Pacific Journal of Mathematics

# POWER-TYPE ENDOMORPHISMS OF SOME CLASS 2 GROUPS

FRANKLIN HAIMO

Vol. 5, No. 2 October 1955

# POWER-TYPE ENDOMORPHISMS OF SOME CLASS 2 GROUPS

FRANKLIN HAIMO

**1. Introduction.** Abelian groups possess endomorphisms of the form $x \longrightarrow x^n$ for each integer $n$. In general, however, non-abelian groups do not possess such power endomorphisms. In an earlier note, it was possible to show [1] for a nilpotent group $G$ with a uniform bound on the size of the classes of conjugates that there exists an integer $n \geq 2$ for which the mapping $x \longrightarrow x^n$ is an endomorphism of $G$ into its center. We shall consider endomorphisms of some groups of class 2 which induce power endomorphisms on the factor-commutator groups. In particular, we shall show, under suitable uniform torsion conditions for the group of inner automorphisms, that such power-type endomorphisms form a ring-like structure. Let $G$ be a group of class 2 for which $Q$, the commutator subgroup, has an exponent [2]. Then the relation [2] $(xy, u) = (x, u)(y, u)$ shows that $x \longrightarrow (x, u)$ is an endomorphism of $G$ into $Q$ for fixed $u \in G$. Let $n$ be any integer such that $n(n-1)/2$ is a multiple of the exponent of $Q$. Then the mapping $x \longrightarrow x^n(x, u)$ is a trivial example of a power-type endomorphism. If $G/Q$ has an exponent $m$, we shall show that the number of distinct endomorphisms of the form $x \longrightarrow x^j$, where $x^j$ is in the center $Z$ of $G$, divides $m$. In particular, a non-abelian group $G$ of class 2 has 1 or $p$ distinct central power endomorphisms if $G/Q$ is an elementary $p$-group (an abelian group with a prime $p$ as its exponent [2]).

**2. Power-type endomorphisms.** Let $G$ be a group with center $Z$ and commutator subgroup $Q$. We assume that $Q \subset Z$ so that [2] $G$ is a group of class 2. Further, suppose that there exists a least positive integer $N$ for which $x \in G$ implies $x^N \in Z$. This means that $G/Z$, a group isomorphic to the group of inner automorphisms of $G$, is a torsion abelian group with exponent $N$. An endomorphism $\alpha$ of $G$ will be called a *power-type* endomorphism if there exists an integer $n = n(\alpha)$ for which $\alpha(x) \equiv x^n \bmod Q$ for every $x \in G$. $\alpha$ induces the power endomorphism

$$\alpha^*(xQ) = x^n Q$$

Received August 20, 1953. This research was supported in part by the USAF under contract No. AF18(600)-568 monitored by the Office of Scientific Research, Air Research and Development Command.

*Pacific J. Math.* 5 (1955), 201-213

on $G/Q$; and conversely, any extension of a power endomorphism of $G/Q$ to an endomorphism of $G$ must be a power-type endomorphism of $G$. For $\alpha$, above, there exist elements

$$q(x) = q(x; \alpha) \in Q$$

such that $\alpha(x) = x^n q(x)$. It is easy to show that if $m$ and $n$ are two possible values for $n(\alpha)$ then $m \equiv n \bmod N$. We note that if $N$ is taken to be the exponent for $G/Q$ rather than for $G/Z$, then $n(\alpha)$ can be chosen least nonnegative, in fact, so that $0 \leq n(\alpha) < N$. We let $\mathfrak{P}$ denote the class of all power-type endomorphisms of a fixed group $G$ of class 2. Let $\iota(x) = x$ for every $x \in G$ be the identity map on $G$. We have $\iota \in \mathfrak{P}$ with $n(\iota) = 1$. If $e$ is the identity element of $G$, let $\nu(x) = e$ for every $x \in G$ be the trivial map of $G$. We have $\nu \in \mathfrak{P}$; in fact, any endomorphism of $G$ which carries $G$ into $Q$ lies in $\mathfrak{P}$. Let the set of all such endomorphisms into the commutator subgroup be denoted by $\mathfrak{N}$. We have $\nu \in \mathfrak{N}$. If $\alpha \in \mathfrak{N}$ then $n(\alpha) = 0$, and conversely (for $\alpha \in \mathfrak{P}$).

