Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Brunetto Piochi

Permutability of centre-by-finite groups

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **83** (1989), n.1, p. 153–158.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1989_8_83_1_153_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1989.

Atti Acc. Lincei Rend. fis.
(8), LXXXIII (1989), pp. 153-158

Teoria dei gruppi. — *Permutability of centre-by-finite groups.* Nota di BRUNETTO PIOCHI, presentata (*) dal Socio G. ZAPPA.

ABSTRACT. — Let G be a group and m be an integer greater than or equal to 2. G is said to be m-permutable if every product of m elements can be reordered at least in one way. We prove that, if G has a centre of finite index z, then G is $(1 + [z/2])$-permutable. More bounds are given on the least m such that G is m-permutable.

KEY WORDS: Centre-by-Finite Groups; Rewritable groups; Permutability.

RIASSUNTO. — *Sulla permutabilità dei gruppi centro-per-finito.* Dato un gruppo G, si forniscono alcune limitazioni al minimo intero m tale che ogni prodotto di m elementi di G possa essere riordinato. In particolare, si prova che se il centro di G ha indice finito z allora $m \leq 1 + [z/2]$.

Let G be a group. G will be said to have the property P_m, or to be *m-permutable* (for short $G \in P_m$) if every product of m elements in G can be rewritten (re-ordered), *i.e.* if for each m-tuple $(c_1, c_2, \ldots c_m)$ of elements of G there exists a non trivial permutation f on the set $\{1, 2, \ldots, m\}$, such that:

$$c_1 c_2 \ldots\ldots c_m = c_{f(1)} c_{f(2)} \ldots\ldots c_{f(m)} .$$

A group G will be said to be *permutable* if $G \in P_m$ for some m.

Such a property is a finiteness condition: a finitely generated torsion group (a.f.g. periodic semigroup, indeed, see [6]) is finite if and only if it is m-permutable for some m [2]. Curzio et al. characterized in [3] permutable groups: they are exactly the finite-by-Abelian-by-finite groups.

If G is a permutable group, a natural problem arises: which is the least integer m such that $G \in P_m$? Denote by $m(G)$ such an integer. In [5] it is shown that for finite groups,

$$\lim_{|G| \to \infty} m(G)/|G| = 0 :$$

however the proof does not entail any efficient suggestion on $m(G)$ for relatively small groups, or for infinite permutable groups. On the contrary, this is given by the following result:

PROPOSITION 1 [3]. *If* $|G'| = h$, *then* $G \in P_{h+1}$. *If there exists an m-permutable subgroup N of G of index h, then* $G \in P_{hm}$.

PROP. 1. Gives some immediate bounds for $m(G)$; e.g. the alternating group A_5 is immediately seen to be 20-permutable.

If the centre of G has a finite index, say $|G/Z(G)| = z$, (in the following z will always denote the index of $Z(G)$) then by Prop. 1. $G \in P_{2z}$. But the existence of a non-trivial centre $Z(G)$ of G should naturally have a stronger effect on $m(G)$. In fact, we shall prove that $G \in P_{1+[z/2]}$ ($[h]$ will denote the greatest integer less than or equal to h). More generally, if p is the least prime number dividing z, then $G \in P_{1+[z/(p-1)]}$.

(*) Nella seduta del 26 novembre 1988.

FINITE GROUPS.

If G is a finite group of order n, then G is trivially n-permutable. Longobardi and Maj (unpublished; reported in [1]) proved that G has the property $P_{[2(n+1)/3]}$. In [4] Garzon and Zalcstein remarked that, if the finite group G has a non-trivial centre of index z, then certainly $G \in P_{z+1}$.

Both results can be easily generalized, as follows: let $C_k = c_1 c_2 \dots c_k$ be the product of a sequence of k elements of G. Consider, for $i = 1, \dots, [k/2]$, the cosets $c_{2i-1}Z(G)$, $c_{2i}Z(G)$, $c_{2i-1}c_{2i}Z(G)$. If the sequence C_k cannot be rewritten, then all these cosets must be different: thus $k \leq 2z/3 + 1$. It immediately follows that G belongs to $P_{[2(z+1)/3]}$.

If G is finite, however, another generalization can be easily obtained. Namely:

COROLLARY 1. *Let G be any finite group G of order n and let p be the least prime integer dividing n; then G belongs to $P_{(n/p)+1}$.*

PROOF. If the order of G is divided by a prime p (or p^2), then by Prop. 1, $G \in P_{2n/p}$ (resp. $P_{2n/p}$). Thus, if G has an Abelian subgroup of order greater than or equal to 4, then $G \in P_{[n/2]}$; if this is not true, then $|G| \leq 6$: hence G is Abelian or it is isomorphic to the symmetric group S_3, which belongs to P_4. Thus, generally $G \in P_{[n/2]+1}$.

