar{q}, r)$. As each of these is handled similarly, we shall restrict ourselves to providing the details for $(\bar{p}, \bar{q}, r) = (4,4,2)$ and indicating the changes necessary for the rest.

If $(\bar{p}, \bar{q}, r) = (4,4,2)$, let $w_1 \in \mathbb{Z}/p * \mathbb{Z}/(\frac{1}{2}q)$ be the image of w under the natural surjection. As w_1 projects to an element of order 2 in $\mathbb{Z}/(\frac{1}{2}q)$, we may choose a representation $\rho : (\mathbb{Z}/p * \mathbb{Z}/(\frac{1}{2}q))/\langle w_1^r \rangle \to \mathrm{SO}(3)$ as in the addendum. If both $p \geq 8$ and $q \geq 8$, then the image of ρ will be nondihedral and nonpolyhedral and thus infinite. At least one of p and q is larger than 7 so we have yet to check $(p, q, r) = (4,8,2)$ and $(p, q, r) = (8,4,2)$. But in either of these cases, the natural map $\mathbb{Z}/p * \mathbb{Z}/q \to \mathbb{Z}/2 * \mathbb{Z}/2$ sends w to some w_1 which abelianizes to $(1,0) \in \mathbb{Z}/2 \oplus \mathbb{Z}/2$ or $(0,1) \in \mathbb{Z}/2 \oplus \mathbb{Z}/2$. Such elements w_1 are of order 2 in $\mathbb{Z}/2 * \mathbb{Z}/2$ and thus $(\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^2 \rangle \twoheadrightarrow \mathbb{Z}/2 * \mathbb{Z}/2$. Evidently this finishes this case.

When $(\bar{p}, \bar{q}, r)$ is a permutation of $(2,3,6)$, $(2,4,6)$ or $(2,6,6)$, one can argue as above to reduce to just a few the number of possibilities for (p, q, r). In the latter two cases, those triples with $(p, q, r) \neq (\bar{p}, \bar{q}, r)$ give groups which admit surjections onto $\mathbb{Z}/2 * \mathbb{Z}/2$, and which are therefore infinite. In the first case, the addendum is used to construct representations from the groups corresponding to those triples with $(p, q, r) \neq (\bar{p}, \bar{q}, r)$ to SO(3). These are shown to have image either infinite, the dihedral group D_4, or the symmetric group S_4. The last two possibilities are excluded by studying the image of w.

The proof of Theorem 2 is now complete. □

Proof of Theorem 3. First we note that consideration of the projections of P onto $A_i * A_j$ $(i \neq j)$ shows that we need only examine the case $n = 2$.

Next let $w \in P = A_1 * A_2$ project to $a_i \in A_i$ $(i = 1, 2)$. Now if $a_i = e$, A_i will include in $P/\langle w^r \rangle$ (simply abelianize). Thus we shall assume below that a_1 and a_2 are nontrivial.

Suppose, as a first case, that $A_1 \cong \mathbb{Z}/p$ and $A_2 \cong \mathbb{Z}/q$ where p and q are prime powers. Let r_1 be a prime power dividing r. Using the addendum to Theorem 1 and Remark 2.3, we see that the compositions

$$\mathbb{Z}/p, \mathbb{Z}/q \to (\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^r \rangle \to (\mathbb{Z}/p * \mathbb{Z}/q)/\langle w^{r_1} \rangle$$

are injections. Thus the theorem holds in this first instance.

Next suppose that A_1 and A_2 are arbitrary. Let B_i be the subgroup of A_i generated by those of its elements occurring in w $(i = 1, 2)$. Clearly we may consider $w \in B_1 * B_2$ and w projects to $a_i \in B_i \backslash \{e\}$. If we can prove that each B_i injects into $(B_1 * B_2)/\langle w^r \rangle$ ($\langle w^r \rangle$ also denoting the normal closure of w^r in $B_1 * B_2$), then the identity

$$(A_1 * A_2)/\langle w^r \rangle \cong A_1 \underset{B_1}{*} (B_1 * B_2/\langle w^r \rangle) \underset{B_2}{*} A_2$$

shows that the general case of the theorem holds.