Suppose that $\alpha$ and $\beta$ are in $\mathfrak{P}$. Then

$$\alpha\beta(x) = \alpha[x^{n(\beta)} q(x; \beta)] = [\alpha(x)]^{n(\beta)} \alpha[q(x; \beta)]$$

$$= [x^{n(\alpha)} q(x; \alpha)]^{n(\beta)} \alpha[q(x; \beta)].$$

Since $Q \subset Z$, we have

$$\alpha\beta(x) = x^{n(\alpha)n(\beta)} [q(x; \alpha)]^{n(\beta)} \alpha[q(x; \beta)].$$

This shows that $\alpha\beta \in \mathfrak{P}$ so that $\mathfrak{P}$ is closed under endomorphism composition. In fact,

$$n(\alpha\beta) \equiv n(\alpha) n(\beta) \bmod N.$$

This multiplication is associative. Suppose that $\alpha \in \mathfrak{P}$ and that $\gamma \in \mathfrak{N}$. Then it is easy to see that $\alpha\gamma$ and $\gamma\alpha \in \mathfrak{N}$, since $Q$ is admissible under every endomorphism of $G$.

Let $\mathfrak{R}$ be the set of all elements of $\mathfrak{P}$ with the property that $\alpha \in \mathfrak{R}$ if and only if $N \mid n(\alpha)$. For endomorphisms $\alpha$ and $\beta$ of $G$, we define a mapping $\alpha + \beta$, (not necessarily an endomorphism), by

$$(\alpha + \beta)(x) = \alpha(x)\beta(x)$$

for every $x \in G$. Then we have the following.

THEOREM 1. *If* $\alpha \in \mathfrak{P}$, *then* $\alpha + \beta \in \mathfrak{P}$ *for every* $\beta \in \mathfrak{P}$ *if and only if* $\alpha \in \mathfrak{R}$. *If* $\alpha + \beta \in \mathfrak{P}$, *then*

$$n(\alpha) + n(\beta) \equiv n(\alpha + \beta) \bmod N,$$

*and*

$$q(x; \alpha + \beta) = q(x; \alpha) q(x; \beta).$$

*Proof.* Suppose that $\alpha + \beta \in \mathfrak{P}$ for every $\beta \in \mathfrak{P}$. Choosing $\beta = \iota$, we have

$$(\alpha + \iota)(xy) = [(\alpha + \iota)(x)]\,[(\alpha + \iota)(y)] = \alpha(x) x \alpha(y) y.$$

On the other hand,

$$(\alpha + \iota)(xy) = \alpha(xy) xy = \alpha(x)\, \alpha(y) xy,$$

so that $\alpha(y) x = x \alpha(y)$ for every $x, y \in G$. This places $\alpha(y) \in Z$; but

$$\alpha(y) = y^{n(\alpha)} q(y; \alpha)$$

where $q(y; \alpha) \in Q \subset Z$. Thus, $y^{n(\alpha)} \in Z$, for every $y \in G$, and $N \mid n(\alpha)$, placing $\alpha \in \mathfrak{R}$. Remaining details are immediate.

For elements of $\mathfrak{P}$, addition is commutative whenever one of the sums involved is in $\mathfrak{P}$, and if all the sums involved are in $\mathfrak{P}$, then addition is associative. A like statement can be made for the distributive law of multiplication over addition. $\mathfrak{R}$ is a ring with the two-sided ideal property in $\mathfrak{P}$ in that if $\alpha \in \mathfrak{P}$, $\beta \in \mathfrak{R}$, then $\alpha\beta$ and $\beta\alpha \in \mathfrak{R}$. $\mathfrak{N}$ likewise can be shown to be a ring which has the two-sided ideal property in $\mathfrak{P}$, therefore in $\mathfrak{R}$.

THEOREM 2. *Let* $G$ *be a non-abelian group of class* 2 *for which the group of inner automorphisms* $J$ *has the exponent* $N$. *If* $G/Q$ *is aperiodic, then* $\mathfrak{N}$ *is a prime ideal in* $\mathfrak{R}$.

*Proof.* Suppose that $\alpha, \beta \in \mathfrak{R}$ and that $\alpha\beta \in \mathfrak{N}$. If $G = Q$, then $Q \subset Z$ implies that $G$ is abelian. Hence we can find $x \in G$, $x \notin Q$ so that

$$\alpha\beta(x) = x^{n(\alpha)n(\beta)} q,$$

where both $q$ and $\alpha\beta(x) \in Q$. Since $G/Q$ is aperiodic, $n(\alpha) n(\beta) = 0$. We have really proved the prime ideal property of $\mathfrak{N}$ in $\mathfrak{P}$. The exponent on $J$, (isomorphic

to $G/Z$) is required only to guarantee the existence of $\mathfrak{R}$. A related result is the following.

THEOREM 3. *Let $G$ be a non-abelian group of class 2 for which $G/Q$ is a p-group with exponent $p^j$. Then $\mathfrak{N}$ is a primary ideal in $\mathfrak{R}$. In particular, if $G/Q$ is an elementary p-group* [2], *then $\mathfrak{N}$ is a prime ideal in $\mathfrak{R}$.*

*Proof.* The proof begins as for Theorem 2. Since $G/Q$ has exponent $p^j$, the latter is a divisor of $n(\alpha)n(\beta)$. If $\alpha \notin \mathfrak{N}$, at least the first power of $p$ would have to divide $n(\beta)$. For, $G/Z$ has an exponent $p^k$ where $1 \leq k \leq j$. Since $n(\beta^j) = [n(\beta)]^j$ we have $p^j \mid n(\beta^j)$ whence $\beta^j \in \mathfrak{N}$. The ring $\mathfrak{R}$ exists since $G/Z$ has an exponent. If $G/Q$ is elementary, then $j = k = 1$ so that $\mathfrak{N}$ is a prime ideal.