Now, suppose that the least prime number dividing n is $p > 2$. Then $|G'| \leq n/p$, and, again by Prop. 1, $G \in P_{n/p+1}$. #

Moreover, let us recall that any p-group G of order p^h, has a normal Abelian subgroup of order p^a, with $a(a+1) \geq 2h$ (see e.g. [7]). It follows immediately that the exponent a must fulfill:

$$h \geq a \geq \left(-1 + \sqrt{1 + 8h}\right)/2 .$$

Denote by $f(h)$, for each integer h, the least integer greater than or equal to

$$\left(-1 + \sqrt{1 + 8h}\right)/2.$$

Let now $n = p_1^{h_1} p_2^{h_2} \dots p_j^{h_j}$ be the order of the finite group G. If N is any p_i-Sylow subgroup of G $(i = 1, \dots j)$, then N has an Abelian subgroup of order $p_i^{f(h_i)}$. Thus, by Prop. 1.:

PROPOSITION 2. *Let $|G| = n = p_1^{h_1} p_2^{h_2} \dots p_j^{h_j}$ and let i be the index of the maximum power $p_i^{f(h_i)}$ $(1 \leq i \leq j)$. Then G has the permutation property P_m with $m = 2n/p_i^{f(h_i)}$.* #

One more bound can be obtained in general for the integer $m(G)$ if we look at the «permutable coverings» of G; namely:

PROPOSITION 3. *If there exists a finite family $\{H_i, 1 \leq i \leq h\}$ of groups such that $G \subset \bigcup_i H_i$, and $H_i \in P_{m_i}$ then $G \in P_m$, with $m = 1 + \sum_{i=1}^{h} (m_i - 1)$.*

PROOF. Consider a sequence C_k of elements of G which cannot be re-ordered: it cannot happen that m_i different left factors of C_k lie in the same subgroup H_i, for $1 \leq i \leq h$. But if $k \geq 1 + \sum_{i=1}^{h} (m_i - 1)$, this must happen for at least one i. Thus, we immediately get a re-ordering of the sequence. #

Centre-by-finite groups.

In the following, we want to give bounds for the integer $m(G)$, when G is not necessarily finite, but the centre of G has a finite index z.

Let us start with some general remarks on the sequences of elements of G. Let $C_k = c_1 c_2 \ldots\ldots c_k$ be the product of any sequence of elements: k will be said the *length* of C_k; a subsequence $c_i \ldots c_j$ with $1 \leq i \leq j \leq k$ will be called a *segment* of C_k; a segment will be called a *prefix* if $i = 1$, a *suffix* if $j = k$.

Lemma 1. *If one of the following holds, then the sequence C_k of elements of G can be re-ordered*:

1) $c_g \ldots c_i \in (c_j \ldots c_h) Z(G)$, *where* $i < j$ *or* $h < g$;

2) $c_g \ldots c_i \in (c_j \ldots c_h) Z(G)$, *where one segment is a proper prefix or suffix of the other*;

3) $c_g \ldots c_i \in (c_g \ldots c_i \ldots c_j)^{-1} Z(G)$, *where* $i < j$.

Proof. 1) Suppose $i < j$; we have:

$$c_1 \ldots c_g \ldots c_i \ldots c_j \ldots c_h \ldots c_k = c_1 \ldots c_{g-1} c_j \ldots c_h x c_{i+1} \ldots c_j \ldots c_h \ldots c_k =$$
$$= c_1 \ldots c_{g-1} c_j \ldots c_h c_{i+1} \ldots c_{j-1} c_g \ldots c_i c_{h+1} \ldots c_k,$$

for some $x \in Z(G)$.

2) trivially, after having cancelled the common elements, it remains a segment of the sequence C_k which is central.

3) Since $c_g \ldots c_i = (c_{i+1} \ldots c_j)^{-1} (c_g \ldots c_i)^{-1} x$, for some $x \in Z(G)$, then $(c_{i+1} \ldots c_j) = (c_g \ldots c_i)^{-2} x$ commutes with $(c_g \ldots c_i)$. #

Let us now state two results on the sequences of a group G:

Proposition 4. *Let A be a (possibly trivial) subgroup of G such that A has a finite index a in G. Every sequence C_a contains a segment which is in A.*

Proof. Consider all the prefixes of C_a:

$$c_1$$
$$c_1 c_2$$
$$\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots$$
$$c_1 c_2 \ldots\ldots c_a.$$

They are a elements of G. If one of them is in A, then we have finished; otherwise, two elements are in the same (say: left) coset of A; that is there exist $y \in G$, $t, t' \in A$ such that:

$$c_1 \ldots c_i = yt$$
$$c_1 \ldots c_i \ldots c_j = yt',$$

Thus,

$$c_{i+1} \ldots c_j = t^{-1} t' \in A. \quad \#$$

PROPOSITION 5. *Let A be a normal subgroup of G, of finite index a. If a sequence $C_{[(a+1)/2]}$ does not contain any segment lying in A, then it contains a segment which belongs to the coset xA, for* **every** $x \in G \setminus A$ such that $x^2 \in A$.

