EXTENDING FREE CYCLIC ACTIONS ON SPHERES

BY

JOHN EWING

ABSTRACT. Connolly and Geist have reduced the problem of determining which free cyclic actions on spheres extend to free actions of specified supergroups to a problem involving a certain transfer map. In this note we develop some algebraic tools for calculating the transfer and show that some cyclic actions do *not* extend to certain supergroups.

1. Introduction. Suppose we are given a finite group G, a subgroup $H \subset G$, and a specific free action of H on the sphere S^{2N+1}. A fundamental problem is to decide whether the specified action of H extends to a free action of G on S^{2N+1}. (Of course, G must be a group which *can* act freely on the sphere.) In case G and H are cyclic groups (and $N \geq 2$), Connolly and Geist [1] have completely solved the problem. Specifically, given positive integers h and k let $C(k)$ and $C(hk)$ denote the cyclic groups of orders k and hk, respectively. They show that a free action of $C(k)$ on S^{2N+1} ($N \geq 2$) extends to a free action of $C(hk)$ if and only if the Reidemeister torsion of the $C(k)$ action is in the image of a certain transfer map (see §2).

It is, however, a solution which requires some elucidation, for, as the authors point out, there are some algebraic difficulties in deciding when the Reidemeister torsion *is* in the image of the transfer. Indeed, the question of whether or not *all* free actions of finite cyclic groups on S^{2N+1} ($N \geq 2$) extend to *all* finite cyclic supergroups is left unsettled by their work. Connolly and Geist note that the evidence suggests that this is the case.

The present paper is intended as an algebraic appendix to [1] which will *partially* resolve some of the algebraic difficulties associated with the transfer. We shall concentrate on the case of cyclic p-groups, where p is prime, but many of the techniques we employ are applicable to the general case.

Our main result is the following.

THEOREM 1.1. *Let p be a prime and let n be a positive integer satisfying*:
(i) $n \geq 4$ *if* $p = 2$,
(ii) $n \geq 3$ *if* $p = 3$,
(iii) $n \geq 2$ *if* $p \geq 5$.
Then for any $N \geq 2$, there exists a free $C(p^n)$ action on S^{2N+1} which does not extend to a free $C(p^{n+1})$ action.

In fact it will be evident from the proof of Theorem 1.1 that in the cases $p = 2$ and $n = 2$ or 3, or $p = 3$ and $n = 2$, every free $C(p^n)$ action *does* extend to a $C(p^{n+1})$ action. The question of whether or not every $C(p)$ action extends to a $C(p^2)$ action is equivalent to a very difficult problem in number theory (see [1] or Observation 3.3). In this connection, it turns out that every free $C(p)$ action extends to a $C(p^2)$ action on S^{2N+1} ($N \geqslant 2$) if p is *semiregular*; that is, p does not divide h_2, the second factor of the class number of the pth cyclotomic field. It is known that all primes $p < 125{,}000$ are semiregular and it is a famous conjecture of Vandiver that all primes are semiregular. Thus, it seems entirely likely that all free $C(p)$ actions on S^{2N+1} *do* extend to $C(p^2)$ actions, which is in sharp contrast to the situation for $n > 1$. The pleasant feature of our work for higher powers of p is that we can entirely circumvent these rather intractable problems in number theory.

The author would like to thank Frank Connolly for many valuable conversations about this work.

2. The main result of Connolly and Geist. We will indicate an action of a finite group G on sphere S^{2N+1} as a map $\mu: G \times S^{2N+1} \to S^{2N+1}$. As in Milnor [3], the Reidemeister torsion $\Delta(\mu)$ of an action μ is a unit in the ring $Q(G)/\langle \Sigma \rangle$, where Σ denotes the sum of the elements of G.

