SOME FINITELY GENERATED ANALOGUES OF A GROUP OF A. H. CLIFFORD

JACQUES LEWIN

Introduction. Let n_1 and n_2 be two elements of a commutative field $\mathfrak{K}$ of characteristic different from 2 that satisfy: (i) $n_1 \neq 0$; (ii) $n_2 \neq 0$; (iii) $n_1 + n_2 \neq 0$. We define the "weighted average" $\alpha * \beta$ of two arbitrary elements α and β of $\mathfrak{K}$ as

$$\alpha * \beta = \frac{n_1 \alpha + n_2 \beta}{n_1 + n_2}.$$

If we are further given a total ordering $>$ on the set of elements of $\mathfrak{K}$, we associate with the triple $(\mathfrak{K}, n_1, n_2)$ the group $H(\mathfrak{K}, n_1, n_2)$ generated by symbols $[\alpha]$, one for each element α of $\mathfrak{K}$, subject to the relations

$$\text{(I)} \qquad [\alpha][\beta][\alpha]^{-1} = [\alpha * \beta] \qquad \text{if } \alpha > \beta.$$

The group $H(\mathfrak{Q}, 1, 1)$, where $\mathfrak{Q}$ is the field of rational numbers, provided one of the first examples of an ordinally simple group **(1)**. In this paper, we investigate the groups $H(\mathfrak{P}, n_1, n_2)$, where $\mathfrak{P}$ is the Galois field of order the prime p, and $n_1, n_2 \in \mathfrak{P}$ satisfy the above conditions. The required total ordering is obtained by making the usual identification of $\mathfrak{P}$ with the ordered set of integers

$$S_p = \{0, 1, \ldots, p-1\}.$$

Our main theorem states that $H(\mathfrak{P}, n_1, n_2)$ is isomorphic to the metacyclic group $M(\mathfrak{P}, n_1, n_2)$ defined by

$$M(\mathfrak{P}, n_1, n_2) = \mathrm{gp}(a, b;\, b^p = 1,\, a^{-1} b^{n_2} a = b^{n_1+n_2}).$$

We should like to thank Professor G. Baumslag, who suggested this investigation, and Professor B. H. Neumann, who suggested a generalization of a first draft of this paper.

Preliminaries. For convenience, we write H for $H(\mathfrak{P}, n_1, n_2)$, M for $M(\mathfrak{P}, n_1, n_2)$ whenever this is unambiguous. Setting $n_3 = n_1 + n_2$, we define a new operation, denoted by $\circ$, on $\mathfrak{P}$ by

$$\alpha \circ \beta = \frac{n_3 \beta - n_1 \alpha}{n_2}, \qquad \alpha, \beta \in \mathfrak{P}.$$

Received November 5, 1963. Supported in part by NSF Grant GP-27 and by an office of Naval Research Postdoctoral Associateship.

It is easily verified that

$$(1) \qquad \alpha \circ (\alpha * \beta) = \beta.$$

Furthermore, it follows immediately from the relations (I) that, if $\gamma = \alpha * \xi$ for some $\xi < \alpha$,

$$(2) \qquad [\alpha]^{-1}[\gamma][\alpha] = [\alpha \circ \gamma].$$

Let k be a positive integer, and let $\square \in \{*, \circ\}$. We write $\alpha \square^k \beta$ for

$$\overbrace{\alpha \square (\ldots (\alpha \square (\alpha \square}^{k \text{ terms}} \beta)) \ldots) .$$

If g_1 and g_2 are elements of a group, we write $[g_1, g_2]$ for the commutator $g_1 g_2 g_1^{-1} g_2^{-1}$ and $g_1^{g_2}$ for the conjugate $g_2 g_1 g_2^{-1}$ of g_1 by g_2.

1. The finiteness of a special factor group of H. In this section, we show that H has a non-trivial centre $\zeta(H)$ and that $H/\zeta(H)$ is finite.

Let $N = N(n_1, n_2)$ be the smallest positive integer such that $n_3^N - n_2^N = 0$. (Such an N always exists since $n_3^{p-1} = n_2^{p-1} = 1$.)