**3. Additive inverses.** An element $\alpha$ of $\mathfrak{P}$ is said to have an additive inverse $\alpha' \in \mathfrak{P}$ if $\alpha + \alpha' = \nu$. If such an additive inverse exists, it is unique, and

$$\alpha'(x) = x^{-n(\alpha)} q(x; \alpha)^{-1}.$$

A mapping with the structure of $\alpha'$ always exists, but it need not be, in general, an endomorphism, *ergo* not an additive inverse. If $\alpha'$ is an additive inverse of $\alpha$, then $\alpha$ is the additive inverse of $\alpha'$. We first prove the following.

LEMMA 1. *$\alpha$ has an additive inverse if and only if the $n(\alpha)$-powers of $G$ form a commutative set.*

*Proof.* Whether the mapping $\alpha'$ is an endomorphism or not, we have

$$\alpha'(x) = [\alpha(x)]^{-1},$$

so that

$$\alpha'(xy) = \alpha'(y)\,\alpha'(x)$$

for every $x, y \in G$. Since $Q \subset Z$, the conclusion follows at once.

Let $\mathfrak{K}$ be the set of all $\alpha \in \mathfrak{P}$ with the property that $\ker \alpha \supset Q$.

LEMMA 2.

(a) *$\mathfrak{K}$ has the ideal property in $\mathfrak{P}$.*

(b) $\mathfrak{K} \supset \mathfrak{R} (\supset \mathfrak{N})$.

(c) *$\alpha \in \mathfrak{P}$ has an additive inverse if and only if $\alpha \in \mathfrak{K}$.*

(d) $\alpha \in \mathfrak{R}$ *and* $\beta \in \mathfrak{K}$ *implies that* $\alpha + \beta \in \mathfrak{K}$.

*Proof.* (a) and (d) are trivial. For $\alpha \in \mathfrak{P}$, we have

$$\alpha(x^{-1}y^{-1}xy) = x^{-n}y^{-n}x^{n}y^{n}$$

where $n = n(\alpha)$. If, further, $\alpha \in \mathfrak{R}$, then $x^n \in Z$ so that $\alpha(x, y) = e$, and (b) is established, since $(x, y) = x^{-1}y^{-1}xy$ is typical of the generators of $Q$. We have $\alpha \in \mathfrak{K}$ if and only if $\alpha(x, y) = e$, that is, if and only if $x^n y^n = y^n x^n$. Lemma 1 now enables us to prove (c).

For fixed $\gamma \in \mathfrak{K}$, we have $\gamma\alpha \in \mathfrak{K}$ for every $\alpha \in \mathfrak{P}$. Write $-\gamma\alpha$ for the additive inverse of $\gamma\alpha$; then $-\gamma\alpha \in \mathfrak{K}$. Let $j_i$ be 0 or 1, and suppose that $\alpha_i \in \mathfrak{P}$, $i = 1, 2, \cdots, m$. A mapping

$$\sum_{i=1}^{m} (-1)^{j_i}\, \gamma\, \alpha_i = \sigma$$

is defined on $G$ into $G$ by

$$\sigma(x) = \prod_{i=1}^{m} x^{n(\gamma)(-1)^{j_i} n(\alpha_i)} [q(x; \gamma)]^{(-1)^{j_i} n(\alpha_i)}.$$

Call such a map a $\gamma - \Sigma$ *map*. It is clear that the sum of two $\gamma - \Sigma$ maps is a $\gamma - \Sigma$ map in the obvious way. The set of $\gamma - \Sigma$ maps is denoted by $(\gamma)$ and will be called the *right principal ideal* generated by $\gamma$ in $\mathfrak{P}$.

THEOREM 4. *If* $\gamma \in \mathfrak{K}$ *then* $(\gamma)$ *is a ring, and* $(\gamma) \subset \mathfrak{K}$.

*Proof.* As we saw above, $(\gamma)$ is closed under addition. $\gamma\nu = \nu$ so that $(\gamma)$ has the zero element $\nu$. If $\sigma$ is defined as above, then

$$\sum_{i=1}^{m} (-1)^{j_i+1}\, \gamma\, \alpha_i = -\sigma \in (\gamma).$$

By its effect on $x \in G$ we see that $\sigma \in \mathfrak{P}$. Since $-\sigma$ exists, $(\gamma) \subset \mathfrak{K}$ by Lemma 2(c). Now $(\gamma\alpha)(\gamma\beta) = \gamma(\alpha\gamma\beta)$, so that $(\gamma)$ is closed under multiplication, once we recall that the distributive law is valid whenever the sums involved are in $\mathfrak{P}$. A similar statement can be made for the associative laws, and we have proved that $(\gamma)$ is a ring included in $\mathfrak{K}$.