If $G = C(k)$, the cyclic group of order k, then there is a "standard" action μ_0 on S^{2N+1} given by

$$\mu_0\big(T, (z_0, z_1, \ldots, z_N)\big) = \exp(2\pi i/k)(z_0, z_1, \ldots, z_N),$$

where T is a chosen generator for $C(k)$. Comparing an arbitrary action μ with the standard action μ_0, we obtain $\Delta(\mu)/\Delta(\mu_0) = u$, a unit in the ring $R(k) = Z[C(k)]/\langle \Sigma \rangle$. The unit u is called the "associated unit" of the action μ. Of course, for any action μ, the associated unit depends on certain choices, and is therefore only well-defined modulo the subgroup $\langle \pm C(k) \rangle \subset R(k)^*$.

The associated unit measures the simple homotopy type of the orbit space of the action. The following result of Wall [5, 14. E. 3] is fundamental to what follows.

PROOF 2.1. *Given any positive integer k and any unit $u \in R(k)^*$, there exists a cellular free action μ on a finite complex of the homotopy type of S^{2N+1} ($N \geqslant 2$) such that the associated unit of μ is u modulo $\langle \pm C(k) \rangle$.*

From now on we let T denote a distinguished generator of $C(hk)$, and we identify $C(k)$ with the subgroup of $C(hk)$ generated by T^h.

Given positive integers k and h Connolly and Geist [1] defined a transfer map tr: $R(hk)^* \to R(k)^*$ and proved the following result.

THEOREM 2.2. *Let $\bar{\mu}$ be a free action of $C(k)$ on S^{2N+1} ($N \geqslant 2$) with associated unit $\bar{u} \in R(k)^*$. Then $\bar{\mu}$ extends to an action μ of $C(hk)$ on S^{2N+1} with associated unit $u \in R(hk)^*$ if and only if $\mathrm{tr}(u) = \bar{u}$ modulo $\langle \pm C(k) \rangle$.*

The description of the transfer map given by Connolly and Geist is perfectly general, for any finite group on the level of K_1. Here is a specifec interpretation for *cyclic* groups $C(k)$ and $C(hk)$.

Let $\mathbf{Z}[x]$ denote the polynomial ring in a single indeterminant x, and let

$$\Sigma = 1 + x + x^2 + \cdots + x^{hk-1}$$

and

$$\overline{\Sigma} = 1 + x^h + x^{2h} + \cdots + x^{(k-1)h}.$$

By mapping the distinguished generators to x and x^h, respectively, we may identify

$$R(hk) = \mathbf{Z}[x]/\langle \Sigma \rangle \quad \text{and} \quad R(k) = \mathbf{Z}[x^h]/\langle \overline{\Sigma} \rangle.$$

In order to define tr: $R(hk)^* \to R(k)^*$ we employ the "intermediate" ring $R(h; k) = \mathbf{Z}[x]/\langle \overline{\Sigma} \rangle$. Clearly there is a projection π: $R(hk) \to R(h; k)$ and an inclusion i: $R(k) \to R(h; k)$. In fact, it is easy to see that $R(h; k)$ is a free $R(k)$ module with basis, say, $\{1, x, x^2, \ldots, x^{h-1}\}$.

Given any element $v \in R(h; k)$, left multiplication by v induces an $R(k)$-linear transformation of $R(h; k)$ to itself. We define the norm $N(v) \in R(k)$ to be the determinant of this transformation.

Finally, given a unit $u \in R(hk)^*$, we define

$$\mathrm{tr}(u) = N(\pi(u)) \in R(k)^*.$$

3. Some observations. We now make some elementary observations which follow directly from the definition of the transfer and Theorem 2.2. Let h and k be positive integers.

Observation 3.1. By explicitly calculating the norm it is easy to see that, $\mathrm{tr}(x) = (-1)^{h+1}x^h \in R(k)^*$. It follows that the transfer map induces a map

$$\widetilde{\mathrm{tr}}: R(hk)^*/\langle \pm C(hk) \rangle \to R(k)^*/\langle \pm C(k) \rangle.$$

Of course, this is *really* the map we are concerned with in applying Theorem 2.2.

If h is odd then clearly $\langle \pm C(k) \rangle$ is contained in the image of tr, and consequently, $\widetilde{\mathrm{tr}}$ is onto if and only if tr is.

