NONTRIVIAL LOWER BOUNDS FOR CLASS GROUPS OF INTEGRAL GROUP RINGS

BY

STEPHEN V. ULLOM[1]

To Olga Taussky, for her support and encouragement

1. Introduction

The aim of this paper is to give general lower bounds for the order of a subgroup $T(ZG)$ of the locally free class group Cl (ZG). $T(ZG)$ is generated by certain locally free modules (see Section 2) which have been considered [10], [15], [17] for their applications in algebraic topology. The lower bounds are expressed in terms of an important invariant of G, namely the Artin exponent $A(G)$. By definition $A(G)$ is the characteristic of the Grothendieck ring $G_0(QG)$ modulo the ideal generated by the image of the induction map $G_0(QC) \rightarrow G_0(QG)$, where C ranges over cyclic subgroups of G (see [16] for details). One knows [8], [9] that $A(G)$ divides the order of G and equals one iff G is cyclic. Our results assert:

THEOREM. *An odd prime p divides the order of the subgroup $T(ZG)$ of* Cl (ZG) *iff p divides the Artin exponent $A(G)$. Also* 2 *divides order of $T(ZG)$ if* 4 *divides $A(G)$ (assuming a Sylow 2-group of G is not dihedral).*

The formal properties of $T(ZG)$ imply it maps onto $T(ZG_0)$, G_0 obtained from G by quotient and subgroups. It follows that the proof reduces to certain groups that are among those considered in Section 3; for these we have a complete determination of $T(ZG)$. In the final analysis all the computations depend on special properties of units in group rings and orders. Our approach allows us to strengthen and extend several known results for noncyclic G and to show a common thread running through the arguments.

2. Definitions and formal properties

Let R be the ring of algebraic integers in an algebraic number field K, Λ an R-order in a finite-dimensional semisimple K-algebra A. Given an R-lattice X and prime p of K, X_p denotes completion at p (if p is infinite, set $R_p = K_p$ and $X_p = K_pX$). The class group Cl Λ is the Grothendieck group of the category of locally free left Λ-modules modulo the subgroup generated by free Λ-modules; (X) denotes the class in Cl Λ of a locally free module X. To get a sufficiently

Received June 30, 1975.

[1] This research was partially supported by a National Science Foundation grant.

explicit description of class groups we use Fröhlich's approach via the idele class group [4].

Let $J(A)$ be the idele group[2] of A, $u(S)$ unit group of a ring S, $U(\Lambda) = \Pi u(\Lambda_p)$ product over all primes p of K, $J(A)'$ the closure of the commutator subgroup of $J(A)$ (where $J(A)$ is topologized by the condition that $U(\Lambda)$ be an open subgroup and $U(\Lambda)$ itself has the product topology). If $\alpha = (\alpha_p) \in J(A)$, then $\Lambda\alpha$ denotes the locally free left Λ-module

$$\Lambda\alpha = \bigcap_p (\Lambda_p \alpha_p \cap A).$$

Fröhlich proved $\alpha \to (\Lambda\alpha)$ induces an isomorphism

$$J(A)/J(A)'u(A)U(\Lambda) \to \mathrm{Cl}\,\Lambda. \tag{2.1}$$

Let $D(\Lambda)$ be the kernel of the extension of scalars map $\mathrm{Cl}\,\Lambda \to \mathrm{Cl}\,\Lambda'$, Λ' a maximal order of A containing Λ. Since all maximal R-orders in A are locally conjugate, it follows from (2.1) that $D(\Lambda)$ is independent of the choice of maximal order. Let Λ_0 be any R-order in A containing Λ. If $\Lambda\alpha \cong \Lambda\mu$, $\mu \in U(\Lambda_0)$, it follows at once from (2.1) that

$$(\Lambda\alpha) \in \mathrm{Ker}\,(\mathrm{Cl}\,\Lambda \to \mathrm{Cl}\,\Lambda_0). \tag{2.2}$$

Now let Λ = group ring RG; G group of order n; $\Sigma = \Sigma_G$, the sum of the elements of G. Form the fiber product of R-orders

$$\begin{array}{ccc} \Lambda & \xrightarrow{\Psi_1} & R \\ {\scriptstyle\Psi_2}\big\downarrow & & \big\downarrow{\scriptstyle\phi_1} \\ \Lambda/(\Sigma) & \xrightarrow[\phi_2]{} & R/nR, \end{array} \tag{2.3}$$

where Ψ_1 is the augmentation map, $\phi_2(\lambda \bmod (\Sigma)) = \Psi_1(\lambda) \bmod nR$, and Ψ_2, ϕ_1 are the quotient maps. Via (2.3) we shall often identify Λ with a subring of $\Gamma = R \times \Lambda/(\Sigma)$. The Λ-ideals $[r, \Sigma] = r\Lambda + \Sigma\Lambda$, where $r \in R$ is prime to n, will be used to produce nontrivial elements of the class group. The notation $a \mid b$ means that a divides b, and $a \nmid b$ is the negation.

