PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 119, Number 4, December 1993

ENDOMORPHISM NEAR-RINGS OF p-GROUPS GENERATED BY THE AUTOMORPHISM AND INNER AUTOMORPHISM GROUPS

GARY L. PETERSON

(Communicated by Maurice Auslander)

ABSTRACT. The purpose of this paper is to investigate the equality of the endomorphism near-rings generated by the automorphism group and inner automorphism group of a nonabelian p-group G. If the automorphism group of G is not a p-group, we find that these near-rings are different. If the automorphism group of G is a p-group, examples are given illustrating that these near-rings can be different and can be the same.

Suppose that G is an additive (but not necessarily abelian) group and S is a semigroup of endomorphisms of G. Under pointwise addition and composition of functions, the set R of all functions from G to G of the form $\varepsilon_1 s_1 + \cdots + \varepsilon_n s_n$, where $\varepsilon_i = \pm 1$ and $s_i \in S$, along with the zero map forms a distributively generated left near-ring when functions are written on the right-hand side. If S is the automorphism group of G, $\mathrm{Aut}(G)$, it is customary to denote this endomorphism near-ring by $A(G)$; if S is the inner automorphism group of G, $\mathrm{Inn}(G)$, this endomorphism near-ring is often denoted by $I(G)$. Of course, if $\mathrm{Aut}(G) = \mathrm{Inn}(G)$, the near-rings $A(G)$ and $I(G)$ coincide, but there are many cases where $\mathrm{Aut}(G) \neq \mathrm{Inn}(G)$ and $A(G) = I(G)$. Instances of this occur, for example, because $A(G) = I(G)$ when G is a finite nonabelian simple group (see [1]). Other examples where $A(G)$ and $I(G)$ are the same as well as examples of where they are different can be found in Chapter 11 of [6]. In this paper, we shall investigate the equality of $A(G)$ and $I(G)$ when G is a finite p-group (p a prime). Related to our study, the reader should note that we always have $\mathrm{Aut}(G) \neq \mathrm{Inn}(G)$ when G is a p-group of order more than p, because G has an outer automorphism of order p by a theorem of Gaschütz [3, III, 19.1].

Suppose now that G is a finite p-group. If G is abelian, it is a simple matter to check that $A(G) = I(G)$ if and only if G is cyclic. Consequently, we will restrict our attention to the case when G is nonabelian. Let us first consider the case when $\mathrm{Aut}(G)$ is not a p-group. In this case we obtain $A(G) \neq I(G)$. In fact, we can prove an even more general result:

Received by the editors March 30, 1992; presented at the 99th Annual Meeting of the American Mathematical Society, January 14, 1993.

1991 *Mathematics Subject Classification*. Primary 16A76; Secondary 20D45, 20E36, 20F28.

Key words and phrases. Endomorphism near-ring, automorphism group, inner automorphism group.

Theorem. *Suppose that G is a nonabelian p-group, A is a group of automorphisms of G containing* $\mathrm{Inn}(G)$, *and R is the endomorphism near-ring of G generated by A. If A is not a p-group, then $R \neq I(G)$.*

Proof. Suppose we did have $R = I(G)$. On the one hand, Corollary 3.3 of [4] tells us that $I(G)$ is a local near-ring. Note that we might as well assume that $A = \mathrm{Aut}(G) \cap R$, since $A \subseteq \mathrm{Aut}(G) \cap R$ and $\mathrm{Aut}(G) \cap R$ additively generates R. Thus by Theorem 2.3 of [4] we conclude that A has a normal p-Sylow subgroup P and that P has a cyclic complement K in A. Let $|K| = k$.

On the other hand, let us apply the theorem of [7]. Suppose that L/H is an R-principal factor of G (that is, $H \subseteq L$ are R-ideals of G such that L/H is a minimal R-module) of order p^n. This theorem tells us that R is not local for an automorphism group of our form when k does not divide $p^i + p^j - 1$ for each $0 \leq i,\ j \leq n-1$. Of course, if $R = I(G)$, then L/H is a minimal normal subgroup of G/H and so has order p. Hence any such $p^i + p^j - 1$ is 1, which is certainly not divisible by k. Thus R is not local, a contradiction.

Now let us consider the case when $\mathrm{Aut}(G)$ is a p-group. In this case we can give examples showing that no general conclusion can be drawn. From [5] we see that the dihedral 2-groups furnish us with examples of p-groups where $\mathrm{Aut}(G)$ is a p-group and $A(G) \neq I(G)$. To obtain examples where we do have $A(G) = I(G)$, we shall consider the semidihedral groups. These are groups of order 2^m with $m > 3$ of the form

$$G = \langle a, b \mid 2^{m-1}a = 2b = 0,\ -b + a + b = (-1 + 2^{m-2})a \rangle.$$

We first shall obtain a description of $I(G)$ similar to the one obtained for the dihedral groups in [5]. Some of the work we are about to do may be omitted if we only wish to see that $A(G) = I(G)$ but will be included since this example may be of independent interest.