THEOREM 5. *Let $G$ be a non-abelian group of class 2, and let $\gamma$ be in $\mathfrak{K}$. If the ring $(\gamma)$ has a right multiplicative identity or a left multiplicative identity, then it has a (unique) two-sided multiplicative identity.*

*Proof.* $(\gamma)$ has a left (right) identity $\sigma \in (\gamma)$ if and only if $\sigma \in (\gamma)$ is a left (right) identity for the set of elements of $(\gamma)$ of the form $\gamma\beta$. More, specifically, $\sigma$ is a left identity if and only if $\sigma\gamma = \gamma$. A routine investigation shows that

$$\sigma\gamma(x) = x^{[n(\gamma)]^2 \sum_{i=1}^{m} (-1)^{j_i} n(\alpha_i) q^{n(\gamma)} \sum_{i=1}^{m} (-1)^{j_i} n(\alpha_i)}$$

where $q = q(x; \gamma)$. Let

$$u = n(\gamma) \sum_{i=1}^{m} (-1)^{j_i} n(\alpha_i) - 1.$$

Then $\sigma\gamma = \gamma$ if and only if

$$x^{n(\gamma)u} q^u = e$$

for every $x \in G$. Hence (1) $\gamma(x^u) = e$ for every $x \in G$, (2) $G/\ker\gamma$ has an exponent dividing $u$ and (3) $\gamma(G)$ has an exponent dividing $u$ are conditions each equivalent to (4) $\sigma$ is a left identity of $(\gamma)$. If (5) $\sigma$ is a right identity of $(\gamma)$, (6) $\gamma\sigma = \gamma$. But one can readily verify that (6) and (1) are equivalent, so that if $\sigma$ is a right identity, it is also a left identity, whence $(\gamma)$ would then have a unique two-sided identity.

If $\sigma$ is a left identity, then $\sigma\gamma = \gamma$ and

$$\gamma\beta\sigma(x) = [\gamma(x)]^{n(\beta)} = \gamma\beta(x)$$

for every $x \in G$. Thus $\sigma$ is also a right identity, and we have proved that every left identity is a right identity.

COROLLARY. *Let $G$ be a non-abelian group of class 2 for which $G/Q$ is an elementary p-group for an odd prime p. Let $\gamma \in \mathfrak{K}$ have the properties* (a) *that $p \nmid n(\gamma) = n$ and* (b) *that there exists an integer $m$ such that* ($b_1$) $mn = 1 \bmod p$ *and* ($b_2$) $m - 1$ *and* $n - 1$ *are relatively prime. Then $(\gamma)$ has an identity.*

*Proof.* $(m - 1, n - 1) = 1$ implies that $((m - 1)n, n - 1) = 1$ and that $(mn - 1, n - 1) = 1$ since $mn - 1 = (m - 1)n + (n - 1)$. Hence we can find an

integer $r$ such that

$$n(n-1)r \equiv m(m-1) \bmod (mn-1). \tag{7}$$

Form the mapping

$$\tau(x) = x^m [q(x;\gamma)]^r.$$

Since $G$ is a group of class 2, we have [2] the identity

$$(xy)^t = x^t y^t z^{v(t)},$$

where

$$z = (y,x) = y^{-1}x^{-1}yx \quad \text{and} \quad v(t) = t(t-1)/2.$$

Since $\gamma$ is an endomorphism, we have

$$q(xy;\gamma)z^{v(n)} = q(x;\gamma)q(y;\gamma).$$

Hence

$$\tau(xy) = x^m y^m z^{v(m)} [q(x;\gamma)]^r [q(y;\gamma)]^r z^{-rv(n)}.$$

Let us write the exponent of $z$ as $h/2$ where $h = m(m-1) - rn(n-1)$. By the choice of $r$ we have $h \equiv 0 \bmod (mn-1)$. But $mn - 1 \equiv 0 \bmod p$, so that $h \equiv 0 \bmod p$. Since $p$ is odd we obtain $h/2 \equiv 0 \bmod p$.