(2.4) PROPOSITION. (i) *$[r, \Sigma]$ is a locally free RG-module equal to $\Lambda\alpha$, idele $\alpha \in J(K \times KG/(\Sigma))$, where*

$$\begin{aligned} \alpha_p &= 1 && \text{if } p \nmid r \\ &= (1, r) \in R_p \times \Lambda_p/(\Sigma) && \text{if } p \mid r. \end{aligned}$$

(ii) *$[r, \Sigma] \cong \Lambda\mu$, $\mu \in U(R \times \Lambda/(\Sigma))$, where $\mu_p = 1$ if $p \mid r$, $\mu_p = (r, 1)$ if $p \nmid r$. Hence $([r, \Sigma]) \in D(RG)$.*

Proof. (i) We must show $[r, \Sigma]_p = \Lambda_p \alpha_p$ for all primes p of K. If $p \nmid r$, then $r \in u(R_p)$ and so $[r, \Sigma]_p = \Lambda_p$. Assume $p \mid r$; then after the identification

[2] $J(A) = \{(\alpha_p) \in \prod u(A_p) : \alpha_p \in u(\Lambda_p)$ for all but finitely many $p\}$.

from (2.3), $\Lambda_p = \Gamma_p$. Moreover, r and $n^{-1}\Sigma \in [r, \Sigma]_p$ correspond to (r, r) and $(1, 0)$ respectively in Γ_p. It follows at once that $[r, \Sigma]_p$ is Λ_p-free on the generator $(1, r)$.

(ii) Define $\beta \in U(\Lambda)$ by $\beta_p = 1$ if $p \mid r$, $\beta_p = r$ if $p \nmid r$. Then $\alpha(1, r^{-1})\beta = \mu$ where we are viewing $(1, r^{-1})$ in $K \times KG/(\Sigma)$, hence $\Lambda\alpha \cong \Lambda\mu$. Use (2.2) to conclude $([r, \Sigma]) \in D(RG)$. *Q.E.D.*

From (2.3) we have an exact Mayer-Vietoris sequence [13, (1.10)] if KG satisfies the Eichler condition

$$(2.5) \qquad u(R) \times u(\Lambda/(\Sigma)) \longrightarrow u(R/nR) \xrightarrow{\partial} D(\Lambda) \longrightarrow D(\Gamma) \longrightarrow 0.$$

In all cases the sequence is exact [13, (1.12)] if the left hand term is replaced by $GL_2(R) \times GL_2(\Lambda/(\Sigma))$.

As an application of [4, XII] we explicate (2.5) in terms of idele groups: First identify $U(R/nR)$ with $u(R/nR)$. There are maps $\phi_1\colon U(R) \to U(R/nR)$, $\phi_2\colon U(\Lambda/(\Sigma)) \to U(R/nR)$ defined via the completions of the old ϕ_i at each p. Then

$$(2.6) \qquad \phi\colon \frac{U(R) \times U(\Lambda/(\Sigma))}{U(\Lambda)} \to u(R/nR),$$

where $\phi((\beta_1, \beta_2) \bmod U(\Lambda)) = \phi_1(\beta_1)\phi_2(\beta_2)^{-1}$ is a bijection between the cosets of the left hand side of (2.6) and the elements of $u(R/nR)$. Thus for the μ defined in (2.4) (ii),

$$\phi(\mu) = \phi_1(r)\phi_2(1)^{-1} = r \bmod nR.$$

After passing to quotients we obtain (also proved in [17]):

(2.7) PROPOSITION. *With the boundary map ∂ of* (2.5)

$$\partial(r \bmod nR) = ([r, \Sigma]).$$

Remark. Since r and Σ belong to $c(\Lambda)$, the center of Λ, we may consider the ideal $[r, \Sigma]_0$ generated by r and Σ in $c(\Lambda)$. Obviously $[r, \Sigma]$ is obtained from $[r, \Sigma]_0$ by extension of scalars. Propositions (2.4), (2.7) and fiber product (2.3) still hold when all orders are replaced by their centers. Note that $([r, \Sigma]_0) = 0$ in Cl $(c(\Lambda))$ is a sufficient condition for $([r, \Sigma]) = 0$ in Cl Λ. However, it is not necessary since if $\Lambda = ZG$, G dihedral group of order $2p$, then $D(c(\Lambda))$ has order $(p - 1)/2$ by [13] or [4a]. Further one can prove the elements of $D(c(\Lambda))$ have the form $([r, \Sigma]_0)$. On the other hand $D(\Lambda) = 0$ (see e.g., [13]).