LEMMA 1. *Let $\alpha, \beta \in \mathfrak{P}$ and let k be a positive integer. Then if $\alpha \neq \beta$,*

$$a *^k \beta = \beta,$$

if and only if $k \equiv 0 \pmod{N}$.

Proof. It is easy to see by induction on k that

$$(3) \qquad \alpha *^k \beta = \frac{\alpha n_1 \sum_{j=0}^{k-1} n_3^j n_2^{k-j-1} + n_2^k \beta}{n_3^k}.$$

Suppose that $\alpha *^k \beta = \beta$ for some value of k. We can rewrite (3) as

$$(4) \qquad (n_3^k - n_2^k)\beta = \alpha n_1 \sum_{j=0}^{k-1} n_3^j n_2^{k-j-1}.$$

Two cases arise. If $n_3^k - n_2^k \neq 0$, then

$$\beta = \frac{\alpha n_1 \sum_{j=0}^{k-1} n_3^j n_2^{k-j-1}}{n_3^k - n_2^k} = \frac{\alpha n_1}{n_3 - n_2} = \alpha,$$

which contradicts the hypothesis that $\alpha \neq \beta$. This proves the "only if" part of the lemma. If, however, $n_3^k - n_2^k = 0$, then

$$0 = \frac{n_3^k - n_2^k}{n_3 - n_2} = \sum_{j=0}^{k-1} n_3^j n_2^{k-j-1}$$

and $\alpha *^k \beta = n_2^k \beta / n_3^k = \beta$, as required.

The equation

$$[p-1]^k[\alpha][p-1]^{-k} = [p-1 *^k \alpha], \qquad \alpha \in \mathfrak{P},$$

now enables us to conclude that $[p-1]^N$ belongs to $\zeta(H)$. This fact in turn enables us to prove the following lemma.

LEMMA 2. *All the generators* $[\alpha]$ *of* H *have a common* N*th power that lies in the centre of* H.

Proof. The equation $[\beta] = [\xi][0][\xi]^{-1}$ always has the solution $[\xi] = [n_3\,\beta/n_1]$. In particular, $[p-1] = [-n_3/n_1][0][-n_3/n_1]^{-1}$. Raising both sides to the Nth power, conjugating both sides by $[-n_3/n_1]^{-1}$, and remembering that $[p-1]^N \in \zeta(H)$, we obtain

$$[p-1]^N = [-n_3/n_1]^{-1}\,[p-1]^N\,[n_3/n_1] = [0]^N.$$

Now, since $[0]^N$ is a central element, and $[\beta]^N$ is a conjugate of $[0]^n$, $[\beta]^n = [0]^n$ for all β, and the lemma is proved.

Let Z be the cyclic subgroup of H generated by $[p-1]^N$. Z is normal in H and, by Lemma 2, the factor group $G = H/Z$ is just the group generated by symbols that we again call $[\alpha]$

$$G = \mathrm{gp}([\alpha]; \alpha \in \mathfrak{P})$$

with the relations (I), and the further relations

$$\text{(II)} \qquad [\alpha]^N = 1.$$

We now show that G is finite.

PROPOSITION 3. *Any non-trivial element of* G *can be expressed in the "reduced form"*

$$(5) \qquad [\alpha_1]^{k_1}\,[\alpha_2]^{k_2} \ldots [\alpha_n]^{k_n}, \qquad \alpha_1 < \alpha_2 < \ldots < \alpha_n,$$

where the k_i's *are positive integers.*

Proof. Let a "string"

$$w = [\alpha_1][\alpha_2] \ldots [\alpha_n], \qquad \alpha_i \in \mathfrak{P},$$

be called an "expanded word." Since all the generators of G are of finite order, every element of G can be expressed as an expanded word. Call the $[\alpha_i]$'s the "letters" of w, n the "length" of w, and α_n the "last index" of w. A word in the form (5), which will be called a "reduced word," can then be thought of as an expanded word of length $\sum^n{}_{i=1} k_i$. We prove the proposition by proving that every expanded word can be expressed as a reduced word. The proof is by double induction on length and on last index. Thus assume that for positive integers k and n

(i) an expanded word of length n can be reduced, and the resulting word has length at most n;

(ii) an expanded word of length $n+1$ whose last index is greater than k can be reduced to a word of length at most $n+1$.