If h is even then -1 may not be contained in the image of tr. In this case, in order to show that $\widetilde{\mathrm{tr}}$ is *not* onto, one is obliged to produce a unit $u \in R(k)^*$ such that u *and* $-u$ are not in the image of tr.

Observation 3.2. Since $R(k)^*$ is not a subgroup of $R(hk)^*$ it is reasonable to ask in what sense tr behaves as a transfer map. For example, is it true that for any $u \in R(k)^*$, $u^h \in \mathrm{Im}\{\mathrm{tr}: R(hk)^* \to R(k)^*\}$?

In case h divides k (or, more generally, when every prime dividing h also divides k), there is a simple "geometric" proof of this fact using Theorem 2.2. Given a unit $u \in R(k)^*$, we can produce a free $C(k)$ action on a sphere with associated unit u^h which *does* extend to a $C(hk)$ action. Start with a free action $\bar{\mu}$ of $C(k)$ on S^{2N+1} ($N \geqslant 2$) with associated unit u. If T and S are generators for $C(k)$ and $C(hk)$, respectively, then define an action μ of $C(hk)$ on the h-fold join of S^{2N+1} with itself by

$$\mu(S, t_1 x_1 \oplus \cdots \oplus t_h x_h) = t_h \bar{\mu}(T, x_h) \oplus t_1 x_1 \oplus \cdots \oplus t_{h-1} x_{h-1}.$$

Under the assumed hypothesis this is a free action of $C(hk)$ on $S^{2h(N+1)-1}$ whose restriction to $C(k)$ is the h-fold join of $\bar{\mu}$ with itself. By [5, 14. E. 8] we see that the

associated unit of this last action is precisely $u^h \in R(k)^*$. By Theorem 2.2 we can conclude that $u^h \in \text{Im(tr)}$ modulo $\langle \pm C(k) \rangle$. Finally, from Observation 3.1 we see that $u^h \in \text{Im}\{\text{tr}: R(hk)^* \to R(k)^*\}$.

Observation 3.3. The transfer is particularly easy when $h = k = p$, a prime. Here $R(p) = \mathbf{Z}[\zeta_0]$ and $R(p; p) = \mathbf{Z}[\zeta_1]$ where $\zeta_j = \exp(2\pi i/p^{j+1})$. The "norm" map is simply the usual norm $N: \mathbf{Z}[\zeta_1] \to \mathbf{Z}[\zeta_0]$.

It is an outstanding conjecture of Iwasawa [2] that the norm map is indeed always onto, and, in fact, it would follow from another outstanding conjecture of Vandiver that all primes are semiregular (see §1).

4. A formula for the transfer. As in §2, given positive integers h and k we may identify $R(hk)$ with $\mathbf{Z}[x]/\langle \Sigma \rangle$ and $R(k)$ with $\mathbf{Z}[x^h]/\langle \overline{\Sigma} \rangle$. Now that the transfer map is really just a "projection" of the norm map from $\mathbf{Z}[x]$ to $\mathbf{Z}[x^h]$. This will allow us to write down an explicit formula for the transfer in the sense that, given $u \in R(hk)^*$ and a representative polynomial $f(x) \in \mathbf{Z}[x]$, we write down a representative polynomial in $\mathbf{Z}[x^h]$ for $\text{tr}(u) \in R(k)^*$.

We first note that $\mathbf{Z}[x]$ is a free $\mathbf{Z}[x^h]$-module with basis $\{1, x, x^2, \dots, x^{h-1}\}$. Given any element $f \in \mathbf{Z}[x]$ left multiplication by f induces a $\mathbf{Z}[x^h]$-linear transformation of $\mathbf{Z}[x]$. We can define the norm $N(f) \in \mathbf{Z}[x^h]$ to be the determinant of the matrix of this transformation.

If $u \in R(hk)^*$ and $f \in \mathbf{Z}[x]$ is a representative for u, then it is easy to see from the definition of the transfer that $N(f) \in \mathbf{Z}[x^h]$ is a representative for $\text{tr}(u) \in R(k)^*$.