PROOF. Consider again the prefixes of $C_{[(a+1)/2]}$ and then multiply them by x, x being any non-trivial element such that $x^2 \in A$, but $x \notin A$:

$$\begin{array}{ll} c_1 & c_1 x \\ c_1 c_2 & c_1 c_2 x \\ \dots\dots & \dots\dots \\ \dots\dots & \dots\dots \\ c_1 c_2 \dots\dots c_{[(a+1)/2]} & c_1 c_2 \dots\dots c_{[(a+1)/2]} x \end{array}$$

They are at least a elements. Suppose that no segment of the sequence is in A.

If $c_1 \dots c_i x \in A$, then we get

$$c_1 \dots c_i \in Ax^{-1} = Ax = xA .$$

If not, we must have one of the following cases:

i) $c_1 \dots c_i$ and $c_1 \dots c_i \dots c_j$ belong to the same coset of A; this implies that a segment of the sequence is in A;

ii) $c_1 \dots c_i x$ and $c_1 \dots c_i \dots c_j x$ belong to the same coset of A; this implies again that:

$$c_{i+j} \dots c_j \in xAx^{-1} = A ;$$

iii) $c_1 \dots c_i$ and $c_1 \dots c_i \dots c_j x$ belong to the same coset of A (we may suppose $j > i$ without loss of generality); then:

$$c_{i+1} \dots c_j \in Ax^{-1} = Ax = xA . \qquad \#$$

If G is finite, then we can choose $A = \{1\}$:

COROLLARY 2. *Let G be a finite group.*

Every sequence C_n of elements of G contains a segment which is equal to 1.

If a sequence $c_{[(n+1)/2]}$ does not contain any segment equal to 1, *then it contains a segment equal to x, for* **every** *$x \in G$ such that $x^2 = 1$, $x \neq 1$.* #

Let now $W = \{xZ(G) \in G/Z(G) : x \notin Z(G)$ and $x^2 \in Z(G)\}$; say $|W| = w$.

PROPOSITION 6. *In a sequence which cannot be re-ordered, there cannot be more than $[(1+w)/2]$ prefixes (suffixes) belonging to different cosets in W.*

PROOF Let a, ab be two different prefixes in a sequence C_k, which cannot be re-ordered. Suppose that $aZ(G)$ and $abZ(G)$ belong to W. One can easily see that $bab \in aZ(G)$ and $baZ(G) \in W$. Suppose that ba belongs to the same coset with a prefix of C_k and say:

$$a = c_1 \dots c_i , \qquad b = c_{i+1} \dots c_j , \qquad ba \in c_1 \dots c_h Z(G) .$$

If $h = i$, then $b \in Z(G)$.

If $h>j$, then say $c_{j+1}\dots c_h=c$; we get:

$$ba\in abcZ(G)\,,\qquad bab\in abcb\,Z(G),\qquad bcb\in Z(G)$$

and b commutes with c.

If $h<i$, then say $c_{h+1}\dots c_i=c$; we get:

$$bac\in a\,Z(G)=bab\,Z(G),\qquad c\in b\,Z(G)\,,$$

and again b commutes with c.

If $i<h<j$, then say $c_{i+1}\dots c_h=c$ and $c_{h+1}\dots c_j=d$; we get:

$$ba\in ac\,Z(G)\quad\text{ and }\quad bad\in ab\,Z(G);$$

hence

$$c\in b^{-1}Z(G)\quad\text{ and }\quad d\in(ba)(ab)\,Z(G)=ba^2bZ\,(G)=b^2Z(G)\,;$$

thus c and d commute.

All these lead to a contradiction. Thus, it must be $h=j$, that is $ba\in ab\,Z(G)$, whence $b\in abaZ(G)=b^{-1}Z(G)$ and $bZ(G)\in W$. By similar arguments, it can be seen that b cannot be in the same coset with any prefix of the sequence: in fact, if we suppose that $b\in c_1\dots c_g Z(G)$, then trivially $g\neq i,j$; also, if $g<i$ or $i<g<j$, then we can commute a and b; at last, if $g>j$, then we get $b\in abx\,Z(G)=baxZ(G)$, where x is the segment $c_{j+1}\dots c_g$, which is immediately seen to belong to $a^{-1}Z(G)=aZ(G)$, thus allowing a re-ordering of the sequence.

