ON COMMUTATIVE PRIME POWER SUBGROUPS OF THE NORM[1]

BY
LAWRENCE THOMAS WOS

The norm $N(G)$ of a group G is the set of elements $x \in G$ such that $x + T = T + x$ for every subgroup T of G. (G will be written additively in spite of the fact that G need not be commutative.) The norm is, therefore, the intersection of the normalizers of all the subgroups of G and is a characteristic, hence normal, subgroup of G. The main results of the paper are that the norm $N(G)$ is contained in the third center of G, and that the group of automorphisms induced on $N(G)$ by G is nilpotent of class 2. With certain reservations concerning the prime 2, we prove furthermore that the norm is contained in the second center if and only if the group of automorphisms induced on $N(G)$ by G is commutative.

R. Baer [4] proved the result that the norm of a group is 0 if and only if the center is 0. This theorem follows directly from our result that the norm is contained in the third center, for if the center is 0, then the third center is 0, and, a fortiori, the norm is 0; the necessity follows from the obvious fact that the norm contains the center.

The main results of the paper are obtained from a larger program, namely, the consideration of norm pairs P, S. A norm pair P, S is defined as a pair of groups P and S, where P is a commutative p-group and a normal subgroup of a group G and contained in the norm of G, and where S is the group of automorphisms induced on P by G. If a is an automorphism of the group P, let $F(a)$ denote the set of $x \in P$ such that $x = xa$, i.e., the elements left fixed by a; let $P(1 - a)$ denote the set of $x - xa = x(1 - a)$ for $x \in P$.

A pair of groups P, S is termed a norm-like pair if P is a commutative p-group and S is a group of automorphisms of P such that, for every $a \in S$, $P(1 - a)$ is cyclic and contained in $F(a)$. We prove that norm pairs are norm-like and that norm-like pairs, under certain conditions, are norm pairs. (If P, S is a norm-like pair, then composition in P will be denoted as addition whereas composition in S will be multiplication.)

If P, S is a norm-like pair, the elements $a \in S$ of S satisfy the equality, $k(1 - a) = 1 - a^k$ for all integers k. With the aid of this equality it will be shown that, if P, S is a norm-like pair, then S is a p-group and, in fact, the order of $a \in S$ equals the order of $P(1 - a)$. For such pairs P, S we prove S is of class 2 and $P = F_3$, where $F_0 = 0$ and $F_i =$ the set of $x \in P$ such that $x - xa \in F_{i-1}$ for every $a \in S$ with $i = 1, \cdots$; with $p \neq 2$, S is commutative if and only if $P = F_2$. These results demonstrate the strong connection between norm pairs and norm-like pairs, especially when one realizes that F_i

Received August 22, 1957.

[1] Work performed under the auspices of the U. S. Atomic Energy Commission.

plays the role of the intersection of P with the i^{th} member of the ascending central series.

Notations

$N(G)$ = the norm of the group G.
$Z(G)$ = the center of G.
$Z_i(G)$ = the i^{th} member of the ascending central series of G; in particular,
$Z_1(G)$ = $Z(G)$.
G_p = the p-component of G, i.e, the set of all elements of G whose order is a power of the prime p.
$o(x)$ = the order of the element x.
$o(G)$ = the order of the group G.
(a) = subgroup generated by a.

Section 1

Throughout the whole of the paper P will denote an additive commutative p-group, i.e., a group all of whose elements have order a power of some fixed prime p. If P is contained in some larger group G as a normal subgroup and a is an element of G, we shall identify a with the automorphism a induces on P and denote the automorphism by a. Consequently $P(1 - a)$ is, for $a \in G$, the commutator subgroup of the group generated by a and P; $F(a)$ is the centralizer of a in G. Since P is commutative, $P(1 - a)$ and $F(a)$ are clearly subgroups of P for every automorphism a of P.

Throughout this section assume that P is contained in the norm $N(G)$ of a group G and that P is a normal subgroup of G. Thus G induces an automorphism group S on P and P, S is, therefore, a norm pair.