Since $G/Q$ has the exponent $p$, $Q \subset Z$ implies that $G/Z$ has an exponent $t$ where $t \mid p$. Since $G$ is non-abelian we have $t = p$. In [1], we proved that if $G/Z$ has the exponent $p$ then the mutual commutator group $(G, Z_2)$ has an exponent $t'$ which divides $p$. Here $Z_2$ is the second member of the ascending central series of $G$. Since $G$ is of class 2 we have $Z_2 = G$, and $(G, Z_2) = Q$. If $t' = 1$, then $G$ is abelian, a contradiction with hypothesis. Hence $t' = p$ and $z^{h/2} = e$, since $z \in Q$ and $p \mid (h/2)$. As a result, $\tau(xy)$ reduces to $\tau(x)\tau(y)$, so that $\tau$ is a power-type endomorphism with $n(\tau) = m$ and

$$q(x;\tau) = [q(x;\gamma)]^r.$$

Then

$$u = n(\gamma)n(\tau) - 1 = mn - 1.$$

Since $p$ is the exponent of $G/Q$ we have $x^u \in Q$ for every $x \in G$. But $\gamma \in \mathfrak{K}$ so that $\gamma(x^u) = e$. Using the theorem and (1) and (4) above, we see that $\gamma\tau$ is the required identity of $(\gamma)$.

**4. Some mappings into $Q$.** Let $\mathfrak{E}$ be the set of all $\alpha \in \mathfrak{P}$ which are extensions both of the identity map on $Q$ and of the identity map on $G/Q$. That is, $\alpha \in \mathfrak{E}$ if and only if $\alpha(x) = xq(x; \alpha)$ for every $x \in G$ and $\alpha(q) = q$ for every $q \in Q$. It can readily be verified that the elements of $\mathfrak{E}$ are automorphisms of $G$ and that, under automorphism composition, they form an abelian group with unity $\iota$. For $\alpha, \beta \in \mathfrak{E}$ and $x, y \in G$, it follows at once that

$$q(xy; \alpha) = q(x; \alpha)q(y; \alpha)$$

and that

$$q(x; \alpha\beta) = q(x; \alpha)q(x; \beta).$$

Let $\theta_x$ be a mapping defined on $\mathfrak{E}$ into $Q$ such that $\theta_x(\alpha) = q(x; \alpha)$ for every $\alpha \in \mathfrak{E}$. It is immediate that the $\theta_x$ are homomorphisms. We can define an addition in the set $\mathfrak{I}$ of mappings $\theta_x$ by

$$(\theta_x + \theta_y)(\alpha) = \theta_x(\alpha)\theta_y(\alpha)$$

for every $\alpha \in \mathfrak{E}$. Likewise define mappings $\phi_\alpha$ on $G$ into $Q$ by $\phi_\alpha(x) = q(x; \alpha)$. Here, too, in the set $\mathfrak{H}$ of mappings $\phi_\alpha$, mappings which are also homomorphisms, an addition is given by

$$(\phi_\alpha + \phi_\beta)(x) = \phi_\alpha(x)\phi_\beta(x)$$

for every $x \in G$. Let $F$ be the set of elements of $G$ which are the fixed points held in common by the elements of $\mathfrak{E}$. Then we obtain the following.

THEOREM 6.

(a) $\mathfrak{I} \cong G/F$.

(b) $\mathfrak{H} = \mathfrak{N}$ *and* $\mathfrak{N} \cong \mathfrak{E}$.

(c) $\mathfrak{N}$ *and* $\mathfrak{I}$ *are dual additive abelian groups in the sense that each can be represented faithfully as a set of homomorphisms on the other into* $Q$.

*Proof.* It is easy to verify that $\theta_x + \theta_y = \theta_{xy}$, and it follows that $\mathfrak{I}$ is an additive abelian group with unity $\theta_e$. Let $F_\alpha$ be the subgroup of all $x \in G$ with $\alpha(x) = x$. For $\alpha \in \mathfrak{E}$, each $F_\alpha$, and hence $F = \cap F_\alpha$, is a normal subgroup of $G$.

$\alpha \in \ker \theta_x$ if and only if $x \in F_\alpha$. $\theta_x = \theta_y$ if and only if $x \equiv y \bmod F$. The mapping $\theta$ on $G$ into $\mathfrak{I}$ given by $\theta(x) = \theta_x$ is a homomorphism onto $\mathfrak{I}$ with kernel $F$. We have established (a).

$\phi_\alpha$ is an endomorphism of $G$ into $Q$ with kern $\phi_\alpha = F_\alpha$. For $\gamma \in \mathfrak{N}$, let $\Gamma$ be a mapping of $G$ into $G$ given by $\Gamma(x) = x\gamma(x)$. Since $\mathfrak{N} \subset \mathfrak{R} \subset \mathfrak{K}$, we have $\Gamma(q) = q\gamma(q) = q$ for every $q \in Q$, so that $\Gamma \in \mathfrak{E}$. Also, $\phi_\Gamma = \gamma$. Hence $\mathfrak{N} \subset \mathfrak{H}$. Trivially, $\mathfrak{H} \subset \mathfrak{N}$. The unity of $\mathfrak{N}$ as a group is $\nu$ which can be represented as $\phi_\iota$. The mapping $\phi$ given by $\phi(\alpha) = \phi_\alpha$ on $\mathfrak{E}$ onto $\mathfrak{H} = \mathfrak{N}$ turns out to be an isomorphism, whence (b).