Let w be an expanded word of length $n+1$ whose last index is k. By assumption (i), we can reduce the leftmost n letters of w. The resulting word is

$$\tilde{w} = [\alpha_1]\ldots[\alpha_m][k],$$

where $[\alpha_1]\ldots[\alpha_m]$ is reduced and $m \leqslant n$. If $\alpha_m \leqslant k$, then $\tilde{w}$ is in reduced form and has length at most $n+1$. We may then assume that $\alpha_m > k$. In this case

$$[\alpha_m][k] = [\alpha_m * k][\alpha_m]$$

and hence

$$\tilde{w} = [\alpha_1]\ldots[\alpha_m * k][\alpha_m],$$

which can be reduced by (ii). Thus we have shown that an expanded word of length $n+1$ whose last index is k can be reduced to a word of length at most $n+1$.

To complete the proof of the proposition, we need only prove the initial stage of each induction. That is, we must show that

(iii) a word of length 1 can be reduced;

(iv) under assumption (i), a word of length $n+1$ whose last index is $p-1$ can be reduced, and the resulting word has length at most $n+1$.

Statement (iii) is trivially true. To prove (iv), let w be a word of length $n+1$ whose last index is $p-1$. By (i), we may reduce the leftmost n letters of w. The resulting word is then automatically in reduced form, and has length at most $n+1$.

Since the generators of G all have order N, the exponents k_i in (5) can be reduced (mod N). There are then at most N^p words of the form (5), and so G is finite, as claimed.

2. A symmetric set of relations for H. In this section we show that the relations (I) hold even when $\alpha < \beta$.

LEMMA 4. *For all* α *in* $\mathfrak{P}$,

$$[p-2]^{-1}[\alpha][p-2] = [p-2\circ\alpha].$$

Proof. By (I), if $\beta \neq p-1$,

$$[p-2][\beta][p-2]^{-1} = [p-2*\beta]$$

or, equivalently,

$$[p-2]^{-1}[p-2*\beta][p-2] = [\beta], \qquad \beta \neq p-1. \tag{6}$$

By (1), $\beta = p-2\circ(p-2*\beta)$, so that, setting $\gamma = p-2*\beta$, equation (6) reads:

$$[p-2]^{-1}[\gamma][p-2] = [p-2\circ\gamma], \qquad \gamma \neq p-2*p-1.$$

https://doi.org/10.4153/CJM-1966-004-3 Published online by Cambridge University Press

The proof of the lemma then reduces to the proof of the single relation:

$$[p-2]^{-1}[p-2*p-1][p-2] = [p-2\circ(p-2*p-1)] = [p-1].$$

By Lemma 1,

$$(p-2)*^k p-1 = p-1 \Leftrightarrow k\equiv 0 \pmod N. \tag{7}$$

Hence, if $k<N$,

$$p-2*^k p-1 = p-2*^{k-1}(p-2*p-1)$$

is strictly less than $p-1$. It then follows that, for $k<N$,

$$[p-2]^{k-1}[p-2*p-1][p-2]^{-(k-1)} = [p-2*^{k-1}(p-2*p-1)] \tag{8}$$

and hence, by (7) and (8),

$$[p-2]^{N-1}[p-2*p-1][p-2]^{-(N-1)} = [p-1)].$$

Since $[p-2]^N\in\zeta(H)$, this last equation can be written as

$$[p-2]^{-1}[p-2*p-1][p-2] = [p-1]$$

and the lemma is proved.

