This department welcomes short notes and problems believed to be new. Contributors should include solutions where known, or background material in case the problem is unsolved. Send all communications concerning this department to I. G. Connell, Department of Mathematics, McGill University, Montreal, P. Q.

GROUPS IN WHICH RAISING TO A POWER IS AN AUTOMORPHISM

H. F. Trotter

For any group G and integer n, let $P_n : G \to G$ be the function defined by $P_n(g) = g^n$ for all $g \in G$. If G is abelian then P_n is a homomorphism for all n. Conversely, it is well known (and easy to show) that if P_2 or P_{-1} is a homomorphism then G is abelian. As the groups G_n described below show, for every n other than 2 and -1 there exist non-abelian groups for which P_n is a homomorphism.

In this note we derive some elementary consequences of the assumption that P_n is an <u>automorphism</u> for some particular value of n. One somewhat surprising result is that P_3 can be an automorphism only if G is abelian.

We begin with some simple lemmas. Let $H(G)$ be the set of integers n such that P_n is a homomorphism of G, and $A(G)$ the set of integers such that P_n is an automorphism of G. Since the composition of P_n and P_m is P_{mn} we have

(1) If $m, n \in H(G)$ then $mn \in H(G)$.

https://doi.org/10.4153/CMB-1965-063-4 Published online by Cambridge University Press

If $m \in A(G)$ then the identity $P_{mn} = P_m P_n$ may be multiplied by P_m^{-1} to give $P_n = P_m^{-1} P_{mn}$. Writing q for mn, this gives

(2) If $m \in A(G)$, $q \in H(G)$ and m divides q, then $q/m \in H(G)$.

We have $n \in H(G)$ if and only if $h^n g^n = (hg)^n$ for all $h, g \in G$. Setting $h = x^{-1}$, $g = y^{-1}$, so that $hg = (yx)^{-1}$, converts this identity into $x^{-n} y^{-n} = (yx)^{-n}$. Premultiplication by x and postmultiplication by y gives $x^{1-n} y^{1-n} = (xy)^{1-n}$. Therefore

(3) If $n \in H(G)$ then $1-n \in H(G)$.

Now suppose $n \in A(G)$. By (3), $1-n \in H(G)$, and hence by (1), $(1-n)^2 \in H(G)$. By (3) again, $1 - (1-n)^2 = 2n - n^2 \in H(G)$, and by (2), $2-n \in H(G)$. A final application of (3) gives $n-1 \in H(G)$ and we have proved

(4) If $n \in A(G)$ then $n-1 \in H(G)$.

COROLLARY. If P_3 is an automorphism then G is abelian (since P_2 is a homomorphism).

LEMMA. If both n and n+1 are in H(G), then $k \in H(G)$ implies $k' \in H(G)$ for all $k' \equiv k \pmod{n}$.

Proof: By assumption, $g^{n+1} h^{n+1} = (gh)^{n+1} = (gh)^n gh = g^n h^n gh$ for all $g, h \in G$. Cancelling g^n on the left and h on the right gives $gh^n = h^n g$, which shows that all n-th powers are in the centre of G. Now suppose $g^k h^k = (gh)^k$ and let r be any integer. We have $g^{k+nr} h^{k+nr} = g^k h^k (g^n h^n)^r = (gh)^k ((gh)^n)^r = (gh)^{k+nr}$, using the facts that h^n, g^n are in the centre of G and that $n \in H(G)$.

https://doi.org/10.4153/CMB-1965-063-4 Published online by Cambridge University Press

THEOREM. If $n+1 \in A(G)$ then $H(G)$ consists of the union of congruence classes modulo n, and contains at least all integers congruent to 0 or 1 modulo n.

Proof: By (4) (with $n+1$ in place of n) the hypothesis of the lemma is satisfied. Obviously 0 and 1 are in $H(G)$ for any group G.

A sequence of examples G_n with $n+1 \in A(G_n)$ which exhibits some non-trivial possibilities for the set $H(G)$ may be defined as follows. The elements of G_n are triples (x, y, z) of integers modulo n (so G_n has order n^3) and multiplication is defined by $(x, y, z)(x', y', z') = (x+x', y+y', z+z' + 2xy')$. The group is non-abelian for $n > 2$. An easy induction shows that $(x, y, z)^k = (kx, ky, kz + k(k-1)xy)$. Thus P_{n+1} is the identity map and $n+1 \in A(G_n)$. Direct calculation shows that $k \in H(G_n)$ if and only if $k(k-1)$ is divisible by n, which is consistent with the conclusion of the theorem.

Princeton University

https://doi.org/10.4153/CMB-1965-063-4 Published online by Cambridge University Press