Reprinted from JOURNAL OF ALGEBRA
Vol. 48, No. 2, October 1977

Printed in Belgium

Correction to "$\aleph_0$-Categoricity of Groups"

JOSEPH G. ROSENSTEIN

Department of Mathematics, Rutgers University, The State University of New Jersey, New Brunswick, New Jersey 08903

Communicated by Walter Feit

Received May 20, 1975

In [1, Sect. 4] I dealt with certain metabelian groups which were called $n - k$ groups. A group G is an $n - k$ group if G has a normal Abelian subgroup H of exponent n such that G/H is cyclic of order k. I stated various results leading up to Theorem 13 which asserts that every $n - q$ group is $\aleph_0$-categorical where q is a prime and n is square-free.

The proofs of these results have been called into question by Professor Gabriel Sabbagh who pointed out that I had made the erroneous assumption, sometimes explicitly and sometimes implicitly, that if G/H is cyclic of order k then an element x of G can be chosen so that xH generates G/H and so that $x^k = 1$. Although this assumption is false in general, the results of this section are correct, subject to certain modifications, and the theorems are correct as stated—as is demonstrated shortly.

Throughout the subsequent discussion G is a fixed $n - k$ group with normal Abelian subgroup H of exponent k and x is an element of G such that $G/H = \langle xH \rangle$.

For any $h \in H$ and any $y \in G$ we define h^y to be $y^{-1}hy$ and, more generally, for any $h \in H$ and any $y_1, y_2, \ldots, y_m \in G$ we define $h^{y_1+y_2+\cdots+y_m}$ to be $h^{y_1}h^{y_2} \cdots h^{y_m}$. We also define h^{-y} to be $(h^{-1})^y = (h^y)^{-1}$ for any $h \in H$ and $g \in G$. Let F_G be the free Abelian group freely generated by the elements of G. Then the definitions above induce in a natural way the definition of an element $h^z \in H$ for any $z \in F_G$ and any $h \in H$. We can also define multiplication in a natural way on F_G, extending the multiplication of G, so that F_G becomes a ring, called the group-ring of G.

LEMMA 1. (1) $(h^{z_1})^{z_2} = h^{z_1 z_2}$ *for any* $z_1, z_2 \in F_G$, $h \in H$.

(2) $h^{z_1+z_2} = h^{z_1}h^{z_2}$ *for any* $z_1, z_2 \in F_G$, $h \in H$.

(3) $h^{-z} = (h^{-1})^z = (h^z)^{-1}$ *for any* $z \in F_G$, $h \in H$.

(4) $(h_1h_2)^z = h_1^z h_2^z$ *for any* $z \in F_G$ *and* $h_1, h_2 \in H$.

ISSN 0021-8693

LEMMA 2. *For any $m \geqslant 0$ and any $h \in H$*

$$(xh)^m = x^m h^{1+x+\cdots+x^{m-1}}.$$

Proof. By induction on m.

We now define a function $N: H \to H$ (N for "norm") by $N(h) = h^{1+x+\cdots+x^{k-1}}$. This is a homomorphism whose image $\mathrm{Im}(N)$ is a subgroup of $C_H(x)$ (the centralizer of x in H) since $x^{-1}N(h)x = h^{(1+x+\cdots+x^{k-1})x} = N(h)$ because $x^k \in H$ implies $h^{x^k} = h = h^1$.

But $\{y^k \mid y \in xH\} = x^k\,\mathrm{Im}(N)$ by Lemma 2, so there is a $y \in xH$ such that $y^k = 1$ iff $1 \in x^k\,\mathrm{Im}(N)$ iff $x^{-k} \in \mathrm{Im}(N)$ iff $x^k \in \mathrm{Im}(N)$.

PROPOSITION 1. *If $(n, k) = 1$, then there is a $y \in G$ such that $G/H = \langle yH \rangle$ and $y^k = 1$.*

Proof. It suffices to show that $x^k \in \mathrm{Im}(N)$, which would follow if $C_H(x) \subseteq \mathrm{Im}(N)$ since $x^k \in C_H(x)$. But for any element $h \in C_H(x)$, we have

$$N(h) = h^{1+x+\cdots+x^{k-1}} = h^k;$$

and given any $c \in C_H(x)$, if c has order $t \mid n$ then, if $at + bk = 1$, we have $(c^b)^k = c^{1-at} = c$ so that $h = c^b$ is a kth root of c in H. So $N(h) = N(c^b) = (c^b)^k = c$ and $C_H(x) \subseteq \mathrm{Im}(N)$. ▮

Hence the proofs of the various propositions involving $n - k$ groups with $(n, k) = 1$ are correct as long as we are careful to select an x for which $x^k = 1$. Thus the questions about the correctness of Proposition 1, Theorems 5 and 6, Proposition 3, Theorem 10a, and Proposition 3′ are resolved.