Let $T(RG)$ be the subgroup of $D(RG)$ consisting of classes $([r, \Sigma])$, i.e., $T(RG) = \operatorname{im} \partial$. T has two important formal properties, analogous to the divisibility of the Artin exponent of G by the Artin exponent of any of its quotient or subgroups.

(2.8) *Quotient.* If $\bar{G}$ is a quotient of G, then the natural map Cl $RG \to$ Cl $R\bar{G}$ sends $([r, \Sigma_G])$ to $([r, \Sigma_{\bar{G}}])$, hence $T(RG)$ onto $T(R\bar{G})$.

(2.9) *Restriction.* If H is a subgroup of G, then res: Cl $RG \to$ Cl RH sends $([r, \Sigma_G])$ to $([r, \Sigma_H])$, hence $T(RG)$ onto $T(RH)$.

Proof of (2.8). The projection $KG \to K\bar{G}$ induces a map

$$\pi \colon K \times KG/(\Sigma_G) \to K \times K\bar{G}/(\Sigma_{\bar{G}}).$$

For the idele α of (2.4)(i) we have $R\bar{G} \otimes_{RG} RG\alpha \cong R\bar{G}\pi(\alpha)$, where π is now viewed as a map of idele groups. But $\pi(\alpha)_p = \pi_p(\alpha_p)$ equals $(1, r) \in R_p \times R_p\bar{G}/(\Sigma_{\bar{G}})$ if $p \mid r$ and equals 1 otherwise. Thus $R\bar{G}\pi(\alpha) = [r, \Sigma_{\bar{G}}]$.

Proof of (2.9). As an RH-module, $[r, \Sigma]$ is locally free of RH-rank $m = (G\colon H) \geq 2$. Let $s_1, \ldots, s_m$ be a system of right coset representatives of H in G, so $R_pG = R_pHs_1 + \cdots + R_pHs_m$ for all p. A left R_pH-basis of $[r, \Sigma]_p \cong R_pG\mu_p$ then is given by $s_1\mu_p, \ldots, s_m\mu_p$. If $p \mid r$, then $\mu_p = 1$. Assume $p \nmid r$; then $\mu_p = re + (1 - e)$ by (2.4) where

$$e = n^{-1}\Sigma_G = n^{-1}\Sigma_H(s_1 + \cdots + s_m).$$

It follows that

$$s_i\mu_p = s_i + \lambda(s_1 + \cdots + s_m), \quad \lambda = n^{-1}(r - 1)\Sigma_H \in K_pH.$$

Let $S^{(m)}$ denote the direct sum of m copies of a ring S and $M_m(S)$ denote the ring of all $m \times m$ matrices with entries in S. Then $R_pG\mu_p = (R_pH)^{(m)}\beta_p$; $\beta_p \in M_m(K_pH)$ has $1 + \lambda$ on the diagonal and λ elsewhere. We set $\beta_p = 1$ for $p \mid r$ and notice that $\beta = (\beta_p) \in J(M_m(KH))$. In other words, as RH-modules, $[r, \Sigma] \cong (RH)^{(m)}\beta$.

We shall transform β and use the one-one correspondence between isomorphism classes of locally free rank m RH-modules ($m \geq 2$) with elements $J(B)/J(B)'u(B)U(M_m(RH))$, by results D. and F. of [4]; here $B = M_m(KH)$. It is easy to see there are $\theta, \theta' \in U(M_m(RH))$ such that

$$\begin{aligned} \gamma_p = (\theta\beta\theta')_p &= 1 \qquad \text{if } p \mid r, \\ &= \begin{bmatrix} 1 + m\lambda & & \\ & 1 & \\ & & \ddots & \\ \lambda & & & 1 \end{bmatrix} \text{if } p \nmid r. \end{aligned}$$

Further if $p \nmid r$, then right multiplication of γ_p by the elementary matrix in $M_m(K_pH)$ with 1 on the diagonal, $-\lambda$ in the $(m, 1)$ position, and zeros elsewhere transforms γ_p to the diagonal matrix $(1 + m\lambda, 1, \ldots, 1)$. But any elementary matrix is a commutator, providing that $m \geq 3$. It follows that $[r, \Sigma_G] \cong RH\,\theta \oplus (RH)^{(m-1)}$, $m \geq 3$. Here $\theta \in J(KH)$ is defined by $\theta_p = 1$ if $p \mid r$, $\theta_p = 1 + m\lambda$ if $p \nmid r$; thus $RH\theta \cong [r, \Sigma_H]$. If $m = 2$, we replace $[r, \Sigma_G]$ by $[r, \Sigma_G] \oplus RG$ and follow the lines of the above proof to conclude

$$[r, \Sigma_G] \oplus RG \cong [r, \Sigma_H] \oplus (RH)^{(2m-1)}.$$

Therefore for all m the equation

$$\text{res}\,([r, \Sigma_G]) = ([r, \Sigma_H])$$

holds on the class group level.