Now, let $a_1,\ a_1a_2,\dots,a_1a_2\dots a_h$ be the prefixes of C_k, which belong to W. We have shown that, for $f=1,\dots,h$, the cosets of $a_2\dots a_fa_1$ (or correspondingly of $a_2\dots a_f$) are elements of W, but do not correspond to any prefix of C_k. All of them must be trivially different from each other, or the sequence could be re-ordered; thus they are exactly $h-1$.

Hence, it must be $h+h-1\le w$ and $h\le(1+w)/2$. #

Theorem 1. *Let G be a group. If the centre $Z(G)$ has a finite index z, then $G\in P_{[z/2]+1}$.*

Proof. Let C_k be a sequence which cannot be re-ordered; consider all the cosets of $Z(G)$ containing the prefixes or their inverses:

$$\begin{array}{ll}
c_1 & c_1^{-1}\\
c_1c_2 & (c_1c_2)^{-1}\\
\dots\dots\dots & \dots\dots\dots\\
\dots\dots\dots & \dots\dots\dots\\
c_1\dots\dots c_k & (c_1\dots\dots c_k)^{-1}.
\end{array}$$

An immediate consequence of Lemma 1. is that all cosets of the elements in the left (or in the right) column are different from each other and that an element in the left column is in the same coset with one in the right column if and only if that coset belongs to W.

If these are exactly h, then we get $2k-h$ different cosets.

Also, none of the present cosets can be $Z(G)$ itself. Hence k must fulfil the condition:

$$2k - h \leq n/z - 1 - (w - h),$$

which by Prop. 6, implies:

$$2k \leq n/z - (w - 2h + 1) \leq n/z.$$

Thus, if $m \geq 1 + [n/2z]$, then G must be m-permutable. #

THEOREM 2. *Let G be a group; suppose that its centre has a finite index z and let p be the least prime number dividing z. Then $G \in P_{[z/(p-1)]+1}$.*

PROOF. Consider the following cosets of $Z(G)$, for a product C_k which cannot be re-ordered:

$$\begin{array}{cccc}
c_1 Z(G) & (c_1)^2 Z(G) & \ldots\ldots. & (c_1)^{p-1} Z(G) \\
c_1 c_2 Z(G) & (c_1 c_2)^2 Z(G) & \ldots\ldots. & (c_1 c_2)^{p-1} Z(G) \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots. & \ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots. & \ldots\ldots\ldots\ldots \\
c_1 \ldots\ldots c_k Z(G) & (c_1 \ldots\ldots c_k)^2 Z(G) & \ldots\ldots. & (c_1 \ldots\ldots c_k)^{p-1} Z(G)
\end{array}$$

All of them are trivially different from $Z(G)$, since every exponent is prime to the order of the corresponding prefix, and no prefix must be central. A similar argument shows that it cannot be:

$$(c_1 \ldots\ldots c_i)^h Z(G) = (c_1 \ldots\ldots c_j)^{h'} Z(G).$$

In fact, if it were true, suppose $j > i$, we would have that, for some integer q,

$$c_1 \ldots\ldots c_j \in (c_1 \ldots c_i)^{hq} Z(G).$$

This implies that the sequence could be re-ordered, as a segment is in the same coset of $Z(G)$ with an adjacent one.

Thus, it must be:

$$k(p-1) \leq n + z - 1,$$

and this proves the result. #

REFERENCES

[1] CURZIO M., 1985. *Sul problema di Burnside.* Quad. Ist. Mat. Appl. Univ. L'Aquila, 8: 1-24.
[2] CURZIO M., LONGOBARDI P. and MAJ M., 1983. *Su di un problema combinatorio in Teoria dei Gruppi.* Atti Acc. Lincei Rend. fis., VIII, 74: 136-142.
[3] CURZIO M., LONGOBARDI P., MAY M. and ROBINSON D. J. S., 1985. *A permutational property of groups.* Arch. Math., 44: 385-389.
[4] GARZON M. and ZALCSTEIN Y., 1987. *On permutation properties in groups and semigroups.* Semigroup Forum, 35: 337-351.
[5] PIOCHI B. and PIRILLO G., 1988. *Sur une propriété combinatoire des groupes finis.* C.R. Acad. Sci. Paris, 307, I: 115-117.
[6] RESTIVO A. and REUTENAUER C., 1984. *On the Burnside problem for semigroups.* J. Algebra, 89; 102-104.
[7] SUZUKI M., 1982. *Group Theory I.* Springer Verlag, Berlin.