The mappings $c_x$ on $\mathfrak{N}$ into $Q$ given by

$$c_x(\gamma) = \theta_x \phi^{-1}(\gamma)$$

for every $\gamma \in \mathfrak{N}$ are homomorphisms. $\gamma \in \ker c_x$ if and only if $x \in \ker \gamma$. We can introduce an addition into the set $\mathfrak{C}$ of mappings $c_x$ by

$$(c_x + c_y)(\gamma) = c_x(\gamma)\, c_y(\gamma)$$

for every $\gamma \in \mathfrak{N}$. There is a homomorphism $\psi$ of $G$ onto $\mathfrak{C}$ with kernel equal to

$$U = \bigcap \ker \gamma,$$

where the cross-cut is taken over all $\gamma \in \mathfrak{N}$; and $\psi(x) = c_x$. A trivial argument shows that $U = F$. One can verify that the correspondence $\theta_x \leftrightarrow c_x$ is one-to-one and is an isomorphism of $\mathfrak{I}$ with $\mathfrak{C}$. Hence $\mathfrak{I}$ is represented faithfully as a set of homomorphisms on $\mathfrak{N}$ into $Q$.

Just as there are homomorphisms $c_x$ on $\mathfrak{N}$ into $Q$, so there are homomorphisms $b_\alpha$ on $\mathfrak{I}$ into $Q$ for each $\alpha \in \mathfrak{E}$, given by $b_\alpha(\theta_x) = \phi_\alpha(x)$. Here, kern $b_\alpha$ consists of all $\theta_x$ with $x \in F_\alpha$. The mapping $b_\alpha$ is single-valued; for $\theta_x = \theta_y$ if and only if there exists $r \in F$ with $y = xr$, and $\phi_\alpha(xr) = \phi_\alpha(x)$. We can introduce an addition into the set $\mathfrak{B}$ of such $b_\alpha$ by

$$(b_\alpha + b_\beta)(\theta_x) = \phi_\alpha(x)\, \phi_\beta(x).$$

Now $b_\alpha + b_\beta = b_{\alpha\beta}$, and, under this addition, $\mathfrak{B}$ becomes an abelian group with unity $b_\iota$. The correspondence $b_\alpha \leftrightarrow \phi_\alpha$ is one-to-one and is an isomorphism of $\mathfrak{B}$ with $\mathfrak{N}$, so that $\mathfrak{N}$ is represented faithfully as a set of homomorphisms on $\mathfrak{I}$ into $Q$, and (c) is established.

Further, there is an isomorphism $\omega$ on $\mathfrak{E}$ onto $\mathfrak{B}$ given by $\omega(\alpha) = b_\alpha$. The mapping

$$\theta_x \omega^{-1} = \delta_x$$

is a homomorphism on $\mathfrak{B}$ into $Q$ with kernel consisting of all $b_\alpha$ with $x \in F_\alpha$. For every $\alpha \in \mathfrak{E}$, let $\zeta_\alpha$ be a mapping defined on $\mathfrak{C}$ into $Q$ by

$$\zeta_\alpha(c_x) = \phi_\alpha(x).$$

It is clear that $\zeta_\alpha$ is a homomorphism with kernel consisting of all $c_x$ where $x \in \text{kern } \phi_\alpha$. We summarize these results as follows.

COROLLARY.

$$\theta_x = \delta_x \omega = c_x \phi$$

*on* $\mathfrak{E}$ *into* $Q$, *and dually,*

$$\phi_\alpha = \zeta_\alpha \psi = b_\alpha \theta$$

*on* $G$ *into* $Q$.

**5. Some enumerations of mappings.**

THEOREM 7. *The elements of* $\mathfrak{P}$ *are in one-to-one correspondence with the ordered pairs* $(n, \lambda)$, *where* $n$ *is an integer,* $\lambda$ *is a mapping of* $G$ *into* $Q$ *and* $n$ *and* $\lambda$ *satisfy*

$$\text{(A)} \qquad \lambda(x)\lambda(y) = \lambda(xy)\, z^{v(n)}$$

*for every* $x, y \in G$, *where* $z = (y, x)$ *and* $v(n) = n(n-1)/2$.

*Proof.* If $\alpha \in \mathfrak{P}$, then $q(x; \alpha) = \lambda(x)$ and $n(\alpha) = n$. Conversely, if $\lambda$ and $n$ are given, and if (A) holds, define $\alpha$ on $G$ into $G$ by $\alpha(x) = x^n \lambda(x)$ for every $x \in G$. Condition (A) and the fact that

$$(xy)^n = x^n y^n z^{v(n)}$$

show that $\alpha$ is an endomorphism and is therefore in $\mathfrak{P}$.