Remark. When $R = Z$, one can give an alternative proof of (2.9) using Lemmas 6.1 and 6.2 of Swan [15].

In the remainder of the paper take $R = \mathbf{Z}$ in order to bring out the sharp distinction between the cyclic and noncyclic cases.

(2.10) PROPOSITION. (i) *$T(ZC) = 0$ if C is cyclic.*

(ii) *$T(ZG)$ is a quotient of $u(Z/nZ)/\{\pm 1\}$ where n is the order of G.*

(iii) *The exponent of $T(ZG)$ divides $A(G)$.*

Proof. Assertion (i) is well known, see e.g., [15], and (ii) follows at once from (2.5) and (2.7). To prove (iii) recall Cl (ZG) is a Frobenius module for the Frobenius functor $G_0(QG)$, see [16, chap. 2]. By Frobenius reciprocity in Cl (ZG)

$$(\text{ind } s) \circ y = \text{ind } (s \circ \text{res } y)$$

where we want $y \in T(ZG)$, $s \in G_0(QC)$, cyclic $C \subset G$, and ind and res are taken between C and G. But res $y = 0$ by (i) and thus (iii) follows.

(2.11) COROLLARY. *By restriction, $T(ZG)$ maps onto the cyclic group $\Pi T(ZG_p)$, product over all p-Sylow subgroups of G.*

Proof. First of all, $T(ZG_p)$ is a p-group by (2.10) (iii) and cyclic by (ii). For each p the restriction map $T(ZG) \to T(ZG_p)$ is onto and by the Chinese remainder theorem for $\mathbf{Z}$, the product of the restriction maps is onto.

Remark. Any automorphism of G extends to an automorphism of RG and Cl (RG). Obviously the ideal $[r, \Sigma]$ is invariant under all such automorphisms. The example G cyclic of order 16 shows that $T(ZG)$ can be a proper subgroup of those elements of $D(ZG)$ fixed by all automorphisms of G. In fact $D(ZG)$ has order 2 and $T(ZG) = 0$ by (2.10) (i).

3. Some special groups

Let C_n denote the cyclic group of order n and $|S|$ denote the cardinality of a set S.

(3.1) PROPOSITION. *Let G be elementary abelian of order p^{s+1}, p odd prime. $T(ZG)$ is cyclic of order p^s with generator* $([1 + p, \Sigma])$.

Proof. We shall use certain automorphisms of QG. Now $QG/(\Sigma) \cong k$ copies $F^{(k)}$ of the field $F = Q(1^{1/p})$, $k = (p^{s+1} - 1)/(p - 1)$. View $ZG/(\Sigma)$ as a subset of $F^{(k)}$ and thus $u \in u(ZG/(\Sigma))$ may be written $u = (u_1, \ldots, u_k)$, $u_i \in u(Z[1^{1/p}]a$.

For integers a prime to p, let σ_a be the automorphism of G given by $g \mapsto g^a$, $g \in G$. Every idempotent of QG is fixed by σ_a, and σ_a restricted to each F sends ω, p-th root of 1, to ω^a. Thus $N = \sigma_1 + \cdots + \sigma_{p-1}$ restricted to F is the norm from F to Q. It follows that $Nu = 1$, $u \in u(ZG/(\Sigma))$. However, for the map ϕ_2 defined in (2.3), $\phi_2(\sigma_a x) = \phi_2(x)$, $x \in ZG/(\Sigma)$. Thus $1 = \phi_2(Nu) = \phi_2(u)^{p-1}$. Since $T(ZG)$ is a p-group and $u(Z/nZ) \simeq C_{p-1} \times C_{p^s}$ with $1 + p$ generating C_{p^s}, we are done.

Remark. Let G_{s+1} be the elementary abelian p-group of order p^{s+1} with $G_{s+1} = G_s \times C_p$, C_p generated by g_{s+1}. Let Σ_s be the sum of the elements of G_s. We describe explicitly a unit u_{s+1} of $ZG_{s+1}/(\Sigma_{s+1})$ whose augmentation is congruent to $r^{p^s} \bmod p^{s+1}$ for given r prime to p (thus proving directly that $T(ZG_{s+1})$ is a p-group). Take $u_1 = 1 + g_1 + \cdots + g_1^{r-1}$ and define u_{s+1} inductively by

$$u_{s+1} = u_s + [(1 + g_s + \cdots + g_s^{r-1})^{p^s} - r^{p^{s-1}}]\Sigma_s/p^s.$$

Of course we are using the same notation for an element of ZG and its image in $ZG/(\Sigma)$.