Let $\alpha,\beta,\gamma\in\mathfrak{P}$. We define $(\alpha*\beta\circ)^k\gamma$ recursively by

$$(\alpha*\beta\circ)\gamma = \alpha*(\beta\circ\gamma) \text{ and } (\alpha*\beta\circ)^k\gamma = (\alpha*\beta\circ)(\alpha*\beta\circ)^{k-1}\gamma.$$

It then follows from the easily verified formula

$$\alpha*(\beta\circ\gamma) = \gamma+(n_1/n_3)(\alpha-\beta)$$

that, for any positive integer k,

$$(\alpha*\beta\circ)^k\gamma = \gamma+k(n_1/n_3)(\alpha-\beta). \tag{9}$$

We derive from equation (9) two useful corollaries.

LEMMA 5. *Let $\alpha,\beta,\gamma\in\mathfrak{P}$ with $\alpha\neq\beta$, and let k_1 and k_2 be two positive integers. Then $(\alpha*\beta\circ)^{k_1}\gamma=(\alpha*\beta\circ)^{k_2}\gamma$ only when $k_1\equiv k_2 \pmod p$. In particular, $(\alpha*\beta\circ)^k\gamma=\gamma$ only when $k\equiv 0\pmod p$.*

LEMMA 6. *Let $\alpha,\beta,\gamma_1,\gamma_2\in\mathfrak{P}$ and let k be a positive integer. Then*

$$(\alpha*\beta\circ)^k\gamma_1 = (\alpha*\beta\circ)^k\gamma_2$$

only when $\gamma_1=\gamma_2$.

PROPOSITION 7. *For all $\alpha,\beta\in\mathfrak{P}$, $[\alpha][\beta][\alpha]^{-1}=[\alpha*\beta]$.*

Proof. Let $\gamma\in\mathfrak{P}$. It follows from Lemma 4 and the relations (I) that

$$[p-1][p-2]^{-1}[\gamma][p-2][p-1]^{-1} = [p-1*(p-2\circ\gamma)].$$

Hence by induction

$$([p-1][p-2]^{-1})^k[\gamma]([p-1][p-2]^{-1})^{-k} = [(p-1*p-2\circ)^k\gamma]. \tag{10}$$

As in Lemma 2, we write $\gamma = \xi * 0$. Equation (10) now reads

$$([p-1][p-2]^{-1})^k[\xi * 0]([p-1][p-2]^{-1})^{-k} = [(p-1*p-2\circ)^k(\xi * 0)]$$

or, equivalently,

$$(11)\quad ([p-1][p-2]^{-1})^k[\xi][0][\xi]^{-1}([p-1][p-2]^{-1})^{-k} = [(p-1*p-2\circ)^k\,(\xi * 0)].$$

Now let α and β be two arbitrary elements of $\mathfrak{P}$. By Lemma 5 there exists a positive integer k such that $(p-1*p-2\circ)^k\,0 = \beta$ and, by Lemma 6, there exists an element ξ of $\mathfrak{P}$ such that $(p-1*p-2\circ)^k\,\xi = \alpha$. For this choice of k and ξ, it follows from (10) that

$$\begin{aligned}([p-1][p-2]^{-1})^k[\xi][0][\xi]^{-1}([p-1][p-2]^{-1})^{-k} &= [\xi]^{([p-1][p-2]^{-1})^k}[0]^{([p-1][p-2]^{-1})^k}([\xi]^{-1})^{([p-1][p-2]^{-1})^{-k}}\\ &= [\alpha][\beta][\alpha]^{-1}.\end{aligned}$$

Therefore, by (11), $[\alpha][\beta][\alpha]^{-1} = [(p-1*p-2\circ)^k(\xi * 0)]$. It now follows from the easily verified formula

$$\alpha * (\beta * \gamma) = (\alpha * \beta) * (\alpha * \gamma), \qquad \alpha, \beta, \gamma \in \mathfrak{P},$$

that

$$(p-1*p-2\circ)^k(\xi * 0) = ((p-1*p-2\circ)^k\xi) * ((p-1*p-2)^k0) = \alpha * \beta$$

and hence that $[\alpha][\beta][\alpha]^{-1} = [\alpha * \beta]$. Since α and β were arbitrary elements of $\mathfrak{P}$, the proposition is proved.