LEMMA 1.1. *The centralizer of P in G contains all elements of infinite order or of order prime to p.*

Proof. Consider $w \in G$ such that $o(w) = 0$ or $o(w)$ is prime to p. $(w) \cap P = 0$ since P is a p-group. For $x \in P$

$$[w, x] = -w - x + w + x = (-w - x + w) + x \in P \text{ since } P \text{ is normal in } G,$$

$$= -w + (-x + w + x) \in (w) \text{ since } x \in P \leqq N(G).$$

So $[w, x] \in (w) \cap P = 0$, or $w + x = x + w$ for every $x \in P$, and the proof is complete.

LEMMA 1.2. *If a is an automorphism induced by an element of G on the p-group P, then $o(a)$ is a power of p, and there exists a p-element $a \in G$ inducing the automorphism a.*

Proof. If $a = 1$, there is nothing to prove. Consider $a \neq 1$. There exists a $w \in G$ such that w induces a on P. If $o(w) = 0$ or is prime to p, w commutes with P elementwise, which contradicts $a \neq 1$; therefore, $o(w) = p^k q$ with $0 < k$ and q prime to p. So there exist elements a and $\tilde{w}$ in G such that

$w = a + \tilde{w}$ and such that $o(a) = p^k$ and $o(\tilde{w}) = q$. $\tilde{w}$ commutes with P, so $a \in G$ induces the automorphism a on P. The order of the automorphism a is the smallest multiple of $a \in G$ contained in the centralizer C of P in G, which is the smallest multiple of a contained in $C \cap (a)$, which equals the index of $C \cap (a)$ in (a) since (a) is a cyclic group; but this index is a power of p since $a \in G$ is a p-element.

THEOREM 1.1. *Let P, S be a norm pair; then, $P(1 - a)$ is, for every $a \in S$, a cyclic group contained in $F(a)$ and isomorphic to $P/F(a)$; if P is not contained in the center $Z(G)$ of G, then P has bounded order, i.e., there exists a positive integer m such that $p^m P = 0$.*

Proof. Let a be an element of S. The mapping of $x \in P$ to $x(1 - a) = x - xa$ is an endomorphism of P with kernel $F(a)$ and image $P(1 - a)$. By the first isomorphism theorem, $P(1 - a)$ is, therefore, isomorphic to $P/F(a)$. Let $a \in G$ induce the automorphism a. For every $x \in P$ we have $x - a - x \in (a)$ since P is part of the norm of G; therefore, $P(1 - a) \leqq (a)$ and thus is a cyclic group which is contained in $F(a)$ since a commutes with multiples of itself.

Now assume that P is not contained in $Z(G)$. Then there exists an $a \in S$ with $a \neq 1$. Let $a \in G$ be a p-element inducing a on P; such an element exists by Lemma 1.2. By the above argument, $P(1 - a)$ is contained in (a) and is cyclic. Since P is a p-group, $P(1 - a)$ has order p^i for some positive integer i and, therefore, equals $p^{k-i}a$ where the order of $a \in G$ is p^k. Consider $x \in F(a)$. Since P is commutative, $a + x$ induces a on P. $P(1 - a) \leqq (a + x)$, so there exists an integer j such that $p^{k-i}a = j(a + x) = ja + jx$. Now we distinguish two cases.

Case 1. $(x) \cap (a) = 0$.

Therefore, $jx = p^{k-i}a - ja = 0$, or $ja = p^{k-i}a$. $ja = p^{k-i}a \neq 0$. Hence $j = p^{k-i}j'$, where $j' \equiv 1 \bmod p^i$. Furthermore $jx = 0$; and this implies $p^{k-i}x = 0$, since $o(x)$ is a power of p. Hence $o(x)$ divides p^{k-i}.

Case 2. $(x) \cap (a) \neq 0$.