The idea in the next three propositions is to write ZG as a fiber product of two orders Λ_1, Λ_2 with say $\Delta = \Lambda_1 \times \Lambda_2$ such that the image of $([r, \Sigma])$ in Cl Δ is zero, but $([r, \Sigma]) \neq 0$ for suitable r.

(3.2) PROPOSITION. *Let G be a noncyclic abelian group of order 2^{s+1} and exponent dividing 4. Then $T(ZG)$ is cyclic of order 2^{s-1} with generator* $([5, \Sigma])$.

Proof. Write $G = \langle y \rangle \times H$, y order $2f$, $f = 1$ or 2. Construct the ideals $I_1 = (y^f - 1)ZG$ and $I_2 = (y^f + 1)ZG$, and form the fiber product

$$(3.3) \qquad \begin{array}{ccc} ZG & \xrightarrow{\Psi_1} & ZG/I_1 \\ {\scriptstyle \Psi_2}\downarrow & & \downarrow{\scriptstyle \phi_1} \\ ZG/I_2 & \xrightarrow[\phi_2]{} & ZG/I_1 + I_2. \end{array}$$

We have $ZG/I_1 \cong ZG_0$ where $G_0 = \langle y^2 \rangle \times H$, $ZG/I_2 \cong RH$ where $R = Z[\omega]$, ω primitive $2f$-root of 1, and $ZG/I_1 + I_2 \cong \bar{Z}G_0$, $\bar{Z} = Z/2Z$.

Recall that $[r, \Sigma] \cong \Lambda\mu$, $\mu \in U(Z \times ZG/(\Sigma))$, where if $p \nmid r$, $\mu_p = (r, 1) = re + (1 - e)$, $e = n^{-1}\Sigma$. Now $\Psi_1(e) = 2n^{-1}\,\Sigma_{G_0}$ and $\Psi_2(e) = 0$. Take $r = 1 + n/2$ for the rest of this proof. We identify $re + (1 - e)$ with

$$(3.4) \qquad (\Psi_1(re + 1 - e), \Psi_2(re + 1 - e)) = (1 + \Sigma_{G_0}, 1) \in ZG_0 \times RH = \Delta$$

Since $1 + \Sigma_{G_0} \in u(Z_pG_0)$ for $p \nmid r$ and $\mu_p = 1$ if $p \mid r$, it follows that $\mu \in U(\Delta)$. Therefore in the exact sequence from (3.3),

$$u(\Delta) \xrightarrow{\phi} u(\bar{Z}G_0) \xrightarrow{\delta} D(ZG) \xrightarrow{f} D(\Delta) \longrightarrow 0,$$

$([r, \Sigma_G]) \in \ker f = \operatorname{im} \delta$. In fact $\delta(1 + \Sigma_{G_0}) = ([r, \Sigma_G])$ by (3.4) and an argument similar to the proof of (2.7).

But $u(\Delta)$ is torsion and [7] therefore consists of roots of 1 times elements of G_0 and H. Thus $1 + \Sigma_{G_0} \notin \operatorname{im} \phi$ if $|G_0| > 2$. Since 5 has order 2^{s-1} in $u(Z/2^{s+1}Z)$ and $5^{2^{s-2}} \equiv r \bmod 2^{s+1}$, we have proved $([5, \Sigma_G])$ has order 2^{s-1} in Cl (ZG).

(3.5) PROPOSITION. *Let H_{2^n} be the quaternion group of order 2^n defined by*

$$H_{2^n} = \langle x, y \mid x^{2^{n-2}} = y^2, \quad y^4 = 1, \quad yxy^{-1} = x^{-1} \rangle.$$

If $n \geq 3$, then $T(ZH) = D(ZH)$ has order 2 with generator $([r, \Sigma])$, $r \equiv \pm 3 \bmod 8$.

Proof. The case $n = 3$ was proved by Martinet [11]. For all $n \geq 3$, we know that $|D(ZH)| = 2$ by [5], so we take restriction from H_{2^n} to H_8 (compare [10]).

(3.6) PROPOSITION. *Let l be an odd prime, q any divisor of $l - 1$, and g a primitive qth root of 1 mod l. Let $\Omega(l, q)$ be the metacyclic group defined by*

$$\Omega(l, q) = \langle x, y \mid x^l = y^q = 1, yxy^{-1} = x^g \rangle.$$

Then $T(Z\Omega) = D_0(Z\Omega)$ is cyclic of order $q/(q, 2)$ where D_0, a subgroup of $D(Z\Omega)$, is defined in the proof below.