3. The commutator subgroup of H**.** We now turn our attention to H', the commutator subgroup of H, and show that it collapses to a cyclic group of order p.

It is clear, since H/H' is infinite cyclic, that the set $\{\ldots, [p-1]^{-1}, [p-1]^0, [p-1], \ldots\}$ is a set of coset representatives of H' in H. A straightforward application of Schreier's technique for finding generators for a subgroup (**2**, p. 33) shows that $W = \{[\gamma][p-1]^{-1}; \gamma \in \mathfrak{P}\}$ is a set of generators for H'. As a first approximation, we prove

LEMMA 8. *H' is abelian.*

Proof. From (9) it follows that

$$[\gamma]^{([0][p-1]^{-1})^k} = [(0*p-1\circ)^k\gamma] = [\gamma + (n_1/n_3)k]$$

and that

$$[\gamma]^{[\alpha][p-1]^{-1}} = [\alpha * (p-1)\circ\gamma] = [\gamma + (n_1/n_3)(\alpha+1)].$$

Let $\bar{\xi}$ be the integer in S_p that corresponds to the element ξ of $\mathfrak{P}$. Then we have, for all $\alpha, \gamma \in \mathfrak{P}$,

$$[\gamma]^{([0][p-1]^{-1})^{\bar{\alpha}+1}} = [\gamma]^{[\alpha][p-1]^{-1}}.$$

https://doi.org/10.4153/CJM-1966-004-3 Published online by Cambridge University Press

The elements $([0][p-1]^{-1})^{\bar{\alpha}+1}$ and $[\alpha][p-1]^{-1}$ then define the same inner automorphism of H. In other words,

$$([0][p-1]^{-1})^{\bar{\alpha}+1} \equiv [\alpha][p-1]^{-1} \pmod{\zeta(H)}.$$

Since $\{[\alpha][p-1]^{-1}; \alpha \in \mathfrak{P}\}$ generates H', H' is cyclic mod $\zeta(H)$ and the lemma is proved.

It is clear that, for any α and β in $\mathfrak{P}$, $[\alpha][\beta]^{-1} \in H'$. It then follows from Lemma 8 that, for all $\alpha, \beta, \gamma \in \mathfrak{P}$,

$$[\gamma][\beta]^{-1}[\alpha][\beta]^{-1} = [\alpha][\beta]^{-1}[\gamma][\beta]^{-1}$$

or, equivalently,

$$[\gamma][\beta]^{-1}[\alpha] = [\alpha][\beta]^{-1}[\gamma], \qquad \alpha, \beta, \gamma \in \mathfrak{P}.$$

Thus

$$[\alpha][\beta]^{-1} = [\gamma][\beta]^{-1}[\alpha][\gamma]^{-1} = [\gamma * \beta]^{-1}[\gamma * \alpha]$$

for any choice of γ in $\mathfrak{P}$. If we let $\gamma = (n_3\beta - n_2\alpha)/n_1$, we find that

$$[\alpha][\beta]^{-1} = \left[\frac{n_3\,\beta - n_2\,\alpha + n_2\,\beta}{n_3}\right]^{-1}[\beta],$$

and hence

$$[\alpha][\beta]^{-2} = \left[\frac{(n_3\,\beta - n_2(\alpha - \beta))}{n_3}\right]^{-1}. \tag{12}$$

Now,

$$[\alpha]^{-1}[\beta][\alpha]^{-1} = [\alpha]^{-1}[\beta][\alpha][\alpha]^{-2} = [\alpha \circ \beta][\alpha]^{-2} \tag{13}$$

and applying (12) to the right-hand side of (13), we obtain

$$[\alpha]^{-1}[\beta][\alpha]^{-1} = [2\alpha - \beta]^{-1}. \tag{14}$$

Suppose now that for some positive integer k and some α in $\mathfrak{P}$

$$[\alpha][p-1]^{-1} = ([0][p-1]^{-1})^{k}.$$

Then

$$\begin{aligned}
([0][p-1]^{-1})^{k+2} &= [0][p-1]^{-1}([0][p-1]^{-1})^{k-1}[0][p-1]^{-1}[0][p-1]^{-1} \\
&= ([0][p-1]^{-1}[\alpha][p-1]^{-1}[0])[p-1]^{-1} \\
&= [0][p-1]^{-1}[\alpha][p-1]^{-1}[0] = [0][-2-\alpha]^{-1}[0] \\
&= [2+\alpha]
\end{aligned}$$