Now for any element $b_1 \in B_1 \backslash \{e\}$, we may choose surjections $\phi_i : B_i \to \mathbb{Z}/p_i$ $(i = 1, 2)$, where the p_i are prime powers and $\phi_1(b_1) \neq e$, $\phi_2(a_2) \neq e$ (this uses the fact that B_1 and B_2 are finitely generated). Clearly $\bar{w} = (\phi_1 * \phi_2)(w)$ projects to $\phi_2(a_2) \in \mathbb{Z}/p_2 \backslash \{e\}$. From above, this implies that $\mathbb{Z}/p_1$ injects into $(\mathbb{Z}/p_1 * \mathbb{Z}/p_2)/\langle \bar{w}^r \rangle$ (whether or not $\phi_1(a_1)$, the projection of $\bar{w}$ in $\mathbb{Z}/p_1$, is trivial). In particular, $\phi_1(b_1)$ is nontrivial there, and thus b_1 is nontrivial in $(B_1 * B_2)/\langle w^r \rangle$. As b_1 was arbitrary, B_1 injects into $(B_1 * B_2)/\langle w^r \rangle$. Similarly B_2 does. The proof of Theorem 3 is now complete. □

3. Topological applications

In this final section we discuss more fully the topological applications of Theorem 1.

Consider the following two statements:

(*) If K is a knot and $a/b \in \mathbb{Q} \cup \{1/0\}$ is such that $M(K, a/b)$ is reducible, then $b = \pm 1$.

(**) If K is a knot and $a/b \in \mathbb{Q} \cup \{1/0\}$ is such that $M(K, a/b) \cong L(p, s) \# L(q, t)$ $(p, q \geq 2)$, then $b = \pm 1$.

Clearly (*) implies (**).

That (*) was true had been suspected for some time and various restrictions on the surgery coefficients a/b which yield reducible $M(K, a/b)$ were known (see [8, §8] and [7, Theorem 1.11] for instance).

In the paper [6], González-Acuña and Short made the key observation that if $\pi_1(M(K, a/b))$ splits as a nontrivial free product, then it is normally generated by the bth power of one of its elements (Proposition 4.2). Then, using Rourke's version of small-cancellation theory [14], they showed that this could only occur if $|b| < 6$ (Theorem (4.3)). Later, Howie improved that to $|b| < 4$ [11].

Now suppose that $M(K, a/b) \cong M_1 \# M_2$ where $H_1(M_i) \not\cong 0$ $(i = 1, 2)$. From [6], $\pi_1(M_1) * \pi_1(M_2)$ is normally generated by a bth power, and as the same is necessarily true for the free product of any quotients of $\pi_1(M_1)$ and $\pi_1(M_2)$, Theorem 1 implies that $b = \pm 1$. Thus Corollary 5 holds, and so in particular, statement (**) is true.

Now Gordon and Luecke [9] observed that it is an immediate consequence of [3, Theorem 2.0.3] that statement (**) implies statement (*). Thus (*) holds.

Next we turn our attention to the problem of determining which connected sums of lens spaces can occur as the result of an integral Dehn surgery on a knot in S^3. That such connected sums do occur is well known [5, 7, 12].

For a torsion class $\alpha \in H_1(M)$, M a closed, oriented 3-manifold, let $\lambda(\alpha) \in \mathbb{Q}/\mathbb{Z}$ denote its self-linking number.

Lemma 3.1. *Suppose* $M(K, a/b) = M_1 \# M_2$ *where* $M_i \not\cong S^3$ $(i = 1, 2)$ *and* $a \neq 0$. *Then if* $\alpha_i \in H_1(M_i)$ *is a generator, there is an integer* u *relatively prime to* a *such that* $\lambda(\alpha_1) + \lambda(\alpha_2) \equiv \pm(u^2/a)$.

Proof. First we remark that $H_1(M(K, a/b)) \cong \mathbb{Z}/a$ and so both $H_1(M_1)$ and $H_1(M_2)$ are cyclic.