Proof. Let $I_1 = (x - 1)Z\Omega$, $I_2 = (x^{l-1} + \cdots + x + 1)Z\Omega$ be ideals of $Z\Omega = \Lambda$. Then $\Lambda/I_1 \cong ZC$ where C is cyclic of order q, $\Lambda/I_2 \cong R \circ C$ a twisted group ring where $R = Z[1^{1/l}]$, and $\Lambda/I_1 + I_2 \cong \bar{Z}C$, $\bar{Z} = Z/lZ$. Let $\Delta = ZC \times R \circ C$. The Mayer-Vietoris sequence arising from Λ as a fiber product reduces to [6]

$$u(R \circ C) \longrightarrow u(\bar{Z}C) \xrightarrow{\delta} D(\Lambda) \xrightarrow{f} D(\Delta) \longrightarrow 0$$

and $D_0(\Lambda) = \ker f$ by definition. Note $T(\Lambda) \subset D_0(\Lambda)$ by (2.8), (2.10), and the fact [6] that $D(R \circ C) = 0$. Take $r \equiv 1 \bmod q$; using $[r, \Sigma] \cong \Lambda\mu$, we have $\mu \in U(\Delta)$ since

$$1 + q^{-1}(r - 1)\Sigma_C \in u(Z_pC) \quad \text{if } p \nmid r.$$

As in the proof of (3.2), $\delta(1 + q^{-1}(r - 1)\Sigma_C) = ([r, \Sigma_\Omega])$. From [6],

$$\operatorname{im} \delta = u(\bar{Z}C)/\operatorname{im} u(R \circ C) \cong u(\bar{Z})/u(\bar{Z})^{q_2}, \quad q_2 = q/(q, 2),$$

the isomorphism given by the determinant map. In particular, $1 + q^{-1}(r - 1)\Sigma_C$ maps to r mod l. Therefore $T(Z\Omega) = \operatorname{im} \delta$.

We can now give short alternate proofs of some of the theorems of [2], [12], [14] and obtain the new result (3.8) (i).

(3.7) LEMMA. *Let $G = S_n$ (resp. A_n) be the symmetric (resp. alternating) group on n symbols. If an odd prime l divides the order of $D(ZG)$, then $l \leq n/2$ (providing $G \neq A_n$, n = prime p such that $(p + 1)/2$ is prime, when the estimate becomes $l \leq (n + 1)/2$).*

Proof. For $G = S_n$ see [18]; now take $G = A_n$ with $n \geq 6$, since $D(ZA_n) = 0$ for $n \leq 5$ (see [14]). Frobenius (see [19]) proves the complex characters of A_n take their values in Q or a quadratic extension of Q; thus if F is the center of a simple component of QA_n, $F = Q$ or a quadratic extension. Let S be the ring of algebraic integers of F and D the difference of S over Z. By [18, Proposition 2.7], it suffices to prove that if $l \neq 2$ divides the order of $u(S/n!(2D)^{-1})$, then $l \leq n/2$ (or $l \leq (n + 1)/2$ in the exceptional case).

Let P be a prime ideal of S above a rational prime p dividing $n!$; define integers e, a, b by

$$P^e \parallel p, \; p^a \parallel n!/2, \; P^b \parallel D$$

(so $b = e - 1$ if p odd). Thus $P^c \parallel n!(2D)^{-1}$, $c = ea - b$. The order of $u(S/P^c)$ is $(NP - 1)(NP)^{c-1}$, NP = absolute norm of P. Assume $l > n/2$. *Case* 1: l divides $(NP)^{c-1}$ for some P. It follows that $l = p$ is odd and $a = 1$, which contradicts $c - 1 > 0$. *Case* 2: l divides $NP - 1$. If $NP = p$, then $l \mid p - 1$ which implies $l \leq n/2$. If $NP = p^2$, then $l \mid p - 1$ or $l \mid p + 1$. The latter possibility implies $n = p$ and $l = (p + 1)/2$.

The next proposition shows the necessary condition of (3.7) is sufficient (excluding the possibly exceptional case).

(3.8) PROPOSITION. (i) *Let $G = S_n$ or A_n. An odd prime l divides $|T(ZG)|$ iff $l \leq n/2$.*

(ii) (Reiner [12]). *If l is an odd prime such that $n/2 < l \leq n$, then $(l - 1)/2$ divides $|T(ZS_n)|$.*

Proof. (i) If l divides $A(G)$, then $l \leq n/2$ by [8]. Conversely, if an odd prime $l \leq n/2$, then the two cycles

$$(1, 2, \ldots, l), \quad (l + 1, l + 2, \ldots, 2l)$$

are in A_n, hence $C_l \times C_l \subset A_n \subset S_n$ and we apply (3.1).

(ii) Observe that $S_n \supset \Omega(l, l - 1)$, l as in the hypotheses of (ii) and apply (3.6).