by (14). Hence

$$[\alpha+2][p-1]^{-1} = ([0][p-1]^{-1})^{k+2}.$$

It follows immediately from these considerations that

$$([0][p-1]^{-1})^{2k+1} = [2k][p-1]^{-1}.$$

Since, by (14),

$$([0][p-1]^{-1})^2 = [0][p-1]^{-1}[0][p-1]^{-1} = [1][p-1]^{-1},$$

it also follows that $([0][p-1]^{-1})^{2k} = [2k-1][p-1]^{-1}$. Finally, we have

$$[k][p-1]^{-1} = ([0][p-1]^{-1})^{k+1}. \tag{15}$$

We have now essentially proved

PROPOSITION 9. *H' is cyclic of order p.*

Proof. Since the set $\{[k][p-1]^{-1}; k \in \mathfrak{P}\}$ generates H', (15) assures that H' is cyclic. To see that H' has order p, it suffices to note that

$$([0][p-1]^{-1})^p = [p-1][p-1]^{-1}.$$

4. The structure of *H*. We are now in a position to prove the main theorem. We remind the reader that we defined the group M as

$$M = \mathrm{gp}(a, b; b^p = 1, a^{-1} b^{n_2} a = b^{n_3}).$$

The relations (15) assure us that the elements $[p-1]$ and $[0][p-1]^{-1}$ together generate H. Let $c = [p-1]$ and $d = [0][p-1]^{-1}$. Then $d^p = 1$ and

$$\begin{aligned} c^{-1} d^{n_2} c &= [p-1]^{-1}([0][p-1]^{-1})^{n_2}[p-1] = ([n_1/n_2][p-1]^{-1})^{n_2} \\ &= ([0][p-1]^{-1})^{n_2}((n_1/n_2)+1) = d^{n_3}. \end{aligned}$$

The correspondence $a \to c$, $b \to d$ can then be extended to an epimorphism $\Phi : M \to H$.

To show that H is an epimorphic image of M, we define for every $\alpha \in S_p$ the element $z(\alpha) = b^{\alpha+1}a$ of M. The set $\{z(\alpha); \alpha \in S_p\}$ clearly generates M and

$$(z(\alpha)z(\beta)z(\alpha))^{-1} = b^{\alpha+1}ab^{\beta+1}aa^{-1}b^{-(\alpha+1)} = b^{\alpha+1}ab^{\beta-\alpha}.$$

Let us again consider n_2 and n_3 as elements of $\mathfrak{P}$. Then b^{n_3/n_2} is defined and $ab^k = b^{(n_3/n_2)k}a$. Hence

$$b^{\alpha+1}ab^{\beta-\alpha} = b^{\alpha+((\beta-\alpha)n_2/n_3)+1}a = b^{(\alpha*\beta)+1}a.$$

Consequently,

$$z(\alpha)z(\beta)(z(\alpha))^{-1} = z(\alpha * \beta)$$

and the correspondence $[\alpha] \to z(\alpha)$ can again be extended to an epimorphism $\Psi: H \to M$.

It is easy to verify that Φ and Ψ are mutually inverse. Φ is then an isomorphism and the proof is complete.

https://doi.org/10.4153/CJM-1966-004-3 Published online by Cambridge University Press

REFERENCES

1. A. H. Clifford, *A noncommutative ordinally simple linearly ordered group*, Proc. Amer. Math. Soc., *2* (1951), 902–903.
2. A. G. Kurosh, *The theory of groups*, vol. II (New York, 1955).

Courant Institute of Mathematical Sciences,
New York, New York, and
California Institute of Technology,
Pasadena, California