Next note that as $M(K, a/b)$ is reducible, $b = \pm 1$.

Now $\alpha = \alpha_1 + \alpha_2 \in H_1(M(K, \pm a))$ generates and thus there is a $u \in \mathbb{Z}$, relatively prime to a, such that $\alpha = u\mu$, where $\mu \in H_1(M(K, \pm a))$ is the class corresponding to a meridian of K.

It is well known, and easy to verify, that $\lambda(\mu) \equiv \pm 1/a$. Hence

$$\lambda(\alpha_1) + \lambda(\alpha_2) \equiv \lambda(\alpha) \equiv u^2 \lambda(\mu) \equiv \frac{\pm u^2}{a}.$$

Thus we are done. □

Proof of Proposition 6. There are generators $\alpha_1 \in H_1(L(p,s))$ and $\alpha_2 \in H_1(L(q,t))$ such that $\lambda(\alpha_1) \equiv -s/p$ and $\lambda(\alpha_2) \equiv -t/q$ (see [15, p. 290]). Then by Lemma 3.1, there is a number v, relatively prime to pq, and an $\varepsilon \in \{\pm 1\}$, so that

$$\frac{s}{p} + \frac{t}{q} \equiv \frac{\varepsilon v^2}{pq} .$$

Then $qs + pt \equiv \varepsilon v^2 \pmod{pq}$ and so

$$\begin{cases} s \equiv \varepsilon v^2 q^{-1} & (\operatorname{mod} p) , \\ t \equiv \varepsilon v^2 p^{-1} & (\operatorname{mod} q) . \end{cases}$$

Hence

$$\begin{aligned} L(p,s) &\cong L(p, \varepsilon v^2 q^{-1}) \\ &\cong \varepsilon L(p, u^2 q) \end{aligned}$$

where u is chosen so that $uv \equiv 1 \pmod{pq}$ (see [2, §5] for the classification of lens spaces).

Similarly

$$L(q,t) \cong \varepsilon L(q, u^2 p) .$$

The proof is now complete. □

References

[1] G. Baumslag, J. Morgan and P. Shalen, Generalised triangle groups, Preprint.
[2] M.M. Cohen, A. Course in Simple Homotopy Theory, Graduate Texts in Mathematics 10 (Springer, Berlin, 1970).
[3] M. Culler, C. Gordon, J. Luecke and P. Shalen, Dehn surgery on knots, M.S.R.I. Preprint, 1985.
[4] B. Fine, J. Howie and G. Rosenberger, One relator quotients and free products of cyclics, Preprint.
[5] R. Fintushel and R. Stern, Constructing lens spaces by surgery on knots, Math. Z. 175 (1980) 33–51.
[6] F. González-Acuña and H. Short, Knot surgery and primeness, Math. Proc. Cambridge Philos. Soc. 99 (1986) 89–102.
[7] C. McA. Gordon, Dehn surgery and satellite knots, Trans. Amer. Math. Soc. 275 (1983) 687–708.
[8] C. McA. Gordon and R.A. Litherland, Incompressible planar surfaces in 3-manifolds, Topology Appl. 18 (1984) 121–144.
[9] C. McA. Gordon and J. Luecke, Only integral Dehn surgeries can yield reducible manifolds, Preprint.
[10] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers (Oxford University Press, Oxford, 4th ed., 1960).
[11] J. Howie, The quotient of a free product of groups by a single high-powered relator, Preprint.
[12] L. Moser, Elementary surgery along a torus knot, Pacific J. Math. 38 (1971) 737–745.
[13] D. Rolfsen, Knots and Links (Publish or Perish, Berkeley, CA, 1976).
[14] C.P. Rourke, Presentations of the trivial group, in: Topology of Low-Dimensional Manifolds, Lecture Notes in Mathematics 722 (Springer, Berlin, 1979) 134–143.
[15] H. Seifert and W. Threlfall, A Textbook of Topology (Academic Press, New York, 1980).
[16] J. Wolf, Spaces of Constant Curvature (Publish or Perish, Boston, MA, 1974).