Remark. The smallest n such that 2 divides the order of $D(ZS_n)$ (resp. $D(ZA_n)$) is $n = 5$ (resp. 7); see [12], [14].

I wish to thank Shizuo Endo for communicating to me the following result.

(3.9) PROPOSITION. *Let SD be the semidihedral group defined by*

$$SD = \langle \sigma, \tau \colon \sigma^{2^{n+1}} = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1+2^n} \rangle, \quad n \geq 2.$$

Then $D(SD) = T(SD)$ has order 2.

Proof. By the methods of [5] one shows the order of $D(SD)$ is at most 2. On the other hand H_8 is a subgroup of SD; we conclude the proof by applying (3.5) and restriction from SD to H_8.

Open Problem. The Artin exponents of the groups of (3.1), (3.2), (3.5), (3.6), (3.9) are p^s, 2^s, 2, q, 4 respectively.[3] In these cases the exponent of $T(ZG)$ is $b \cdot A(G)$ where $b = 1$ or $1/2$. Does this always hold? In particular, if $|G| = p^{s+1}$, p odd prime, does $([1 + p, \sum])$ always have order p^s for G noncyclic? The results of (3.1), (3.2) show that the upper bound given in [18] for the exponent of $D(ZG)$, G a p-group, is attained for every s with suitable G.

4. Subgroups and Artin exponents

Let $t(G) = |T(ZG)|$. A group obtained from G by successive quotient and subgroups we call a subquotient of G. Denote by C, Q, D, or SD a 2-group which is respectively cyclic, quaternion, dihedral, or semidihedral. In fact [8] these are the only p-groups for which $A(G) \neq |G|p^{-1}$; $A(C) = 1$ and $A(D) = A(Q) = 2$, and $A(SD) = 4$. In (4.1) we record Lam's [1, pp. 586–7] description of $A(G)$ by hyperelementary subgroups. G_p denotes a Sylow p-subgroup of G and $A_p(G)$ the p-part of $A(G)$.

(4.1) THEOREM. *$A_p(G) = \sup (A_p(H))$ as H ranges over all p-hyperelementary subgroups of G, i.e., H is a semidirect product*

$$H = N \times_{s-d} H_p, \quad N \text{ cyclic normal in } H.$$

Further, $A_p(H) = \sup (A(H_p), |a(H, N)|)$ provided that if $p = 2$, then $H_p \neq Q$, D, or SD. $a(H, N)$ denotes the image of H_p in Aut N.

The following two lemmas show that divisibility properties of $A(G)$ force G to contain subgroups from the list of Section 3.

(4.2) LEMMA. *Assume $G_p \subset G$ is cyclic and $A_p(G) = p^s$, $s \geq 1$. The metacyclic group $\Omega(l, p^s)$ is a subquotient of G for some prime l.*

Proof. Since $A(G_p) = 1$, $G \supset H = N \times_{s-d} H_p$ as in (4.1) with $A_p(G) = A_p(H) = |a(H, N)|$. Cyclic subgroups (of N) are invariant under all automorphisms and $a(H, N)$ is cyclic, thus there exists a prime $l \neq p$ such that H has a subquotient $H_0 = N_l \times_{s-d} C_{p^s}$, C_{p^s} acting faithfully on N_l. Finally H_0 maps onto $\Omega(l, p^s)$.

(4.3) LEMMA. *Suppose G is a 2-group with $4 \mid A(G)$, and $G \neq SD$. Then the maximal abelian quotient $G^{ab} \neq C_2 \times C_2$, hence G^{ab} maps onto a noncyclic group of order* 8.

Proof. Since G is not cyclic, neither is G^{ab}. Therefore $G^{ab} \neq C_2 \times C_2$ will yield the desired conclusion.

Let sol (G) be the number of solutions in G to equation $x^2 = 1$. Now [3, p. 22]

$$(4.4) \qquad \text{sol}\,(G) = \sum_{\chi(1)=1} b(\chi) + 2 \sum_{\chi(1)=2} b(\chi) + \sum_{\chi(1)>2} b(\chi)\chi(1)$$

[3] Lam's assertion [8] that $A(SD) = 2$ is incorrect.

where χ ranges over all the complex irreducible characters of G and $b(\chi)$ is 0 if χ is not real, 1 if χ is character of a real representation of G, and -1 otherwise. From [8], $4 \mid A(G)$ implies $4 \mid \mathrm{sol}\,(G)$ or $G = SD$. By hypothesis, $G \neq SD$.

Assume $G^{ab} \cong C_2 \times C_2$ for a contradiction; there are four degree 1 characters, hence by (4.4) $\sum b(\chi)$, summed over the d characters χ with $\chi(1) = 2$, is even. From representation theory, $|G| \equiv 4 + 4d \bmod 16$ which implies $|G|/4 \equiv 1 + d \bmod 4$, so d is odd. However, if χ is not real then the conjugate $\bar{\chi} \neq \chi$ is another irreducible character. The statements d odd and $\sum_{\chi(1)=2} b(\chi)$ even are inconsistent.