Now suppose $f \in \mathbf{Z}[x]$ and write $f = \sum_{i=0}^{h-1} A_i x^i$ where $A_i \in \mathbf{Z}[x^h]$ for $0 \leqslant i < h$. With respect to the basis $\{1, x, x^2, \dots, x^{h-1}\}$, left multiplication by f corresponds to the matrix

$$M = \begin{pmatrix} A_0 & x^h A_{h-1} & x^h A_{h-2} & & x^h A_1 \\ A_1 & A_0 & x^h A_{h-1} & & x^h A_2 \\ A_2 & A_1 & A_0 & \cdots & x^h A_3 \\ \vdots & \vdots & \vdots & & \vdots \\ A_{h-1} & A_{h-2} & A_{h-3} & \cdots & A_0 \end{pmatrix}.$$

We can calculate the determinant of M as follows. Consider the matrix

$$T = \begin{pmatrix} 0 & 0 & & 0 & x^h \\ 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & & 1 & 0 \end{pmatrix}.$$

Over the field of rational functions $\mathbf{Q}(x)$ the characteristic polynomial of T is $X^h - x^h = 0$. It follows that the eigenvalues of T are

$$\{\zeta^j x \mid j = 0, 1, \dots, h-1\},$$

where $\zeta = \exp(2\pi i/h)$.

Now the matrix M can be written as $M = \sum_{i=0}^{h-1} A_i T^i$. Hence, the eigenvalues of M must be

$$\left\{ \sum_{1=0}^{h-1} A_i(\zeta^j x)^i \,|\, j = 0, 1, \ldots, h-1 \right\}.$$

We conclude that

$$\det(M) = \prod_{j=0}^{h-1} \sum_{i=0}^{h-1} A_i(\zeta^j x)^i.$$

Of course, for each i, $A_i(x)$ is a polynomial in x^h, and consequently $A_i(\zeta^j x) = A_i(x)$. It follows that if

$$f = \sum_{i=0}^{N} a_i x^i \in \mathbf{Z}[x],$$

then

$$N(f) = \prod_{j=0}^{h-1} \sum_{i=0}^{N} a_i(\zeta^j x)^i \in \mathbf{Z}[x^h].$$

We summarize our results in the following proposition.

PROPOSITION 4.1. *Given $u \in R(hk)^*$ suppose $f = \sum_{i=0}^{N} a_i x^i$ is a representative for u in $\mathbf{Z}[x]$. Then*

$$\prod_{j=0}^{h-1} \sum_{i=0}^{N} a_i(\zeta^j x)^i$$

is a representative for $\mathrm{tr}(u)$ *in* $\mathbf{Z}[x^h]$, *where $\zeta = \exp(2\pi i/h)$.* □

5. Some more observations. Using the "formula" of §4 we can make some further elementary observations about the transfer. As before, h and k are positive integers, tr: $R(hk)^* \to R(k)^*$ and N: $\mathbf{Z}[x] \to \mathbf{Z}[x^h]$.

Observation 5.1. Simply by inspecting the roots we notice that for any complex number α,

$$\prod_{j=0}^{h-1} (\zeta^j x - \alpha) = (-1)^{h-1}(x^h - \alpha^h).$$

It follows that for any $f \in \mathbf{Z}[x]$, if

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_t)$$

then

$$N(f) = a^h(-1)^{t(h-1)}(x^h - \alpha_1^h)(x^h - \alpha_2^h) \cdots (x^h - \alpha_t^h).$$

This, of course, allows us *in principle* to write down an even *more* explicit formula for $N(f)$, specifying its coefficients in terms of the coefficients of f.

Observation 5.2. For any positive integer n we define the group of "cyclotomic" units of $R(n)^*$ to be the group of units generated by units of the form $\pm x^t$ and

$(x^s - 1)/(x - 1)$, where $(s, n) = 1$. We have already observed that for tr: $R(hk)^* \to R(k)^*$, $\text{tr}(x) = (-1)^h x^h$. From Observation 5.1 we see that

$$\text{tr} \, \frac{x^s - 1}{x - 1} = \frac{x^{hs} - 1}{x^h - 1},$$

where $(s, hk) = 1$. We conclude that, modulo $\langle \pm 1 \rangle$ (as explained in Observation 3.1), the transfer maps the cyclotomic units of $R(hk)^*$ onto those of $R(k)^*$.