The inner automorphism of G induced by an element $g \in G$ will be denoted $[g]$, and $[0]$ will be denoted as 1. Also, we shall indicate a map from G to G by giving the respective images of general elements na and $na + b$ of G in a bracketed pair $[\ ,\ ]$. For example,

$$[ka] = [na,\ (n - 2k + k2^{m-2})a + b]$$

and

$$[ka + b] = [(-n + n2^{m-2})a,\ (-n + n2^{m-2} + 2k - k2^{m-2})a + b].$$

Let us set

$$\delta = -1 + [a] = [0,\ (2 - 2^{m-2})a] \quad \text{and} \quad \alpha = 1 + [b] = [n2^{m-2}a,\ 2na].$$

The reader can verify that

$$[ka] = -k\delta + 1 \quad \text{and} \quad [ka + b] = k\delta - 1 + \alpha,$$

so that we have $I(G) = \langle 1, \delta, \alpha \rangle$ as additive groups.

Note that $\alpha + \delta = \delta + \alpha$. Also we have $\langle \alpha \rangle \cap \langle \delta \rangle = 0$ for suppose $r\alpha = s\delta$, where r and s are integers with $0 \leq r,\ s < 2^{m-2}$. Applying these maps to $2^{m-2}a + b$, we see that $0 = s(2 - 2^{m-2})a$. Thus, $s = 0$ and hence $\langle \alpha, \delta \rangle = \langle \alpha \rangle \oplus \langle \delta \rangle$. Next, $-1 + \alpha + 1 = -\alpha$ and $-1 + \delta + 1 = -\delta$, so $\langle \alpha, \delta \rangle$ is normal in $I(G)$. Finally, let us verify that $\langle 1 \rangle \cap \langle \alpha, \delta \rangle = 0$. Suppose that $t = r\alpha + s\delta$, where t, r, and s are integers with $0 \leq t < 2^{m-1}$ and $0 \leq r, s < 2^{m-2}$. Applying t and $r\alpha + s\delta$ to b, we obtain $tb = s(2 - 2^{m-2})a$, which implies $s = 0$ and $2 \mid t$. Applying t and $r\alpha$ to $2a + b$, which has order 2, we see that $0 = 4ra$, so that 2^{m-3} and hence 2 divides r. Now applying t and $r\alpha$ to a, we have $ta = 0$, which forces $t = 0$ and hence $r = 0$. Thus, $I(G)$ is the semidirect product of $\langle 1 \rangle$ and $\langle \alpha, \delta \rangle = \langle \alpha \rangle \oplus \langle \delta \rangle$. Further, $|I(G)| = 2^{3m-5}$.

Let us now turn our attention to $A(G)$. In order to describe the elements of $\mathrm{Aut}(G)$, first note that an element of the form $ja + b$ has order 2 if j is even and order 4 if j is odd. Thus $\langle a \rangle$ is a characteristic subgroup of G, and the image of a under an element of $\mathrm{Aut}(G)$ must have the form ia, where $(i, 2^{m-1}) = 1$. Also the image of b under an element of $\mathrm{Aut}(G)$ must have the form $ja + b$, where j is even. Conversely, it is a simple matter to check that a mapping sending a to ia and b to $ja + b$ for such i and j extends to an automorphism of G. Thus $\mathrm{Aut}(G)$ consists of the maps of the form $[ina, (j + in)a + b]$, where $(i, 2^{m-1}) = 1$ and j is even. Further, $|\mathrm{Aut}(G)| = \varphi(2^{m-1}) \cdot 2^{m-2} = 2^{2m-4}$.

Consider the automorphisms

$$\sigma = [-na, -na + b], \quad \beta = [5na, 5na + b], \quad \tau_j = [na, (j + n)a + b],$$

where j is even. Since σ and β restricted to $\langle a \rangle$ generate $\mathrm{Aut}(\langle a \rangle)$ [2, Lemma 5.4.1], it follows that the automorphisms σ, β, and τ_j $(0 < j/2 < 2^{m-2})$ generate $\mathrm{Aut}(G)$. Note that $\tau_j = [(j/2)(-1 + 2^{m-3})a] \in \mathrm{Inn}(G)$. Let us set

$$\psi = 1 + \sigma = [0, (2n - n2^{m-2})a].$$

We then obtain

$$\alpha = (1 - 2^{m-3})(2^{m-2} + \psi).$$

Solving this equation for ψ, we get ψ and hence σ in $I(G)$. Further we have

$$\beta = 5 - 2\psi$$

so that $\beta \in I(G)$. Thus $A(G) = I(G)$.

References

1. A. Fröhlich, *The near-ring generated by the inner automorphisms of a finite simple group*, J. London Math. Soc. **33** (1958), 95–107.
2. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
3. B. Huppert, *Endliche Gruppen*. I, Springer-Verlag, Berlin, 1967.
4. C. Lyons and G. Peterson, *Local endomorphism near-rings*, Proc. Edinburgh Math. Soc. **31** (1988), 409–414.
5. J. Malone and C. Lyons, *Finite dihedral groups and d.g. near-rings*. II, Compositio Math. **26** (1973), 249–259.
6. J. Meldrum, *Near-rings and their links with groups*, Pitman, London, 1985.
7. G. Peterson, *Automorphism groups emitting local endomorphism near-rings*, Proc. Amer. Math. Soc. **105** (1989), 840–843.

Department of Mathematics, James Madison University, Harrisonburg, Virginia 22807

E-mail address: `fac-gpeterso@jmuvax1.acs.jmu.edu`