$(x) \cap (a)$ therefore contains all elements of order p in (a), which are in turn all elements of order p in (x). Let U be the subgroup of G generated by a and x; U is a finite commutative p-group since $x \in F(a)$ and x and a are p-elements. The maximum of $o(u)$ for $u \in U$ equals the maximum of $o(x)$ and $o(a)$ since x and a are p-elements for the same prime p. Assume by way of contradiction that the maximum order of the elements in U is $o(x)$. Since every element of maximum order in a finite commutative group generates a direct summand, (x) is a direct summand of U. Hence there exists a subgroup V such that $U = (x) + V$ with $(x) \cap V = 0$. If $V \cap (a) \neq 0$, V contains all elements of order p in (a); but these elements are in (x), which contradicts $V \cap (x) = 0$. So $V \cap (a) = 0$. Since U is generated by a and x, the direct summand V is cyclic, and there exists $v = ha + jx$ for integers j and h such that $V = (v)$. Then $P(1 - v) = P(1 - ha) \leqq V \cap (ha) \leqq V \cap (a) = 0$, so that v induces 1

on P. But a is a linear combination of v and x, both of which commute with P, and a does not induce the identity on P. Thus we have a contradiction, and our assumption that $o(x)$ was maximal in U is false. So $o(x) \leqq o(a)$, and this holds for all $x \in F(a)$ since x was chosen arbitrarily. As noted before, $P/F(a)$ is isomorphic to $P(1 - a)$. So $P/F(a)$ has order p^i, or $p^i y \in F(a)$ for every $y \in P$. But $p^k x = 0$ for every $x \in F(a)$ from the above; therefore $p^{k+i}P = 0$, and P has bounded order.

Section II

We now turn to more general considerations and therefore make the following definition.

DEFINITION. *We term the pair P, S of groups P and S a norm-like pair if S is an automorphism group of P such that, for every $a \in S$,*

1. *$P(1 - a)$ is cyclic, and,*
2. *$P(1 - a)$ is contained in $F(a)$.*

Throughout this section P, S will be a norm-like pair, but P is not assumed to be contained in some larger group. However, we assume that P is a p-group. We shall use the additive notation in P, but the multiplicative notation in S.

LEMMA 2.1. *For every pair of automorphisms a and b in S, $F(a)b = F(a)$.*

Proof. Let x be an arbitrary element of $F(a)$. Then

$$x(1 - b) = x - xb = x - xab = x(1 - ab).$$

From property 2 of S,

$$y = x(1 - b) = x(1 - ab) \in F(b) \cap F(ab);$$

so $y = yb = yab$. By applying b^{-1}, $y = ya$. Since $x \in F(a)$, $x - y = xb \in F(a)$. So $F(a)b \leqq F(a)$. By the same argument but with b replaced by b^{-1}, $F(a)b^{-1} \leqq F(a)$. Applying b to the last inequality, $F(a) \leqq F(a)b$, which completes the proof.

The following lemma proves a very useful and somewhat surprising equality obeyed by the elements of S.

LEMMA 2.2. *The following three properties of elements a and b in S are equivalent: $P(1 - a) \leqq F(b)$; $(1 - a)b = 1 - a$; $1 - ab = (1 - a) + (1 - b)$.*

Proof. The equivalence of the first two properties, and their equivalence with the third property, may be inferred from the identity:

$$1 - ab = 1 - b + b - ab = (1 - b) + (1 - a)b.$$

COROLLARY 2.1. *If $P(1 - a) \leqq F(b)$ and $P(1 - b) \leqq F(a)$, then $ab = ba$.*

Proof. The hypotheses imply by Lemma 2.2 that

$$1 - ab = (1 - a) + (1 - b) = 1 - ba;$$

and this in turn implies $ab = ba$.

COROLLARY 2.2. *If U is a subgroup of S such that $P(1 - a) \leqq F(b)$ for every pair of elements a, b in U, then mapping x in U on $1 - x$ (in the ring of endomorphisms of P) is a homomorphism.*

This is an immediate consequence of Lemma 2.2.

COROLLARY 2.2′. *If a is an element in S and k an integer, then* $1 - a^k = k(1 - a)$.

This is a special case of Corollary 2.2.

LEMMA 2.3. *For every $a \in S$, $o(a) = o(P(1 - a))$.*

Proof. From property 1 of S, there exists an $x \in P$ such that $x(1 - a)$ generates $P(1 - a)$. Let $o(P(1 - a)) = r$. If $y \in P$, then

$$ya^r = y - y + ya^r = y - y(1 - a^r) = y - ry(1 - a) \qquad \text{by Corollary 2.2′,}$$

$$= y \qquad \text{since } r = o(P(1 - a)).$$

On the other hand $xa^i = x - ix(1 - a)$, so that $x = xa^i$ if, and only if, $r \mid i$. Hence $o(a) = r = o(P(1 - a))$.

Since P is assumed to be a p-group for the prime p, S is therefore a p-group for that prime.

LEMMA 2.4. *If, for a and b in S, C is the subgroup of S generated by a and b, and if $P(1 - C)$ is the subgroup of P generated by all the $P(1 - c)$ for $c \in C$, then $P(1 - C) = P(1 - a) + P(1 - b)$, and $o(c) \leqq \max [o(a), o(b)]$ for every $c \in C$.*

Proof. It is clear that $Q = P(1 - a) + P(1 - b) \leqq P(1 - C)$. Since $x(1 - a)b = x(1 - a) + xa(1 - b) - x(1 - b)$, it follows that $Qb \leqq Q$. Likewise we see that $Qa \leqq Q$. It is clear now that both a and b induce the identity automorphism in P/Q; and this implies that all of C induces the identity on P/Q and that therefore $P(1 - C) \leqq Q$. Hence $Q = P(1 - C)$. For the remainder of the lemma remember that, if a commutative p-group is the sum of 2 cyclic groups, the order of each of its cyclic subgroups cannot exceed the maximum of the orders of the 2 summands. From Lemma 2.3, the order of c in C equals the order of $P(1 - c)$. Since, for every $c \in C$, $P(1 - c)$ is cyclic by property 1 of S, we can apply the previous remark to yield $o(c) \leqq \max [o(a), o(b)]$.

DEFINITION. *If a and b are in S, we say a and b are disjoint elements, or just disjoint, when $P(1 - a) \cap P(1 - b) = 0$.*

COROLLARY 2.3. *If $C \leqq S$ is the group generated by a and b, and if a and b are disjoint elements or $o(a) \neq o(b)$, then $o(ab) = \max [o(a), o(b)]$.*

Proof. Assume by symmetry that $o(a) \leqq o(b)$. By Lemma 2.4, $o(ab) \leqq \max [o(a), o(b)]$.

Case 1. $o(a) < o(b)$.

Then $o(ab) \leqq o(b)$. Since C is also generated by a and ab, $o(b) \leqq \max [o(a), o(ab)]$. But $o(a) < o(b)$, so $o(b) \leqq o(ab)$. So $o(b) = o(ab) = \max [o(a), o(b)]$.

Case 2. a and b are disjoint.

If $o(a) < o(b)$, then $o(ab) = \max [o(a), o(b)]$ by Case 1. Assume therefore that $o(a) = o(b)$. Since a and b are disjoint, $P(1 - C) = P(1 - a) + P(1 - b)$ and hence, by Lemma 2.3, $o(P(1 - C)) = o(a) \cdot o(b) = o(a)^2$. Since C is likewise generated by a and ab, we have $P(1 - C) = P(1 - a) + P(1 - ab)$; and we deduce that $o(P(1 - C))$ is a divisor of $o(a) \cdot o(b)$ by Lemma 2.3. But it follows from Lemma 2.4 that $o(ab)$ is a divisor of $\max [o(a), o(b)] = o(a)$. Hence $o(a)^2 = o(P(1 - C))$ is both a divisor and a multiple of $o(a) \cdot o(ab)$. Consequently $o(ab) = o(a) = \max [o(a), o(b)]$.

Section III

We still continue the study of norm-like pairs P, S, obtaining various necessary and sufficient conditions for elements of S to commute.

LEMMA 3.1. *If, for $a \in S$ and $b \in S$, any of the following four conditions holds, then $ab = ba$:*

1. *$P(1 - a) \leqq F(b)$ and $P(1 - b) \leqq F(a)$;*
2. *$P(1 - a) \leqq P(1 - b)$;*
3. *$0 = P(1 - a) \cap P(1 - b)$;*
4. *there exists $a\ c \in S$ such that $o(a) \leqq o(c)$ and c and b are disjoint elements.*

Proof. Assume condition 1. Then $(1 - a)(1 - b) = 0 = (1 - b)(1 - a)$, so $1 - a - b + ab = 1 - b - a + ba = 1 - a - b + ba$; cancelling from both sides, $ab = ba$. Assume 2. If the inequality is actually equality, then property 2 of S reduces condition 2 to condition 1. So assume the inequality is strict. By Lemma 2.3, $o(a) < o(b)$; by Corollary 2.1, $o(ab) = o(b)$. Applying Lemma 2.4, $P(1 - b) = P(1 - ab)$. As in the argument above, b commutes with ab, so $ab = ba$. Assume 3. Assume by symmetry that $o(a) \leqq o(b)$. Let C be the subgroup of S generated by a and b. Then

$$o(P(1 - C)) = o(a) \cdot o(b) = \frac{o(a) \cdot o(ba)}{o[P(1 - a) \cap P(1 - ba)]}.$$

By Corollary 2.1, $o(ba) \leqq o(b)$, so $0 = P(1 - a) \cap P(1 - ba)$. Consider $x \in P(1 - b)$. From property 2 of S,

$$x(1 - a) = x(1 - ba) \in P(1 - a) \cap P(1 - ba);$$

so $x(1-a)=0$, and $P(1-b)\leqq F(a)$. Adding this to the fact that $P(1-a)\leqq F(a)$ yields $P(1-C)\leqq F(a)$. So $P(1-ba)\leqq F(a)$, and therefore, $P(1-ba)\leqq F(a)\cap F(ba)\leqq F(b)$, by applying a^{-1}. Hence, $P(1-a)\leqq P(1-C)\leqq F(b)$, and we are again reduced to condition 1, thus proving condition 3 implies $ab=ba$. Assume 4. If a and b are disjoint, we can apply 3. Assume a and b are not disjoint. Since $P(1-d)$ is a cyclic p-group for every $d\in S$, and since c and b are assumed disjoint, c and a must be disjoint. Since it is assumed that $o(a)\leqq o(c)$, we reproduce the counting argument used above in 3 to yield a and ca are disjoint. Since b and a are not disjoint by assumption, b and ca are. By 3, $bc=cb$, and $bca=cab$. So $cab=bca=cba$, and $ab=ba$ again.

COROLLARY 3.1. *If, for $a\in S$, there exist $c\in S$ and $d\in S$ such that $o(a)\leqq o(c)\leqq o(d)$ and such that c and d are disjoint, then $a\in Z(S)$; if $P(1-S)\leqq F(S)$, where $P(1-S)$ is the group generated by all $P(1-a)$ for $a\in S$ and $F(S)=\bigcap_{a\in S}F(a)$, then S is commutative.*

Proof. Consider an arbitrary $b\in S$. If b and c are disjoint, we can apply condition 4 of Lemma 3.1 to yield $ab=ba$. If b and c are not disjoint, then b and d are, since c and d are disjoint, and we can apply condition 4 to the triple a, d, b and obtain $ab=ba$. Since b was chosen arbitrarily, a is contained in the center of S. For the second half of the corollary, consider an arbitrary pair of elements a and b in S. $P(1-a)\leqq P(1-S)\leqq F(S)\leqq F(b)$; similarly, $P(1-b)\leqq F(a)$. Applying condition 1 of Lemma 3.1 yields $ab=ba$. a and b were chosen arbitrarily, and the proof is complete.

LEMMA 3.2. *If, for a and b in S, $ab=ba$, then $P(1-a^2)\leqq F(b)$.*

Proof. Using property 2 of S,

$$1-ab=1-a+a-ab=(1-a+a-ab)ab=(1-a)b+a(1-b)a$$
$$=b-1+1-ab+a^2-a^2b=1-ab+a^2-1+(1-a^2)b;$$

the last equality follows from the fact that endomorphisms of a commutative group additively commute. Subtracting $1-ab$ from the first and last and transposing a^2-1, we have $1-a^2=(1-a^2)b$, and the result is established.

COROLLARY 3.2. *If P is a p-group with $p\neq 2$, then $a\in Z(S)$ if and only if, for every $b\in S$, $P(1-a)\leqq F(b)$ and $P(1-b)\leqq F(a)$.*

Proof. The sufficiency has been established by condition 1 of Lemma 3.1. For the necessity, let a be in the center of S. Consider an arbitrary $b\in S$. From the previous lemma, $P(1-a^2)\leqq F(b)$. From property 1 of S, there exists an $x\in P$ such that $x(1-a)$ generates $P(1-a)$. From Lemma 2.2, $x(1-a^2)=2x(1-a)\in F(b)$. But 2 and p are relatively prime, so $2x(1-a)$ generates $P(1-a)$, and $P(1-a)$ is, therefore, contained in $F(b)$. By the same argument, $P(1-b)\leqq F(a)$. Since b was chosen arbitrarily, we have the result.

For Theorem 3.1 and for future use, we define $F_0 = 0$, $F_1 = F(S) = \bigcap_{a \in S} F(a)$, $F_2 =$ all $x \in P$ such that $x \equiv xa \bmod F_1$ for every $a \in S$, and, inductively, $F_i =$ the set of $x \in P$ such that $x \equiv xa \bmod F_{i-1}$ for every $a \in S$ $(i = 1, 2, \cdots)$. F_2 is that subgroup of P whose elements generate cosets mod F_1 which are left fixed by every $a \in S$; there is no confusion in applying an element of S to P/F_1 since the modulus is S-invariant.

THEOREM 3.1. *If P, S is a norm-like pair but with $p \neq 2$, and if S is commutative, then $P = F_2$, and $(1 - S)^2$, the set of $(1 - a)(1 - b)$ for all a and b in S, is 0; conversely, if P, S is a norm-like pair and $P = F_2$, then S is commutative.*

Proof. Assume S is commutative and $p \neq 2$. Consider $a \in S$. By Corollary 3.2, $P(1 - a) \leqq F(b)$ for every $b \in S$. Therefore, for every $a \in S$, $P(1 - a) \leqq F(S) = F_1$. So, for every $x \in P$ and every $a \in S$, $x \equiv xa \bmod F_1$, which is equivalent to $P = F_2$. Since, for every $x \in P$ and every a and b in S, $x(1 - a) \in F(b)$, we have $x(1 - a)(1 - b) = 0$, or $(1 - a)(1 - b)$ is the 0-endomorphism of P for every a and b in S. Since $P = F_2$ implies $P(1 - S) \leqq F(S) = F_1$, the converse of the theorem is a direct consequence of Corollary 3.1.

Section IV

Throughout this Section let P, S be a norm-like pair but with the added assumption that the elements of P have bounded order p^m, i.e., there exists a positive integer m such that $p^m P = 0$. By Lemma 2.3, $S^{p^m} = 1$, so S contains elements of maximum order. In fact, every element of S has maximum order in S or can be written as a product of two such, for let $a \in S$ be of maximum order in S and consider $c \in S$. If $o(c)$ is maximal in S, there is nothing to prove. If $o(c) < o(a)$, then $o(ac) = o(a)$ by Corollary 2.1, and $c = a^{-1}ac$ is a product of two elements of maximum order.

Remark. If S contains elements a and b of maximum order such that a and b are disjoint, then for an arbitrary $c \in S$ application of Corollary 3.1 to the triple c, b, a yields $c \in Z(S)$. Hence, S equals its center and is consequently commutative.

LEMMA 4.1. *If S contains elements a and b of maximum order p^k such that a and b are disjoint, then $F(S) = F(m)$ for every $m \in S$ of maximum order in S, $P/F(S)$ is cyclic of order p^k, and $P = F_2$.*

Proof. Let a and b be elements of S which are disjoint and have maximum order p^k. By duplicating the argument at the end of the proof of Corollary 2.1, we see that ab and b are disjoint and a and ba are disjoint. If $x \in F(a)$, $x(1 - b) = x(1 - ab) = 0$ since b and ab are disjoint; so $F(a) \leqq F(b)$. Similarly, $F(b) \leqq F(a)$. So $F(b) = F(a)$. If $c \in S$ is of maximum order in S, then c and a, or c and b, are disjoint since all $P(1 - d)$ with $d \in S$ are cyclic p-groups. Applying the above argument to the proper pair, say c and a,

we have $F(c) = F(a)$. Therefore, all $F(m)$ are equal for $m \in S$ of maximum order in S. Since S is generated by its elements of maximum order [as noted at the beginning of this section], $F(S)$ is the intersection of all the $F(m)$ for $m \in S$ of maximum order. But all these $F(m)$ have been shown to be equal; and thus we have $F(S) = F(m)$ for every $m \in S$ of maximum order; and the first part of the lemma is established. As in Theorem 1.1, $P/F(m)$ is isomorphic to $P(1 - m)$ which is cyclic and has order $o(m)$. But $F(S) = F(m)$ for $m \in S$ of maximum order, and $o(m) = p^k$. So $P/F(S)$ is cyclic of order p^k. For every $m \in S$ of maximum order, $P(1 - m) \leqq F(m) = F(S)$. Since every element of S is of maximum order in S or is a product of 2 such elements, Lemma 2.4 yields $P(1 - S) \leqq F(S) = F_1$. This is precisely equivalent to $P = F_2$.

Remark. If $P/F(S)$ is cyclic, then there exists an $x \in P$ such that $x(1 - a)$ generates $P(1 - a)$ for every $a \in S$. For let $x \in P$ be a representative of a coset which generates $P/F(S)$. Consider $a \in S$. From property 1 of S, there exists a $y \in P$ such that $y(1 - a)$ generates $P(1 - a)$. $y = kx + z$ for some integer k and some $z \in F(S)$. $y(1 - a) = (kx + z)(1 - a) = kx(1 - a)$ since $F(S) \leqq F(a)$. So $x(1 - a)$ generates $P(1 - a)$.

THEOREM 4.1. *If P, S is a norm-like pair, S is nilpotent of class 2, i.e., $S = Z_2(S)$.*

Proof. If S contains elements a and b of maximum order which are disjoint, then S is commutative as has already been remarked. If S does not contain 2 such elements, let $D = \bigcap_{m \in S} P(1 - m)$ with m of maximum order in S; then we are going to show that $0 < D \leqq P$, and that there exist elements a and b of maximum order such that $P(1 - a) \cap P(1 - b) = D$. For let $m \in S$ be of maximum order in S. We can consider the various intersections $P(1 - m) \cap P(1 - k)$ for every $k \in S$ of maximum order. Since $P(1 - m)$ is a cyclic p-group, and since the lattice of subgroups of a cyclic p-group is simply ordered and contains a finite number of elements, there exists a $j \in S$ of maximum order such that $P(1 - m) \cap P(1 - j) = E \leqq P(1 - m) \cap P(1 - k)$ for every $k \in S$ of maximum order in S. Therefore, $E \leqq P(1 - k)$ for every $k \in S$ of maximum order, and hence $E \leqq D$. From the definition of D, $D \leqq P(1 - m) \cap P(1 - j) = E$. So $D = E$, and m and j are the elements whose existence we wish to establish. Let $T \leqq S$ be the set of all $a \in S$ such that $P(1 - a) \leqq D$; T is a normal subgroup of S. If $o(D) = p^i$, and if $a \in S$ is of maximum order p^k, applying Lemma 2.3 to S/T and P/D yields $o(aT) = p^{k-i}$. We claim aT has maximum order in S/T, for consider $cT \in S/T$. If $o(c)$ is maximal in S, then $o(cT) = p^{k-i} = o(aT)$. If not, then $o(ac) = o(a)$ from Corollary 2.1. Let $R \leqq S/T$ be the group generated by aT and acT. Applying Lemma 2.4 to R, we have $o(cT) \leqq \max[o(aT), o(acT)]$, hence $\leqq p^{k-i}$. So $o(cT) \leqq o(aT)$ for every $cT \in S/T$, and aT has maximum order in S/T. Since $P(1 - a) \cap P(1 - b) = D$,

$$(P/D)(1 - aT) \cap (P/D)(1 - bT) = D,$$

the 0 of P/D. Applying the first remark of this section to S/T, we see that S/T is commutative. For every $t \in T$ and every $m \in S$ of maximum order, $P(1 - t) \leqq D \leqq P(1 - m)$. From Lemma 3.1, $tm = mt$ for every $t \in T$ and every $m \in S$ of maximum order in S. Since S is generated by its elements of maximum order, $T \leqq Z(S)$. Therefore, $S = Z_2(S)$.