We turn now to a discussion of p–p groups. Proposition 2 (concerning 2–2 groups), Proposition 4 (concerning 3–3 groups), and Proposition 4′ (concerning p–p groups) are correct, modulo a few emendations. (Each use of the "fact" that $x^k = 1$ can be replaced by a similar use of the fact that $x^k \in H$, and so commutes with every element of H; each word of the form xwx in the statement of Proposition 1 should be replaced by $x^{-1}wx$.) The theorems based on these propositions are also correct—that is, every p–p group is $\aleph_0$-categorical. The application of the propositions in the theorems, however, is incorrect.

More specifically, in Proposition 2 (resp. 4) we show that we can assign two (resp. 3) invariants to each 2–2 group (resp. 3–3 group). We then claim that for each such set of invariants there is a unique 2–2 group (resp. 3–3 group) with those invariants and furthermore that group is $\aleph_0$-categorical. This is incorrect. What is true is that for each such set of invariants there are exactly two 2-2 groups (resp. three 3-3 groups) with those invariants and, furthermore, each of these groups is $\aleph_0$-categorical.

We prove this result in the general case, for an arbitrary prime p. (In the case

$p = 2$, Proposition 2 may be applied directly to give the result, but Proposition 4, although correct, is not sufficiently informative.)

We first define a function $g: H \to H$ by $g(h) = h^{x-1} = h^{-1}(x^{-1}hx)$. Then $\ker(g) = C_H(x)$ and $\mathrm{Im}(g) = \{z \in H \mid (\exists h \in H)(x^{-1}hx = hz)\}$. Since $h^{pz} = (h^z)^p = 1$ for any $z \in F_G$ it follows that $h^{(x-1)^p} = h^{x^p-1} = 1$ so that $g^p(h) = 1$ for all h. Also since $N(h) = h^{(1+x+\cdots+x^{p-1})} = h^{(x^p-1/x-1)} = h^{((x-1)^p/x-1)} = h^{(x-1)^{p-1}} = g^{p-1}(h)$, we see that $g^{p-1}(h) = N(h)$ for all $h \in H$.

We note also that by the remarks preceding Proposition 1, we may assume, without loss of generality, that if $x^p \in \mathrm{Im}(N)$, then $x^p = 1$, and hence that if $x^p \in \mathrm{Im}(g^{p-1})$ then $x^p = 1$.

PROPOSITION 2. *Let G be a p–p group and let xH generate G/H. Then there are subgroups $H_1, H_2, \ldots, H_p$ of H such that*

(i) $H = H_1 \oplus H_2 \oplus \cdots \oplus H_p$,

(ii) $H_1 \oplus \cdots \oplus H_i = \ker(g^i)$ *for each* i, $1 \leqslant i \leqslant p$,

(iii) *for each* i, $1 \leqslant i \leqslant p$, *there are subgroups* $H_i^i, H_i^{i+1}, \ldots, H_i^p$ *of* H_i,

so that

(a) $H_i = H_i^i \oplus H_i^{i+1} \oplus \cdots \oplus H_i^p$,

(b) *g maps H_{i+1}^t isomorphically onto H_i^t for all $i \geqslant 1$ and all $t \geqslant i+1$.*

(iv) *There is an $i \leqslant p$ such that $x^p \in H_1^i$; furthermore, if $x \in H_1^p$ then* $x^p = 1$.

Proof. Before proving this, we observe that the proposition implies that H can be decomposed into $(p(p+1))/2$ subgroups which can be pictured as follows:

H_1	H_1^1	H_1^2	H_1^3	$\cdots$	H_1^{p-2}	H_1^{p-1}	H_1^p
H_2		H_2^2	H_2^3	$\cdots$	H_2^{p-2}	H_2^{p-1}	H_2^p
H_3			H_3^3	$\cdots$	H_3^{p-2}	H_3^{p-1}	H_3^p
$\vdots$				$\ddots$		$\vdots$	
H_{p-2}					H_{p-2}^{p-2}	H_{p-2}^{p-1}	H_{p-2}^{p-1}
H_{p-1}						H^{p-1}	H^p

The top row is $C_H(x) = \ker(g)$; the top i rows add up to $\ker(g_i)$. The function g maps each box isomorphically onto the box immediately above it—except of course that the top row is mapped by g to 1. The image of g then consists of all boxes except the left-most of each row, and, more generally, the image of g^i consists of all boxes except the i left-most boxes of each row. Thus $\mathrm{Im}(g^{p-1}) = \mathrm{Im}(N) = H_1{}^p$.