COROLLARY. *If* $Q$ *has the exponent* $m$, *and if* $n$ *is an integer for which* $m \mid v(n)$, *then* $x \longrightarrow x^n$ *is a power endomorphism of* $G$.

*Proof.* If we let $\lambda(x) = e$ for every $x \in G$ then the pair $(n, \lambda)$ satisfies (A) since, here, $z^{v(n)} = e$.

THEOREM 8. *For* $\alpha, \beta \in \mathfrak{P}$, *a necessary and sufficient condition that* $n(\alpha) = n(\beta)$ *is that there exists a* $\gamma = \gamma_{\alpha,\beta} \in \mathfrak{N}$ *such that* $\alpha = \beta + \gamma$.

*Proof.* Suppose that $n(\alpha) = n(\beta)$. Define a mapping $\gamma$ by

$$\gamma(x) = q(x; \alpha)[q(x; \beta)]^{-1}.$$

We have

$$(\beta + \gamma)(x) = \beta(x)\gamma(x) = x^{n(\beta)}q(x; \beta)q(x; \alpha)[q(x; \beta)]^{-1}$$

$$= x^{n(\alpha)}q(x; \alpha) = \alpha(x),$$

so that $\beta + \gamma = \alpha$. Now

$$\gamma(xy) = q(xy; \alpha)[q(xy; \beta)]^{-1};$$

hence if we apply (A) to each of the $q$'s and simplify, it turns out that $\gamma(xy) = \gamma(x)\gamma(y)$, so that $\gamma$ is an endomorphism lying in $\mathfrak{N}$.

COROLLARY. *Let* $M$ *be the cardinal of* $\mathfrak{N}$. *Then* $\mathfrak{P}$ *decomposes into partition classes, each of cardinal* $M$, *in such a way that* $\alpha$ *and* $\beta$ *are in the same partition class if and only if* $n(\alpha) = n(\beta)$.

Examples of such partition classes are $\mathfrak{N}$ (where $n = 0$) and $\mathfrak{E}$ (where $n = 1$). Nontrivial $\mathfrak{E}$ and $\mathfrak{E} \cong \mathfrak{N}$ along with an exponent on $Q$ imply, by the Corollary of Theorem 7, the existence of an infinite number of partition classes.

Let $I_N$ denote the group of integers, modulo $N$.

THEOREM 9. *Let* $G$ *be a group of class* 2 *with exponent* $N$ *on* $G/Z$. *Then there exists a nontrivial mapping* $\tau$ *on* $\mathfrak{P}$ *into* $I_N$ *which preserves addition and multiplication (whenever they are defined on* $\mathfrak{P}$). $\mathfrak{N} \subset \ker \tau$.

*Proof.* Let $j_N$ denote the residue class, modulo $N$, to which the integer $j$ belongs. Let $\tau(\alpha) = (n(\alpha))_N$. Then $\tau(\iota) = 1_N$, so that $\tau$ is nontrivial. The remaining statements are apparent. Note, however, that if $N$ is the exponent of $G/Q$, then $\ker \tau = \mathfrak{N}$.

It should be noted that a well known lemma of Grün leads to nontrivial $\mathfrak{N}$ and hence to nontrivial elements of $\mathfrak{P}$. For, by this lemma, the mappings of the type $x \longrightarrow (x, u)$ for each fixed $u \in G$, $u \notin Z$ are in $\mathfrak{N}$ for groups of class 2.

Let $G/Q$ have exponent $n$, so that $G/Z$ has exponent $t \mid n$. By [1, Lemma,

p. 370], the mutual commutator group $(G, G) = Q$ has an exponent $k \mid t$. If $t$ is odd, then $k \mid v(t)$, and $(xy)^t = x^t y^t$, whence $x \longrightarrow x^t$ is a central endomorphism of $G$. If $t$ is even, then $x \longrightarrow x^{2t}$ is a central endomorphism. Since $x^n \in Q$, and since $k$ is the exponent of $Q$, we have $x^{kn} = e$ for every $x \in G$. Now $t$ is the exponent of $G/Z$, so that $t$ must generate the ideal of exponents of central power endomorphisms of $G$ in case $t$ is odd. The central power endomorphisms are then all

$$x \longrightarrow x^{jt} \qquad (j = 0, 1, 2, \cdots (kn/t) - 1).$$

If $kn$ is not the exponent of $G$ but only an integral multiple thereof, then the number of distinct central power endomorphisms will be reduced (in proportion) to a submultiple of $kn/t$.