(4.5) THEOREM. (i) *If an odd prime* $p \mid A(G)$, *then* $p \mid t(G)$.
(ii) *If* $4 \mid A(G)$ *and* G_2 *is not dihedral, then* $2 \mid t(G)$.

Remarks. It may well be unnecessary to assume G_2 is not dihedral. However, $A(G)$ even does not imply $t(G)$ even, e.g., if G is dihedral of order $2p$ or dihedral of order 2^n, then (see [13], [5]) $D(ZG) = 0$ and $A(G) = 2$.

Proof. p odd. If G_p is not cyclic, then a standard result of group theory asserts $G_p \supset C_p \times C_p$ and by (3.1), $t(C_p \times C_p) = p$. If G_p is cyclic we apply (4.2), $t(\Omega(l, p)) = p$, and use (2.8), (2.9) as usual.

$p = 2$. If G_2 is cyclic, apply (4.2) with hypothesis that $4 \mid A(G)$, and finally note $t(\Omega(l, 4)) = 2$. If G_2 is quaternion (resp. semidihedral) we are done by (3.5) (resp. (3.9)). It remains to consider $G_2 \neq C, Q, D$, or SD (thus $4 \mid A(G_2)$). Then we conclude the proof by (4.3) applied to G_2, and the fact that t (noncyclic abelian group of order 8) $= 2$ by (3.2).

(4.6) COROLLARY. $t(G) > 1$ *for all* G *containing a noncyclic subgroup of odd order.*

REFERENCES

1. H. BASS, *Algebraic K-theory*, Math. Lecture Note Series, Benjamin, New York, 1968.
2. S. ENDO AND T. MIYATA, *On the projective class group of finite groups*, to appear.
3. W. FEIT, *Characters of finite groups*, Benjamin, New York, 1967.
4. A. FRÖHLICH, *Locally free modules over arithmetic orders*, J. für Math., vol. 274/275 (1975), pp. 112–124.
4a. ———, *The Picard group of noncommutative rings, in particular of orders*, Trans. Amer. Math. Soc., vol. 180 (1973), pp. 1–46.
5. A. FRÖHLICH, M. E. KEATING AND S. M. J. WILSON, *The class groups of quaternion and dihedral 2-groups*, Mathematika, vol. 21 (1974), pp. 64–71.
6. S. GALOVICH, I. REINER AND S. ULLOM, *Class groups for integral representations of metacyclic groups*, Mathematika, vol. 19 (1972), pp. 105–111.
7. G. HIGMAN, *The units of group rings*, Proc. London Math. Soc. (2), vol. 46 (1940), pp. 231–248.
8. T. Y. LAM, *Artin exponent of finite groups*, J. Algebra, vol. 9 (1968), pp. 94–119.
9. ———, *Induction theorems for Grothendieck groups and Whitehead groups of finite groups*, Ann. Sci. École Norm. Sup., vol. 1 (1968), pp. 91–148.
10. R. LEE AND C. THOMAS, *Free finite group actions on* S^3, Bull. Amer. Math. Soc., vol. 79 (1973), pp. 211–215.

11. J. MARTINET, *Modules sur l'algèbre du groupe quaternion*, Ann. Sci. École Norm. Sup., vol. 4 (1971), pp. 399–408.
12. I. REINER, *Projective class groups of symmetric and alternating groups*, Linear and Multilinear Algebra, vol. 3 (1975), pp. 115–121.
13. I. REINER AND S. ULLOM, *A Mayer-Vietoris sequence for class groups*, J. Algebra, vol. 31 (1974), pp. 305–342.
14. ———, *Remarks on class groups of integral group rings*, Symp. Math. Inst. Nazionale Alta Mat. (Rome), vol. 13 (1974), pp. 501–516.
15. R. G. SWAN, *Periodic resolutions for finite groups*, Ann. of Math., vol. 72 (1960), pp. 267–291.
16. R. G. SWAN AND E. G. EVANS, *K-theory of finite groups and orders*, Springer Lecture Notes, no. 149, Berlin, 1970.
17. C. B. THOMAS AND C. T. C. WALL, *The topological spherical space form problem I*, Compositio Math., vol. 23 (1971), pp. 101–114.
18. S. ULLOM, *The exponent of class groups*, J. Algebra, vol. 29 (1974), pp. 124–132.
19. W. SPECHT, *Darstellungstheorie der alternierenden Gruppe*, Math. Zeitschr., vol. 43 (1938), pp. 553–572.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS