Proceedings of the Edinburgh Mathematical Society (1994) 37, 227–237 ©

SOME RESULTS ON SYMMETRICALLY-PRESENTED GROUPS

by D. L. JOHNSON and R. W. K. ODONI

(Received 17th June 1992)

Necessary and sufficient conditions are found on an ideal $\mathfrak{a} \lhd \mathbb{Z}[x]$ for the additive group $[\mathfrak{a}]_+$ of $\mathbb{Z}[x]/\mathfrak{a}$ to be finite and cyclic. As a consequence, the abelianizations of certain cyclically-presented groups are computed explicitly.

1980 *Mathematical subject classification*: 20F05, 11R09.

0. Introduction

Let $n \in \mathbb{N}$ and let F_n be the free group on n symbols $x_1, \ldots, x_n$. Let S_n be the symmetric group on $\{1, \ldots, n\}$ and, for $\sigma \in S_n$, consider the automorphism of F_n given by $x_i \mapsto x_{\sigma(i)}$, $1 \leqq i \leqq n$, which we again denote by σ. Now for any word $w \in F_n$ and any subgroup $\Gamma \leqq S_n$, we define a group $G_n(w, \Gamma)$ by the presentation

$$G_n(w, \Gamma) = \langle x_1, \ldots, x_n \,|\, \sigma(w), \sigma \in \Gamma \rangle = F_n/N, \tag{0.1}$$

where N is the normal closure of $\{\sigma(w): \sigma \in \Gamma\}$ in F_n, and call groups of this type *symmetrically presented.*

The chief aims of this paper are to provide criteria for the abelianization $G_n(w, \Gamma)^{ab}$ of $G_n(w, \Gamma)$ to be finite and finite cyclic, respectively. We remark that special cases of $G_n(w, \Gamma)$ have been discussed by numerous authors, and cite as examples (all with $\Gamma = \langle (1\,2 \ldots n) \rangle$):

(i) the 3-manifold groups [**9**]

$$K_n, \quad w = x_1 x_3 x_2^{-1}, \tag{0.2}$$

(ii) the Fibonacci groups of Conway [**3, 4, 8**]

$$F(r, n), \quad w = x_1 x_2 \ldots x_r x_{r+1}^{-1}, \tag{0.3}$$

(iii) and their generalizations

$$F(r, s, c, n), \quad w = x_1 x_2 \ldots x_r x_{s+1}^{-c}, \tag{0.4}$$

where all subscripts are reduced modulo n to lie in the set $\{1,2,\dots,n\}$. (For the special case $c=1$ see [2]).

For $u\in F_n$, let $\bar{u}$ denote the image of u in F_n^{ab}, so that F_n^{ab} is the free abelian group on $\bar{x}_1,\dots,\bar{x}_n$. Denoting the binary operation in F_n^{ab} by $+$, we have that $F_n^{ab}\cong\mathbb{Z}^n$ as a $\mathbb{Z}$-module. Moreover, F_n^{ab} has an obvious (left) $\mathbb{Z}\Gamma$-module structure induced by the permutation action of Γ on $x_1,\dots,x_n$, and then

$$G_n(w,\Gamma)^{ab}\underset{\mathbb{Z}}{\cong} F_n^{ab}/\mathbb{Z}\Gamma\cdot\bar{w}. \tag{0.5}$$

We give in Section 1 some general criteria for the finiteness of $G_n(w,\Gamma)^{ab}$ based on the isomorphism (0.5). Roughly speaking, there is a sharp dichotomy between the cases Γ transitive and Γ intransitive. Specifically, we show that when Γ is intransitive $G_n(w,\Gamma)^{ab}$ is infinite for every $w\in F_n$, while in the transitive case $G_n(w,\Gamma)^{ab}$ is finite for "almost all" $w\in F_n$. In Section 2, we consider the case where Γ is transitive abelian, and show that the structure of $G_n(w,\Gamma)^{ab}$ is that of the additive group $[\mathfrak{a}]_+$ of $\mathbb{Z}[t_1,\dots,t_k]/\mathfrak{a}$ for some ideal $\mathfrak{a}$ in the polynomial ring $\mathbb{Z}[t_1,\dots,t_k]$ in k (commuting) independent variables $t_1,\dots,t_k$ over $\mathbb{Z}$. In Section 3 we give a simple necessary and sufficient condition for $[\mathfrak{a}]_+$ to be finite cyclic, while in Section 4 we illustrate our results in the case where Γ is cyclic with specific calculations for examples (0.2) and (0.4) above.

We are indebted to several people for useful discussions and criticisms during the course of writing this paper. In particular, we acknowledge the contributions of K. A. Brown, M. W. Bunder, A.-C. Kim, S. J. Pride, G. C. Smith and M. J. Tomkinson.

1. Finiteness criteria

Throughout this section, "R-module" will mean "left R-module". Various standard results from representation theory will be quoted; for these [5] is a convenient reference.

We start from the isomorphism (0.5), and for convenience identify $\bar{x}_i$ with the row vector $(0,\dots,0,1,0,\dots,0)$, having 1 in the ith column, in $\mathbb{Z}^n$. Let $E=\sum_{i=1}^n \mathbb{Z}\bar{x}_i$, and for subrings R of $\mathbb{C}$ let $R\cdot E=\sum_{i=1}^n R\bar{x}_i$; this has a natural $R\Gamma$-module structure induced by the action of Γ on $\{x_1,\dots,x_n\}$.

Lemma 1.1. (i) *$G_n(w,\Gamma)^{ab}$ is finite if and only if $\mathbb{Q}\cdot E=\mathbb{Q}\Gamma\cdot\bar{w}$.*

(ii) *$\mathbb{Q}\cdot E=\mathbb{Q}\Gamma\cdot\bar{w}$ implies that $\mathbb{C}\cdot E=\mathbb{C}\Gamma\cdot\bar{w}$.*

Proof. Of these, only (i) requires proof. Suppose first that $G_n(w,\Gamma)^{ab}$ is finite, of order k say. Then $k\bar{x}_i\in\mathbb{Z}\Gamma\cdot\bar{w}$ for $i\leqq n$, so that $\bar{x}_1,\dots,\bar{x}_n\in\mathbb{Q}\Gamma\cdot\bar{w}$, whence $\mathbb{Q}\cdot E=\mathbb{Q}\Gamma\cdot\bar{w}$. For the converse, if $\mathbb{Q}\cdot E=\mathbb{Q}\Gamma\cdot\bar{w}$, then $\bar{x}_i=\lambda_i\bar{w}$ with $\lambda_i\in\mathbb{Q}\Gamma$, $1\leqq i\leqq n$. Choosing $d\in\mathbb{N}$ such that $d\lambda_1,\dots,d\lambda_n\in\mathbb{Z}\Gamma$, we see that $G_n(w,\Gamma)^{ab}$ is finite, of order dividing d^n. □

Lemma. 1.2. *If Γ is intransitive, then $G_n(w,\Gamma)^{ab}$ is infinite for all $w\in F_n$.*

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

Proof. In view of Lemma 1.1, it is enough to show that $\mathbb{C}\cdot E$ is not a cyclic $\mathbb{C}\Gamma$-module, that is, not of the form $\mathbb{C}\Gamma\cdot\xi$ for $\xi\in\mathbb{C}\cdot E$.

Suppose for a contradiction that Γ is intransitive but $\mathbb{C}\cdot E$ is cyclic, so that there is a $\mathbb{C}\Gamma$-epimorphism $\pi:\mathbb{C}\Gamma\to\mathbb{C}\cdot E$. It follows that

$$1=(\chi_1,\chi_r)\geqq(\chi_1,\chi_e),$$

where χ_r,χ_e,χ_1 are the characters of $\mathbb{C}\Gamma,\mathbb{C}\cdot E$, and the trivial $\mathbb{C}\Gamma$-module, respectively. But (χ_1,χ_e) is just the number of orbits of Γ on $\{1,2,\ldots,n\}$, and this is greater than 1 by hypothesis. □

We assume henceforth that Γ is transitive and fix the following notation:

$$H=\mathrm{stab}(x_1),\quad \Gamma=\bigcup_{i=1}^{n}\gamma_i H,$$

$$e_H=|H|^{-1}\sum_{h\in H}h\in\mathbb{Q}\Gamma,\ (e_H^2=e_H).$$

Lemma 1.3. *For transitive Γ, $\mathbb{Q}\cdot E\cong\mathbb{Q}\Gamma\cdot e_H$ and so $\mathbb{Q}\cdot E$ is a cyclic $\mathbb{Q}\Gamma$-module.*

Lemma 1.4. *Let Γ be transitive and put $M=\mathbb{Q}\Gamma\cdot e_H$. Then* (i) *the elements $v_i=\gamma_i e_H$ form a $\mathbb{Q}$-basis for M, and* (ii) *there is a non-zero homogeneous polynomial $P_\Gamma=P_\Gamma(t_1,\ldots,t_n)\in\mathbb{Q}[t_1,\ldots,t_n]$ of degree n in n commuting indeterminates such that, for $q_i\in\mathbb{Q}$, $1\leqq i\leqq n$, $\mathbb{Q}\Gamma\cdot\sum_{i=1}^{n}q_iv_i=M$ whenever $P_\Gamma(q_1,\ldots,q_n)\neq 0$.*

Proof. Part (i) is clear. For (ii), let $L(\mu)$: $M\to M$ be the $\mathbb{Q}$-linear map sending v_i to $v_i\mu$, $1\leqq i\leqq n$, $\mu\in M$. For $q_1,\ldots,q_n\in\mathbb{Q}$, we have

$$L\left(\sum_{i=1}^{n}q_iv_i\right)=\sum_{i=1}^{n}q_iL(v_i).$$

Now define

$$P_\Gamma(t_1,\ldots,t_n)=\det\left(\sum_{i=1}^{n}t_iL(v_i)\right)\in\mathbb{Q}[t_1,\ldots,t_n].$$

Then

$$\det\left(\sum_{i=1}^{n}q_iL(v_i)\right)=\det\left(L\left(\sum_{i=1}^{n}q_iv_i\right)\right)=P_\Gamma(q_1,\ldots,q_n)$$

whenever $q_1,\ldots,q_n\in\mathbb{Q}$. Clearly $\det(L(e_H))=1$, so that $P_\Gamma\neq 0$ in $\mathbb{Q}[t_1,\ldots,t_n]$. Let

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

$q_1, \ldots, q_n \in \mathbb{Q}$ with $P_\Gamma(q_1, \ldots, q_n) \neq 0$ and set $\mu = \sum_{i=1}^n q_i v_i$. Then $\det(L(\mu)) \neq 0$ so that $L(\mu)$ is surjective and $M = M\mu$. Hence

$$\mathbb{Q}\Gamma \cdot \mu \subseteq M = M\mu \subseteq \mathbb{Q}\Gamma \cdot \mu,$$

that is, $M = \mathbb{Q}\Gamma \cdot \mu$ as required. That P_Γ is homogeneous of degree n is clear from the definition. □

Corollary 1.5. *For transitive* Γ, *there is a non-zero homogeneous polynomial* P_Γ^* *of degree* n *in* n *variables such that* $G_n(w, \Gamma)^{ab}$ *is finite whenever* $P_\Gamma^*(r_1, \ldots, r_n) \neq 0$, *where* $\bar{w} = \sum_{i=1}^n r_i \bar{x}_i$.

We remark that, in any given case of interest, there is in principle no difficulty in calculating the polynomial P_Γ^*. Indeed, taking $\bar{x}_i$ as $\gamma_i e_H$ in $\mathbb{Q}\Gamma \cdot e_H$, where $\gamma_i x_1 = x_i$, P_Γ^* is just the P_Γ of Lemma 1.4.

2. Transitive abelian Γ

The results of the previous section can be greatly refined and simplified in the favourable special case when Γ is transitive and *abelian*, and we make this assumption now.

In this case, it is clear that $H = \{1\}$, $|\Gamma| = n$, and the action of Γ on $\{x_1, \ldots, x_n\}$ is equivalent to the (left) regular representation of Γ on itself. We can thus index the x's by the elements of Γ, so that

$$\gamma x_\delta = x_{\gamma\delta}, \quad \text{for all} \quad \gamma, \delta \in \Gamma$$

and $E \cong \mathbb{Z}\Gamma$ as $\mathbb{Z}\Gamma$-modules. Now write

$$\bar{w} = \sum_{\gamma \in \Gamma} r(\gamma) \bar{x}_\gamma \in G_n(w, \Gamma)^{ab}$$

and associate with w the element

$$w^* = \sum_{\gamma \in \Gamma} r(\gamma) \gamma \in \mathbb{Z}\Gamma.$$

As $E \cong \mathbb{Z}\Gamma$, our isomorphism (0.5) can in this case be expressed as

$$G_n(w, \Gamma)^{ab} \underset{\mathbb{Z}}{\cong} \mathbb{Z}\Gamma / \mathbb{Z}\Gamma \cdot w^*. \tag{2.1}$$

In the first place, (2.1) yields a simple formula for the order of $G_n(w, \Gamma)^{ab}$. For $\alpha \in \mathbb{Q}\Gamma$, let L_α be the $\mathbb{Q}$-linear map from $\mathbb{Q}\Gamma$ to itself sending $\gamma \in \Gamma$ to $\alpha\gamma$, and let $N(\alpha)$ be the determinant of L_α. It is clear that $N(\alpha) \in \mathbb{Q}$ and is non-zero if and only if α is a unit in

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

$\mathbb{Q}\Gamma$. We can evaluate $N(\alpha)$ using the characters of Γ, as follows. Let $\Gamma^* = \mathrm{Hom}(\Gamma, \mathbb{C}^*)$ be the character group of Γ. For $\chi \in \Gamma^*$, we extend χ to a $\mathbb{Q}$-algebra homomorphism from $\mathbb{Q}\Gamma$ to $\mathbb{C}$ by defining

$$\chi\left(\sum_{\gamma\in\Gamma} a_\gamma \gamma\right) = \sum_{\gamma\in\Gamma} \alpha_\gamma \chi(\gamma), \quad \text{all} \quad a_\gamma \in \mathbb{Q}.$$

Then it is easily checked that

$$N(\alpha) = \prod_{\chi\in\Gamma^*} \chi(\alpha). \tag{2.2}$$

Now consider (2.1). If $N(w^*) = 0$, then $\mathbb{Q}\Gamma \cdot w^* \neq \mathbb{Q}\Gamma = E$, and so $G_n(w, \Gamma)^{ab}$ is infinite; otherwise, $N(w^*)$ is a non-zero integer (since it is an algebraic integer in $\mathbb{Q}$), and $|N(w^*)|$ is the order of the (finite) group $G_n(w, \Gamma)^{ab}$, which can thus be evaluated using (2.2).

These calculations do not, of course, say anything about the *structure* of $G_n(w, \Gamma)^{ab}$. For this purpose, it is generally more convenient to present $\mathbb{Z}\Gamma$ as a quotient of a polynomial ring over $\mathbb{Z}$. To do this, suppose that Γ is the direct product of k finite cyclic groups of orders $n_1, \ldots, n_k$, so that $n = \prod_{i=1}^k n_i$. Let $t_1, \ldots, t_k$ be independent (commuting) variables over $\mathbb{Z}$. Then we clearly have a ring epimorphism

$$\pi: \mathbb{Z}[t_1, \ldots, t_k] \twoheadrightarrow \mathbb{Z}\Gamma$$

with $\mathrm{Ker}\,\pi = (t_1^{n_1} - 1, \ldots, t_k^{n_k} - 1)$. Choosing $f \in \mathbb{Z}[t_1, \ldots, t_k]$ such that $\pi(f) = w^*$, it follows from (2.1) that

$$G_n(w, \Gamma)^{ab} \underset{\mathbb{Z}}{\cong} \mathbb{Z}[t_1, \ldots, t_k]/\mathfrak{a}, \tag{2.3}$$

where

$$\mathfrak{a} = (t_1^{n_1} - 1, \ldots, t_k^{n_k} - 1, f). \tag{2.4}$$

This leads to the following general problem: if $R = \mathbb{Z}[t_1, \ldots, t_k]$ and $\mathfrak{a} \lhd R$, then what is the structure of $[\mathfrak{a}]_+$, the additive group of $R/\mathfrak{a}$? In the next section, we find simple necessary and sufficient conditions for $[\mathfrak{a}]_+$ to be finite cyclic.

3. Cyclic quotients of $\mathbb{Z}[t_1, \ldots, t_k]$

This section will be devoted to proving the following theorem, which is the main result of this paper.

Theorem 3.1. *Let $k \in \mathbb{N}$, $R = \mathbb{Z}[t_1, \ldots, t_k]$, and $\mathfrak{a} \lhd R$. Then the additive group $[\mathfrak{a}]_+$ of $R/\mathfrak{a}$ is finite and cyclic if and only if the following two conditions hold.*

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

(i) $\mathfrak{a} \cap \mathbb{Z} \neq 0$, *and*

(ii) *for all primes* $p \in \mathbb{N}$, *either* $\mathfrak{a} + pR = R$ *or* $\mathfrak{a} + pR = (p, t_1 - a_1, \ldots, t_k - a_k)$ *for some* $(a_1, \ldots, a_k) \in \mathbb{Z}^k$ *depending on* p.

Proof. We first prove necessity. Suppose that $[\mathfrak{a}]_+$ is cyclic of order $v \in \mathbb{N}$. Then $vR \subseteq \mathfrak{a}$, so that $0 \neq v\mathbb{Z} \subseteq \mathfrak{a} \cap \mathbb{Z}$ and (i) holds. Now let $p \in \mathbb{N}$ be prime. Then $[\mathfrak{a} + pR]_+$ is a quotient of $[\mathfrak{a}]_+$ and is thus finite and cyclic. Suppose that $\mathfrak{a} = (f_1, \ldots, f_s)$ and let $\bar{f}_i$ be the mod p-reduction of f_i, $1 \leqq i \leqq s$. There is a ring isomorphism

$$R/\mathfrak{a} + pR \cong \mathbb{F}_p[t]/(\bar{f}_1, \ldots, \bar{f}_s), \tag{3.1}$$

where $\mathbb{F}_p$ is the field $\mathbb{Z}/p\mathbb{Z}$ and $t = (t_1, \ldots, t_k)$, induced by reduction modulo p. Since the right-hand side of (3.1) is an $\mathbb{F}_p$-algebra, its additive group has exponent p or 1. Thus, $R/\mathfrak{a} + pR$ is either 0 or $\mathbb{F}_p$, that is, $\mathfrak{a} + pR$ is equal either to R or to $(p, t_1 - a_1, \ldots, t_k - a_k)$ for some $(a_1, \ldots, a_k) \in \mathbb{Z}^k$. Thus, (ii) holds.

The proof of sufficiency is rather harder. We assume that (i) and (ii) both hold, with $\mathfrak{a} \cap \mathbb{Z} = m\mathbb{Z}$ say, $m \in \mathbb{N}$, so that $mR \subseteq \mathfrak{a}$. We factorise $m = \prod_j p_j^{e_j}$ with distinct primes $p_j \in \mathbb{N}$, and all $e_j \in \mathbb{N}$, and put $\mathfrak{b}_j = \mathfrak{a} + p_j^{e_j} R$. Then $\mathfrak{b}_i + \mathfrak{b}_j = R$ for $i \neq j$, while

$$\mathfrak{a} \subseteq \bigcap_j \mathfrak{b}_j = \prod_j \mathfrak{b}_j \subseteq \mathfrak{a} + mR = \mathfrak{a}.$$

Hence, $\mathfrak{a} = \prod_j \mathfrak{b}_j$. The Chinese remainder theorem now gives

$$R/\mathfrak{a} \cong \prod_j R/\mathfrak{b}_j, \tag{3.2}$$

and

$$[\mathfrak{a}]_+ = \bigoplus_j [\mathfrak{b}_j]_+. \tag{3.3}$$

Since $p_j^{e_j} R \subseteq \mathfrak{b}_j$, $[\mathfrak{b}_j]_+$ is a p_j-torsion group (possibly trivial), so that $[\mathfrak{a}]_+$ is finite cyclic if and only if each $[\mathfrak{b}_j]_+$ is. We now show that condition (ii) guarantees the latter.

Let p be any one of the p_j, and let $e = e_j \geqq 1$ and $\mathfrak{b} = \mathfrak{a} + p^e R = \mathfrak{b}_j$. First of all we must have $\mathfrak{a} + pR \neq R$. For otherwise we can solve $1 = a + pr$, $a \in \mathfrak{a}$, $r \in R$, and then $p^{-1}m = p^{-1}ma + mr \in \mathfrak{a}$ since $m \in \mathfrak{a}$, which contradicts $\mathfrak{a} \cap \mathbb{Z} = m\mathbb{Z}$. We thus have

$$\mathfrak{a} + pR = (p, t_1 - a_1, \ldots, t_k - a_k)$$

for some $\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$. We now approach the core of the proof, which is embodied in the following assertion.

(*) *For each* $n \in \mathbb{N}$, *there is a corresponding* $\mathbf{b} = \mathbf{b}(n) \equiv \mathbf{a} \pmod{p}$ *in* $\mathbb{Z}^k$ *such that* $(p^n, t_1 - b_1, \ldots, t_k - b_k) \subseteq \mathfrak{a} + p^n R$.

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

Let us first see how this yields the result. Letting $\mathfrak{c}=(p^n, t_1-b_1, \ldots, t_k-b_k)$, we see that $[\mathfrak{a}+p^nR]_+$ is a quotient of $[\mathfrak{c}]_+$, and since $R/\mathfrak{c}\cong\mathbb{Z}/p^n\mathbb{Z}$, it follows that $[\mathfrak{c}]_+$ is cyclic of order p^n. Taking $n=e=e_j$, $p=p_j$, we deduce that $[\mathfrak{b}_j]_+$ is cyclic of order dividing $p_j^{e_j}$, and then the result follows from (3.3).

It remains to prove assertion (*). This is done by induction on n, taking $\mathbf{b}(1)=\mathbf{a}\in\mathbb{Z}^k$ when $n=1$. Now let $n\geqq 1$ and suppose we have some $\mathbf{b}\equiv\mathbf{a} \pmod p$ in $\mathbb{Z}^k$ such that $(p^n, t_1-b_1, \ldots, t_k-b_k)\subseteq\mathfrak{a}+p^nR$. By applying a suitable $\mathbb{Z}$-automorphism of R, we see that without loss of generality we may take $\mathbf{b}=\mathbf{0}\equiv\mathbf{a} \pmod p$, in which case,

$$\mathfrak{a}+pR=(p, t_1, \ldots, t_k)\supseteq\mathfrak{a}+p^nR\supseteq(p^n, t_1, \ldots, t_k).$$

Now let $\mathfrak{a}=(f_1, \ldots, f_s)$, $f_i\in R$, and let $\mathfrak{b}$ be the ideal $(t_1, \ldots, t_k)$ in R. Then there exist $h_i, g_{ij}\in R$ such that

$$f_i=ph_i+\sum_{j=1}^{k} g_{ij}t_j, \quad 1\leqq i\leqq s. \tag{3.4}$$

In particular,

$$f_i\equiv\phi_i \pmod{(p, \mathfrak{b}^2)}, \quad 1\leqq i\leqq s, \tag{3.5}$$

where $\phi_i=\sum_{j\leqq k} g_{ij}(\mathbf{0})t_j$; here $\theta(\mathbf{0})\in\mathbb{Z}$ means the evaluation of $\theta\in R$ at $\mathbf{t}=\mathbf{0}$. Clearly,

$$\mathfrak{a}+pR=(p, \mathfrak{b})=(p, \phi_1, \ldots, \phi_s, \mathfrak{b}^2). \tag{3.6}$$

A simple calculation involving the comparison of polynomials of given total degree now shows that

$$t_q\equiv\sum_{i=1}^{s} e_{qi}\phi_i \pmod p, \quad 1\leqq q\leqq k, \tag{3.7}$$

for some $e_{qi}\in\mathbb{Z}$. Let $\mathbf{E}$ be the $k\times s$ matrix (e_{qi}) and $\mathbf{G}$ the $s\times k$ matrix $(g_{ij}(\mathbf{0}))$. Then (3.7) implies that

$$\mathbf{EG}=\mathbf{I}+p\mathbf{V}, \tag{3.8}$$

where $\mathbf{I}$ is the $k\times k$ identity matrix and $\mathbf{V}$ is some $k\times k$ matrix over $\mathbb{Z}$, since the t_q are (algebraically) independent modulo p.

Now define, for $1\leqq q\leqq k$, $\psi_q=\sum_{i=1}^{s} e_{qi}f_i\in\mathfrak{a}$. It follows from (3.4) that

$$\psi_q=p\sum_{i=1}^{s} e_{qi}h_i+\sum_{i=1}^{s}\sum_{j=1}^{k} e_{qi}g_{ij}(\mathbf{0})t_j+\rho_q, \tag{3.9}$$

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

where $\rho_q \in \mathfrak{b}^2$. Now, by hypothesis, $\mathfrak{b} \subseteq \mathfrak{a} + p^n R$, so that $\mathfrak{a}$, $p\mathfrak{b}, \mathfrak{b}^2 \subseteq \mathfrak{a} + p^{n+1}R$. These facts, together with (3.8) and (3.9), imply that

$$t_q + p\sum_{i=1}^{s} e_{qi}h_i(0) \in \mathfrak{a} + p^{n+1}R, \quad 1 \leqq q \leqq k.$$

We now take $b'_q = -p\sum_{i=1}^{s} e_{qi}h_i(\mathbf{0}) \in p\mathbb{Z}$, $1 \leqq q \leqq k$, and deduce that p^{n+1}, $t_1 - b'_1, \ldots, t_k - b'_k \in \mathfrak{a} + p^{n+1}R$, where $\mathbf{b}' \equiv \mathbf{a} \equiv \mathbf{0} \pmod{p}$ in $\mathbb{Z}^k$. This completes the proof of assertion (*).

□

4. Cyclic Γ: two examples

In the special case of cyclic Γ, which is the most frequently encountered in practice, it seems natural to call $G_n(w, \Gamma)$ *cyclically presented*. For the examples mentioned in the introduction, we shall find necessary and sufficient conditions on the parameters for $F(r, s, c, n)^{ab}$ to be finite, and describe the structure of K_n^{ab} precisely. The $F(r, n)$ have been extensively studied, and their abelianizations form the subject of [6], [1], [7]; indeed the first of these contains a proof of part (i) of the following result for these groups.

Proposition 4.1. *Let* $\Gamma = \langle (1\,2 \ldots n) \rangle$, $w \in F_n$, *and* $f(t)$ *the exponent-sum polynomial of* (2.4). *Then*

(i) $G_n(w, \Gamma)^{ab}$ *is finite if and only if the resultant* $\rho = f * g \neq 0$, *where* $g(t) = t^n - 1$, *and then its order is* $|\rho|$, *and*

(ii) $G_n(w, \Gamma)^{ab}$ *is finite cyclic if and only if in addition the highest common factor* $(\bar{f}, \bar{g})$ *in* $\mathbb{F}_p[t]$ *is linear for every prime* p *dividing* $|\rho|$.

Proof. (i) A relation matrix for $G_n(w, \Gamma)^{ab}$ is the circulant matrix C whose first row consists of the exponent sums e_i of x_i in w, $1 \leqq i \leqq n$. Then the determinant of C is just the product of the values of $f(x)$ on all nth roots of unity, that is, $\pm\rho$. Thus, the group is infinite if and only if $\rho = 0$ and otherwise has order $|\rho|$.

(ii) We assume that $\rho \neq 0$ and refer to the conditions of Theorem 3.1 with $\mathfrak{a} = (f, g)$. Since $\rho \neq 0$, (i) is automatic and (ii) splits into two cases.

(a) $p \nmid |\rho| \Leftrightarrow (\bar{f}, \bar{g}) = 1$ in $\mathbb{F}_p \Leftrightarrow \mathfrak{a} + pR = R$, where $R = \mathbb{Z}[t]$.

(b) $p \mid |\rho| \Leftrightarrow (\bar{f}, \bar{g}) = (t - a) \Leftrightarrow \mathfrak{a} + pR = (p, t - a)$. □

For our first example, consider the group $F(r, s, c, n)$ given by (0.4) with associated polynomial

$$f(t) = 1 + t + \cdots + t^{r-1} - ct^s,$$

where $r, s, c \in \mathbb{Z}$, $r \geqq 2$. We seek necessary and sufficient conditions on the parameters for

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

this to vanish on an nth root of unity and consider first four cases depending on the value of c.

Case (i): $c=r$. Then $f(1)=0$.

Case (ii): $c=0$ and $(r,n)=h>1$. Then f vanishes on a primitive hth root of unity.

Case (iii): $c=\pm 1$, $\exists m \mid n$, $m>1$, with $r\equiv 1 \pmod m$ and either $s\equiv 0 \pmod m$ and $c=1$, or $s\equiv m/2 \pmod m$ and $c=-1$, with m even in the second case. Then f vanishes on a primitive mth root of unity.

Case (iv): $c=(-1)^u 2$, $s=1+3u$, $r\equiv 3 \pmod 6$ and $n\equiv 0 \pmod 6$. If λ is a primitive sixth root on unity, then

$$f(\lambda)=1+\lambda+\lambda^2-(-1)^u\cdot 2\cdot\lambda\cdot\lambda^{3u}=1-\lambda+\lambda^2=0.$$

Proposition 4.2. *The group $F(r,s,c,n)^{ab}$ is infinite in the above four cases and finite otherwise.*

Proof. Only the second assertion requires proof, so we assume that $c\neq r$ (case (i)). If $c=0$ and r,n are coprime, then $g_* f\neq 0$ and the group is finite. Thus, we may also assume that $c\neq 0$ (case (ii)). Now let λ be a primitive mth root of unity with $m \mid n$ and $f(\lambda)=0$. Then we claim that the parameters satisfy the conditions in case (iii) or case (iv). From $f(\lambda)=0$ we obtain

$$\lambda^r-1=c\lambda^s(\lambda-1), \tag{4.1}$$

whence,

$$c\lambda^s-1=\lambda^r(c\lambda^{s-r+1}-1). \tag{4.2}$$

Since $|\lambda|=1$, $|c\lambda^s-1|=|c\lambda^{s-r+1}-1|$, and since $c\neq 0$ we have

$$\lambda^{s-r+1}=\lambda^{\pm s}.$$

If $\lambda^{s-r+1}=\lambda^s$, then $\lambda^{r-1}=1$ and it follows from (4.2) that

$$(\lambda-1)(c\lambda^s-1)=0.$$

But $f(1)\neq 0$ so $\lambda\neq 1$ and $c\lambda^s=1$. This implies that $c=\pm 1=\lambda^s$, which gives case (iii).

There remains the possibility that $\lambda^{s-r+1}=\lambda^{-s}$, which we have to reduce to case (iv) under the assumption that $c\neq\pm 1$. Thus, $\lambda^{r-1}=\lambda^{2s}$ and

$$\frac{\lambda^{2s+1}-1}{\lambda-1}=c\lambda^s \tag{4.3}$$

using (4.1), with $c\notin\{0,\pm 1,r\}$ and $m=\operatorname{ord}\lambda>1$. Let $\operatorname{ord}\lambda^{2s+1}=d \mid m$. Taking norms from $\mathbf{Q}(\lambda)$ to $\mathbf{Q}$ in (4.3) we have

https://doi.org/10.1017/S0013091500006039 Published online by Cambridge University Press

$$c^{\phi(m)}(-1)^{s\phi(m)} = (\Phi_d(1))^{\phi(m)/\phi(d)}/\Phi_m(1), \tag{4.4}$$

where Φ_m is the mth cyclotomic polynomial and ϕ is the Euler totient function.

Now let p be a prime dividing c, $p^t \| c$ say. Then $p \mid \Phi_d(1)$ by (4.4) which implies that $d = p^k$, $k \geqq 1$, and $\Phi_d(1) = p$. Comparing powers of p in both sides of (4.4), we have

$$t\phi(m) \leqq \phi(m)/\phi(d).$$

This forces $t = 1$ and $\phi(d) = 1$. Since $d = p^k$, this means that $p = 2$ and $k = 1$. Hence, $c = \pm 2$ and $\lambda^{2s+1} = -1$. Substitutimg into (4.3), we obtain

$$2 = \pm 2\lambda^s(1-\lambda). \tag{4.5}$$

Squaring this gives $4 = -4\lambda^{-1}(1-\lambda)^2$, that is, $\lambda^2 - \lambda + 1 = 0$, so that $m = \operatorname{ord} \lambda = 6$. It now follows from (4.5) that $s \equiv 1 \pmod 3$, $s = 1 + 3u$ say, and that

$$\operatorname{sgn} c = \lambda^{1+3u}(1-\lambda) = \lambda(1-\lambda)(-1)^u,$$

that is, $\lambda(\lambda - 1) = (-1)^{u+1} \operatorname{sgn} c$. Thus $(-1)^u = \operatorname{sgn} c$. Finally, $\lambda^{2s} = \lambda^{r-1}$, whence $r - 1 \equiv 2s \equiv 2 \pmod 6$. This completes the verification of the conditions of case (iv). □

For our second example, we take the group K_n given by (0.2), with associated polynomial

$$f(t) = t^2 - t + 1 = \Phi_6(t),$$

the sixth cyclotomic polynomial; it is interesting to note that this same f is also associated with $F(3, 1, 2, n)$ in the previous example. As above, let $g(t) = t^n - 1$ and consider four cases.

Case (i): $n \equiv 0 \pmod 6$. Here $\Phi_6 \mid g$, $\rho = 0$ and K_n^{ab} is infinite.

Case (ii): $n \equiv \pm 1 \pmod 6$. Here, K_n^{ab} is trivial, and K_n is perfect.

Case (iii): $n \equiv 3 \pmod 6$. Here $\rho = 4$ and $\bar{f}$ is irreducible over $\mathbb{F}_2$. Its zeros thus belong to $\mathbb{F}_4 \backslash \mathbb{F}_2$ and so have order 3. Thus they are both zeros of $t^n - 1$ in this case. Hence, the highest common factor of $\bar{f}$ and $\bar{g}$ has degree 2 and K_n^{ab} is non-cyclic, namely $C_2 \oplus C_2$.

Case (iv): $n \equiv +2 \pmod 6$. Here $\rho = 3$ and, modulo $p = 3$, $\bar{f} = (t+1)^2$. Since -1 is a simple zero of $\bar{g}$ in this case, it follows that $(\bar{f}, \bar{g}) = t + 1$, proving that K_n^{ab} is cyclic, namely C_3.

REFERENCES

1. M. W. Bunder, D. L. Johnson and A.-C. Kim, The exponents of Fibonacci algebras, Fibonacci Quarterly, submitted.

2. C. M. Campbell and E. F. Robertson, The orders of certain metacyclic groups, *Bull. London Math. Soc.* **6** (1974), 312–314.

3. J. H. Conway, Advanced problem 5327, *Amer. Math. Monthly* **72** (1965), 915.

4. J. H. Conway, Solution to advanced problem 5327, *Amer. Math Monthly* **74** (1967), 91–93.

5. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (John Wiley, New York 1962).

6. D. L. Johnson, A note on the Fibonacci groups, *Israel J. Math.* **17** (1974), 27–282.

7. D. L. Johnson and A.-C. Kim, Cyclic Fibonacci algebras, in preparation.

8. R. M. Thomas, The Fibonacci groups revisited, in *Groups St Andrews 1989* (eds. C. M. Campbell and E. F. Robertson), CUP, Cambridge 1991, 445–454.

9. R. M. Thomas, On a question of Kim concerning certain group presentations, *Bull. Korean Math. Soc.* **28** (1991), 219–224.

Mathematics Department
University of Nottingham
University Park
Nottingham NG7 2RD

Mathematics Department
University of Glasgow
University Gardens
Glasgow G12 8QW