If $t$ is even, then the generator $t'$ of the ideal of exponents of central power endomorphisms of $G$ must have the property $t \mid t' \mid 2t$. Hence $t' = t$ or $t' = 2t$. If $t' = t$ then the $kn/t$ mappings $x \longrightarrow x^{jt}$ include all the central power endomorphisms (with possible repetitions). In fact, if $k$ is odd, then $k \mid t/2$, and $t' = t$. If $t = t'$, then $k \mid v(t)$. It follows readily that $k \equiv 0 \mod 2^r$ implies $t \equiv 0 \mod 2^{r+1}$. Thus $k \equiv 0 \mod 2^r$ and $t \not\equiv 0 \mod 2^{r+1}$ imply $t' = 2t$. Whenever $t' = 2t$, there are, at most, $kn/2t$ central power endomorphisms of $G$. Since, in any event, a submultiple of $kn/t$ or of $kn/2t$ is a submultiple of $n$, we have proved the following.

THEOREM 10. *Let $G$ be a group of class 2 for which $G/Q$ has exponent $n$. Then the number of central power endomorphisms of $G$ divides $n$.*

The above is a generalization of the following: Let $G$ be an abelian group with exponent $n$. Then there are precisely $n$ power endomorphisms of $G$; for, $x^{n+m} = x^m$.

COROLLARY. *Let $G$ be a non-abelian group of class 2 for which $G/Q$ is an elementary* p-group [2] *for an odd prime* p. *Let $G$ have at least one nontrivial element of order $\neq$ p. Then $G$ has precisely* p *central power endomorphisms. If* p = 2, *then $G$ has only the trivial central power endomorphism.*

*Proof.* Since $G$ is non-abelian we have $k \neq 1$, and $k \mid n = p$ implies $k = p$, so that $k \mid t \mid n$ leads to $t = p$. Likewise, $kn = p^2$. The exponent of $G$ is not p, since there exists $y \in G$ with $y^p \neq e$. Hence the exponent of $G$ must be $p^2$. If p is odd, then there are precisely $kn/t = p$ central power endomorphisms. The set of these endomorphisms is generated by the endomorphism $x \longrightarrow x^p$ under

endomorphism composition. If $p = 2$ then $x \longrightarrow x^2$ is not an endomorphism; for, if it were, $(xy)^2 = x^2y^2$ would imply $yx = xy$, whence $G$ would be abelian. Since $x^4 = e$, $G$ has only the one trivial central power endomorphism, $x \longrightarrow x^4 = e$.

In a non-abelian group of class 2, as in the Corollary above, we can find an element of $\mathfrak{K}$ for which the corresponding right principal ideal does not have a unity. Let $\eta(x) = x^p$ so that $n(\eta) = p$. Since $k = p$ we have $\eta \in \mathfrak{K}$. If $(\eta)$ had an identity, then there would exist mappings $\alpha_i \in \mathfrak{P}$, $i = 1, 2, \cdots, m$, with

$$p \Sigma n(\alpha_i) \equiv 1 \bmod p^2,$$

by the proof of Theorem 5, item (3), and the fact that $p^2$ is the exponent of $G \supset \eta(G)$. But the congruence $p\xi \equiv 1 \bmod p^2$ has no solution $\xi$.

## REFERENCES

1. F. Haimo, *Groups with a certain condition on conjugates*, Canadian J. Math., **4** (1952), 369-372.

2. H. Zassenhaus, *Gruppentheorie*, Leipzig and Berlin, 1937.

WASHINGTON UNIVERSITY
SAINT LOUIS, MISSOURI

# PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

H. L. ROYDEN
Stanford University
Stanford, California

R. P. DILWORTH
California Institute of Technology
Pasadena 4, California

E. HEWITT
University of Washington
Seattle 5, Washington

A. HORN*
University of California
Los Angeles 24, California

## ASSOCIATE EDITORS

| | | | |
|---|---|---|---|
| H. BUSEMANN | P. R. HALMOS | R. D. JAMES | GEORGE PÓLYA |
| HERBERT FEDERER | HEINZ HOPF | BORGE JESSEN | J. J. STOKER |
| MARSHALL HALL | ALFRED HORN | PAUL LÉVY | KOSAKU YOSIDA |

## SPONSORS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA, BERKELEY
UNIVERSITY OF CALIFORNIA, DAVIS
UNIVERSITY OF CALIFORNIA, LOS ANGELES
UNIVERSITY OF CALIFORNIA, SANTA BARBARA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD RESEARCH INSTITUTE
STANFORD UNIVERSITY
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
HUGHES AIRCRAFT COMPANY
SHELL DEVELOPMENT COMPANY


---

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. Manuscripts intended for the outgoing editors should be sent to their successors. All other communications to the editors should be addressed to the managing editor, Alfred Horn at the University of California, Los Angeles 24, California.

50 reprints of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

---


The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, c/o University of California Press, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 10, 1-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

* During the absence of E. G. Straus.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

**Pacific Journal of Mathematics**
Vol. 5, No. 2 October, 1955