This is particularly significant when k is prime, since, in this case, the group of cyclotomic units of $R(k)^*$ has finite index, and, moreover, the index is precisely h_2, the second factor of the class number of $R(k)$.

We note that for all primes $k < 70$, $h_2 = 1$, and hence for these primes *every* $C(k)$ action extends to a $C(hk)$ action–no matter *what* h is!

Observation 5.3. There is an interesting filtration of the groups $R(hk)^*$ and $R(k)^*$. For any positive integer t define

$$R_t(hk)^* = \left\{ u \in R(hk)^* \mid u \equiv 1 \bmod h^t R(hk) \right\}.$$

The groups $R_t(k)^*$ are defined similarly.

Now the transfer respects this filtration in a rather strong way. Specifically, if $u \in R_t(hk)^*$ then $\text{tr}(u) \in R_{t+1}(k)^*$. To see this, we choose a representative for u of the form $f(x) = 1 + h^t g(x)$ where $g(x) \in \mathbf{Z}[x]$. Then from the formula of §4 we have

$$N(f) = \prod_{j=0}^{h-1} \left(1 + h^t g(\zeta^j x) \right)$$

$$= 1 + \sum_{j=0}^{h-1} h^t g(\zeta^j x) + h^{t+1} \cdot (\text{stuff}).$$

Using the fact that

$$\sum_{j=0}^{h-1} \zeta^{ij} = \begin{cases} 0 & \text{if } h \nmid i, \\ h & \text{if } h \mid i, \end{cases}$$

we see that $\sum_{j=0}^{h-1} g(\zeta^j x)$ is divisible by h. Consequently, $N(f) \equiv 1 \bmod h^{t+1}$ and, projecting onto $R(k)$, we have our result.

This will be a key observation for proving Theorem 1.1.

6. Cyclic p-groups. We now restrict our attention to cyclic p-groups for a fixed prime p. Throughout this section we let

$\zeta_n = \exp(2\pi i/p^{n+1})$,
$\lambda_n = \zeta_n - 1$,
$\Sigma_n = (x^{p^{n+1}} - 1)/(x - 1) \in \mathbf{Z}[x]$, and
$\Phi_n = (x^{p^{n+1}} - 1)/(x^{p^n} - 1) \in \mathbf{Z}[x]$.

Of course, Φ_n is the p^{n+1}st cyclotomic polynomial and so we may identify $\mathbf{Z}[x]/\langle \Phi_n \rangle$ with $\mathbf{Z}[\zeta_n]$ by sending x to ζ_n.

Now for any positive integer n we can provide an inductive description of $R(p^{n+1})^*$. As before, having chosen a generator for $C(p^{n+1})$ we may identify

$R(p^{n+1})$ with $\mathbf{Z}[x]/\langle\Sigma_n\rangle$. By factoring $\Sigma_n = \Sigma_{n-1}\cdot\Phi_n$ and noting that $\langle\Sigma_{n-1}\rangle\cap$ $\langle\Phi_n\rangle = \{0\}$ we obtain a pull-back diagram:

$$
\begin{array}{ccc}
R(p^{n+1}) & \overset{i_2}{\to} & \mathbf{Z}[\zeta_n] \\
i_1\downarrow & & \downarrow j_2 \\
R(p^n) & \overset{j_1}{\to} & \mathbf{Z}[x]/\langle\Phi_n\rangle + \langle\Sigma_{n-1}\rangle
\end{array}
$$

where all maps are the obvious projections.

We need to identify the term $\mathbf{Z}[x]/\langle\Phi_n\rangle + \langle\Sigma_{n-1}\rangle$. On the one hand, it is evident that $i_1(\Phi_n) = p \in R(p^n)$. Consequently, $\mathbf{Z}[x]/\langle\Phi_n\rangle + \langle\Sigma_{n-1}\rangle = R(p^n)/\langle p\rangle$ and j_1 is simply reduction mod p. On the other hand, $i_2(\Sigma_{n-1}) = (\zeta_n^{p^n} - 1)/(\zeta_n - 1) \in \mathbf{Z}[\zeta_n]$. A standard argument shows that $\langle(\zeta_n^{p^n} - 1)/(\zeta_n - 1)\rangle = \langle\lambda_n^{p^{n-1}}\rangle$ in $\mathbf{Z}[\zeta_n]$. Hence $\mathbf{Z}[x]/\langle\Phi_n\rangle + \langle\Sigma_{n-1}\rangle = \mathbf{Z}[\zeta_n]/\langle\lambda_n^{p^{n-1}}\rangle$ and j_2 is just reduction modulo $\langle\lambda_n^{p^{n-1}}\rangle$.

In the usual way, the pull-back diagram above induces an exact sequence of unit groups

$$1 \to R(p^{n+1})^* \overset{i}{\to} R(p^n)^* \times \mathbf{Z}[\zeta_n] \overset{j}{\to} (R(p^n)/\langle p\rangle)^*,$$

where $i(u) = (i_1(u), i_2(u))$ and $j(u_1, u_2) = j_1(u_1)j_2(u_2^{-1})$. In particular, $(u_1, u_2) \in R(p^n)^* \times \mathbf{Z}[\zeta_n]^*$ is in the image of i if and only if $j_1(u_1) = j_2(u_2)$ in $R(p^n)/\langle p\rangle$. In this case we say (u_1, u_2) represents a unit of $R(p^{n+1})^*$.

REMARK 6.1. Of course we may repeat the process above to obtain an embedding

$$R(p^{n+1})^* \to \prod_{k=0}^{n} \mathbf{Z}[\zeta_k]^*.$$

However, for large n it is rather difficult to give a practical description of the image of this embedding.

Now, returning to the definition of the transfer from §2, we see that for $n > 1$ the following diagram commutes:

$$
\begin{array}{ccc}
R(p^{n+1})^* & \overset{i}{\to} & R(p^n)^* \times \mathbf{Z}[\zeta_n]^* \\
\mathrm{tr}\downarrow & & \downarrow \mathrm{tr} \times N_n \\
R(p^n)^* & \overset{i}{\to} & R(p^{n-1})^* \times \mathbf{Z}[\zeta_{n-1}]
\end{array}
$$

where $N_n: \mathbf{Z}[\zeta_n]^* \to \mathbf{Z}[\zeta_{n-1}]^*$ is the norm map. We shall use this diagram to reduce the problem of determining when $\mathrm{tr}: R(p^{n+1})^* \to R(p^n)^*$ is onto to a similar problem one stage further down. First, we require a lemma and some notation.

LEMMA 6.2. *Suppose* $v \in \mathbf{Z}[\zeta_n]^*$. *Then* $N_n(v) \equiv 1 \bmod(\lambda_{n-1}^{p^{n-1}})$ *if and only if* $v \equiv 1 \bmod \lambda_n^{p^{n-1}}$. $\square$

This is due to Serre [4, V. 3] and the proof will not be repeated here.

Notation. For any positive integer n let

$$R_1(p^n)^* = \{u \in R(p^n)^* \mid u \equiv 1 \bmod(p)\}.$$

We note that by Observation 5.3, if $u \in R_1(p^n)^*$ then $\mathrm{tr}(u) \in R_1(p^{n-1})^*$; indeed, it is evident that even more can be said about $\mathrm{tr}(u)$.

THEOREM 6.3. *Suppose $n > 1$. The map* $\mathrm{tr}: R(p^{n+1})^* \to R(p^n)^*$ *is onto only if* $\mathrm{tr} \mid :$ $R_1(p^n)^* \to R_1(p^{n-1})^*$ *is onto. If p is semiregular then the converse is true as well.*

PROOF. Suppose $\mathrm{tr}: R(p^{n+1})^* \to R(p^n)^*$ is onto and consider $u \in R_1(p^{n-1})^*$. From the remarks made above we see that $(u, 1) \in R_1(p^{n-1})^* \times \mathbf{Z}[\zeta_{n-1}]^*$ represents a unit of $R(p^n)^*$. Hence, there is a unit $v \in R(p^{n+1})^*$ with $i(v) = (v_1, v_2) \in R(p^n)^* \times \mathbf{Z}[\zeta_n]$ such that $\mathrm{tr}(v_1) = u$ and $N_n(v_2) = 1$. By Lemma 6.2 we conclude that $v_2 \equiv 1 \bmod(\lambda_n^{p^{n-1}})$ and therefore $v_2 \equiv 1 \bmod p$. Since (v_1, v_2) represents a unit of $R(p^{n+1})^*$ we see that $v_1 \equiv 1 \bmod p$; that is, $v_1 \in R_1(p^n)^*$. Hence $\mathrm{tr} \mid : R_1(p^n)^* \to R_1(p^{n-1})^*$ is onto.

To prove the converse, in case p is semiregular, we combine Observations 3.2 and 5.2. From the first, we see that the index of $\mathrm{Im}(\mathrm{tr})$ in $R(p^n)^*$ is a power of p. To use the second observation we note that the "cyclotomic" units of $R(p^n)^*$ map onto the cyclotomic units of $\mathbf{Z}[\zeta_{n-1}]^*$. Since p is semiregular, the index of these cyclotomic units in $\mathbf{Z}[\zeta_{n-1}]^*$ is relatively prime to p. Now given $(u_1, u_2) \in R(p^{n-1})^* \times \mathbf{Z}[\zeta_{n-1}]^*$, representing a unit of $R(p^n)^*$, suppose u_2^k is cyclotomic for some integer $k \not\equiv 0 \bmod p$. From Observation 5.2 we see that modulo the image of tr, (u_1^k, u_2^k) is congruent to a unit of the form $(v, 1) \in R(p^{n-1})^* \times \mathbf{Z}[\zeta_{n-1}]^*$, where of course $v \in R_1(p^{n-1})^*$. Since $\mathrm{tr} \mid : R_1(p^n)^* \to R_1(p^{n-1})^*$ is onto, we conclude that $(u_1^k, u_2^k) \in \mathrm{Im}(\mathrm{tr})$. Since $k \not\equiv 0 \bmod p$ we see that $(u_1, u_2) \in \mathrm{Im}(\mathrm{tr})$, and hence $\mathrm{tr}: R(p^{n+1})^* \to R(p^n)$ is onto. This concludes the proof.

7. The proof of Theorem 1.1.

The strategy for proving Theorem 1.1 is now evident. From the work of Connolly and Geist (Theorem 2.2), we need only to show that for the given values of n and p, $\mathrm{tr}: R(p^{n+1})^* \to R(p^n)^*$ is not onto. (In case $p = 2$, we need to show it is not onto modulo $\langle \pm 1 \rangle$, as explained in Observation 3.1.) From Theorem 6.3, it is enough to show that $\mathrm{tr}: R_1(p^n)^* \to R_1(p^{n-1})^*$ is not onto. But from Observation 5.3 we see that if $v \in R_1(p^n)^*$ then $\mathrm{tr}(v) \equiv 1 \bmod p^2$ in $R(p^{n-1})$. Hence, we will be done if we can produce a unit $u \in R_1(p^{n-1})^*$ such that $u \not\equiv 1 \bmod p^2$.

In what follows it will be convenient to shift our integer n by 1.

PROPOSITION 7.1. *Let p be a prime and n be a positive integer satisfying:*
(i) $n \geqslant 3$ *if $p = 2$,*
(ii) $n \geqslant 2$ *if $p = 3$,*
(iii) $n \geqslant 1$ *if $p \geqslant 5$.*
Then there is a unit $u \in R_1(p^n)^*$ such that $u \not\equiv 1 \bmod p^2$; and $u \not\equiv \pm 1 \bmod 4$ in case $p = 2$.