It is clear that we need only define $H_i{}^1$ for each i since $H_j{}^i$ must be $g^{i-j}(H_i{}^i)$ for each i and each $j < i$.

We choose $H_p{}^p$ so that

$$\ker g^{p-1} \oplus H_p{}^p = \ker g^p = H$$

and we define $H_i{}^p$ to be $g^{p-i}(H_p{}^p)$ for all $i < p$.

Assume inductively that $H_j{}^j$ has been defined for all $j > i$, that $H_t{}^j = g^{j-t}$ for all $t < j$, and that if $x^p \in H_1{}^j \oplus H_1^{j+1} \oplus \cdots \oplus H_1{}^p$ then $x^p \in H_1{}^t$ for some t, $j \leqslant t \leqslant p$.

Proceeding to step i, we first choose H_0 so that $\ker(g^{i-1}) \oplus H_0 \oplus H_i^{i+1} \oplus \cdots \oplus H_i{}^p = \ker(g^i)$. If $x^p \notin (g^{i-1}(H_0) \oplus H_1^{i+1} \oplus \cdots \oplus H_1{}^p) - (H_1^{i+1} \oplus \cdots \oplus H_1{}^p)$ then we let $H_i{}^i$ be H_0 and we let $H_t{}^i$ be $g^{i-t}(H_i{}^i)$ for $t < 1$. If not, then we choose $H_i{}^i$ so that $x^p \in g^{i-1}(H_i{}^i)$. Indeed suppose $x^p = ab$ where $a \in g^{-1}(H_0)$ and $b \in H_1^{i+1} \oplus \cdots \oplus H_1{}^p$, find a' and b' so that $a' \in H_0$, $b' \in H_i^{i+1} \oplus \cdots \oplus H_i{}^p$, $g^{i-1}(a') = a$, and $g^{i-1}(b') = b$, and choose $H_i{}^i$ so that

$$H_i{}^i \oplus H_i^{i+1} \oplus \cdots \oplus H_i{}^p = H_0 \oplus H_i^{i+1} \oplus \cdots \oplus H_i{}^p$$

and so that $a'b' \in H_i{}^i$. Define $H_t{}^i$ to be $g^{i-t}(H_i{}^i)$ for $t < i$. In this case, $x^p = ab = g^{i-1}(a'b') \in H_1{}^i$.

It is easily verified that if we define $H_1, \ldots, H_p$ so that Proposition 2(iii)(a) holds, then (i) and (ii) also hold. To verify that g maps H_{i+1}^t isomorphically onto $H_i{}^t$ for each $i \geqslant 1$ and each $t \geqslant i+1$ we observe that if $g(h_1) = g(h_2)$ then $g(h_1 h_2^{-1}) = 1$ so that $h_1 h_2^{-1} \in \ker(g)$; but the only element of H_{i+1}^t which is also in $\ker(g)$ is 1, so that $h_1 = h_2$. Finally (v) is correct since either x^p is in $H_1{}^1$, or $H_1{}^2$, or $\cdots$ or H_1^{p-1} or $x^p \in H_1{}^p$ in which case $x^p = 1$ by the remarks preceding the proposition.

Thus with each p–p group we can associate the invariants $\langle m_1, m_2, \ldots, m_p\rangle$ by stipulating that m_i is the cardinality of a basis of $H_i{}^i$. For each p-tuple $\langle m_1, m_2, \ldots, m_p\rangle$ of cardinal $\leqslant \aleph_0$ there are at most p distinct groups with those invariants, and, assuming that $m_i > 0$ for $i = 1, \ldots, p-1$, there are exactly p distinct groups with those invariants. For it is clear that if we are given two p–p groups G and G' with subgroups H and H' and $G/H = \langle xH\rangle$ and $G'/H' = \langle x'H'\rangle$; and if we define g and the $H_j{}^i$'s and g' and the (H'^i_j)'s as in Proposition 2, then $G \simeq G'$ iff $x^p \in H_1{}^i \leftrightarrow x^p \in H'^i_1$. This completes the verification of the claims made earlier and thus we have proved

THEOREM. *Every p–p group is* $\aleph_0$*-categorical.*

Thus the following is also correct.

THEOREM 13. *Let n be square-free and p a prime. Then every n–p group is* $\aleph_0$*-categorical.*

ACKNOWLEDGMENT

I am greatly indebted to Professor Richard Lyons who provided information and observations upon which this note is based.

REFERENCE

1. JOSEPH G. ROSENSTEIN, $\aleph_0$-categoricity of groups, *J. Algebra* **25** (1973), 435–467.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.