PROOF. We first consider the cases when p is odd. Consider the unit

$$u = (x + x^{-1})^{p^n(p-1)} \in R(p^n)^*,$$

where as usual we are identifying $R(p^n) = \mathbf{Z}[x]/\langle \Sigma_n \rangle$.

We first note that $(x + x^{-1})^{p^n} \equiv 2 \bmod p$, so that $u \in R_1(p^n)^*$.

To prove that $u \not\equiv 1 \bmod p^2$ it will be convenient to use the projection ϕ: $R(p^n) \to \mathbf{Z}[\zeta_{n-1}]$ given by $\phi(x) = \zeta_{n-1}$. Clearly it suffices to show that $\phi(u) \not\equiv 1 \bmod p^2$ in $\mathbf{Z}[\zeta_{n-1}]$.

Now in $\mathbf{Z}[\zeta_{n-1}]$ we know that $\langle p \rangle = \langle \lambda_{n-1}^{p^{n-1}(p-1)} \rangle$, where $\lambda_{n-1} = \zeta_{n-1} - 1$. Let ν denote the valuation associated to the prime λ_{n-1}. We must show that $\nu(\phi(u) - 1) < 2p^{n-1}(p-1)$.

Let $\xi = \zeta_{n-1} + \zeta_{n-1}^{-1}$, so that $\phi(u) = \xi^{p^n(p-1)}$. We may factor

$$\xi^{p^n(p-1)} - 1 = \prod_{j=0}^{p^n-1} \left(\xi^{p-1} - \zeta_{n-1}^j \right).$$

It is easy to check that $\nu(\xi^{p-1} - 1) = 2$, and that

$$\nu(\zeta_{n-1}^j - 1) = \begin{cases} \infty & \text{if } j = 0, \\ 1 & \text{if } p \nmid j, \\ > p^{n-1}(p-1) & \text{if } p \mid j. \end{cases}$$

Therefore, provided $p^{n-1}(p-1) > 2$, we see that

$$\nu\left(\xi^{p-1} - \zeta_{n-1}^j\right) = \begin{cases} 2 & \text{if } j = 0, \\ 1 & \text{if } 1 \leqslant j \leqslant p^n - 1. \end{cases}$$

It follows that $\nu(\xi^{p^n(p-1)} - 1) = p^n + 2$. Under the restrictions on n and p we see that $p^n + 2 < 2p^{n-1}(p-1)$. The proposition is therefore proved for p odd.

For $p = 2$ consider the unit

$$u = \left(x + x^2 + x^3\right)^{2^{n-1}} \in R(2^n)^*.$$

Letting $y = x^{2^{n-2}}$ we see that

$$\left(x + x^2 + x^3\right)^{2^{n-2}} \equiv y + y^2 + y^3 \quad \bmod 2.$$

Consequently.

$$u \equiv 1 + 2\left(1 + y + y^2 + y^3\right) \quad \bmod 4.$$

If $n \geqslant 3$ then it is easy to see that $1 + y + y^2 + y^3 \not\equiv 0$, $1 \bmod 2$ and hence $u \not\equiv \pm 1 \bmod 4$. The proof is now complete.

REMARK 7.2. It is easy to verify that in case $p = 2$ and $n = 1$ or 2, or $p = 3$ and $n = 1$, if $u \in R_2(p^n)^*$ then $u \equiv 1 \bmod p^2$. Indeed, one easily sees that tr: $R_1(p^{n+1})^* \to R_1(p^n)^*$ is onto in these cases; $R_1(p^n)$ simply contains too few units.

References

1. F. Connolly and R. Geist, *On extending free group actions on spheres and a conjecture of Iwasawa*, Trans. Amer. Math. Soc. (to appear).
2. K. Iwasawa, *On the theory of cyclotomic fields*, Ann. of Math. (2) **70** (1959).
3. J. Milnor, *Whitehead torsion*, Bull. Amer. Math. Soc. **72** (1966).
4. J-P. Serre, *Corps locaux*, Hermann, Paris, 1968.
5. C. T. C. Wall, *Surgery on compact manifolds*, Academic Press, New York, 1970.

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47405