THEOREM 4.2. *If P, S is a norm-like pair, $P = F_3$.*

Proof. If S contains elements a and b of maximum order which are disjoint, then, by Lemma 4.1, $P = F_2 \leqq F_3$; so $P = F_3$. If S does not contain two such elements, we can define T and D as in the previous theorem. Since S/T is an automorphism group of P/D satisfying the hypothesis of Lemma 4.1, we conclude that P/D equals its F_2 with respect to S/T. Since $D \leqq F(S) = F_1$, this is equivalent to $P = F_3$.

THEOREM 4.3. *If P, S is a norm-like pair such that S contains elements a and b of maximum order which are disjoint and such that $p \neq 2$, then S and $P(1 - S)$ are isomorphic.*

Proof. By Lemma 4.1, $P/F(S)$ is cyclic; therefore, by the second remark of this section, there exists an $x \in P$ such that $x(1 - c)$ generates $P(1 - c)$ for every $c \in S$. The existence of the elements a and b implies that S is commutative; this coupled with the fact that $p \neq 2$ implies $P(1 - d) \leqq F(c)$ for every d and c in S, by Theorem 2.1. Therefore, for every c and d in S and every $y \in P$,

$$\begin{aligned} y(1 - cd) &= y(1 - c + c - cd) \\ &= y(1 - c) + y(1 - d)c = y(1 - c) + y(1 - d). \end{aligned}$$

If, for $a_i \in S$ and $y_i \in P$, $\sum_i y_i(1 - a_i)$ is an arbitrary element of $P(1 - S)$, then there exist integers k_i such that

$$\sum_i y_i(1 - a_i) = \sum_i k_i x(1 - a_i) = \sum_i x(1 - a_i^{k_i}) = x\left(1 - \prod_i a_i^{k_i}\right).$$

So every element of $P(1 - S)$ equals $x(1 - c)$ for some $c \in S$ and that special x whose existence was established earlier in the proof. If we map $c \in S$ to $x(1 - c) \in P$, we have a homomorphism from S onto $P(1 - S)$, and its kernel is exactly 1.

Section V

We now turn to consideration of the norm $N(G)$ of the group G. By Theorem 1.1, we see that, if P, S is a norm pair, then P, S is a norm-like pair. We can therefore apply all results established in Sections II, III, and IV to norm pairs P, S. For example, where S is a member of the norm pair P, S and $a \in S$, $o(a) = o(P(1 - a))$, and $F(a)$ is normal in G.

THEOREM 5.1. *The norm $N(G)$ of the group G is contained in the third center $Z_3(G)$ of G.*

Proof. It follows directly from the definition of the norm that all subgroups of $N(G)$ are normal in $N(G)$ which is, therefore, commutative or hamiltonian.

Case 1. $N(G)$ contains an element of infinite order.

In this case, the norm and center of G are the same (see Baer [1, 3]), and the theorem is trivially true.

Case 2. $N(G)$ is commutative and contains no elements of infinite order.

Then $N(G)$ equals the direct sum of N_p, where N_p is the p-component of $N(G)$, i.e., N_p is that subgroup of the norm consisting of all $x \in N(G)$ whose order is a power of the prime p. Consider the prime p. N_p is a characteristic subgroup of $N(G)$, and $N(G)$ is characteristic in G; so N_p is normal in G, and G induces a group of automorphisms S_p on N_p. N_p, S_p is a norm pair. $N_p \leqq Z(G)$, or, by Theorem 1.1, N_p has bounded order. In the latter case we can apply Theorem 4.2 to yield $N_p = F_3$. But F_i is precisely the intersection of P with the i^{th} member of the ascending central series of G, and therefore N_p is contained in $Z_3(G)$. Since p was chosen arbitrarily and $N(G)$ equals the direct sum of the N_p, $N(G) \leqq Z_3(G)$, which completes Case 2.

Case 3. $N(G)$ is hamiltonian.

By a well known theorem hamiltonian groups are the direct sum of three groups: a commutative group all of whose elements have odd order, a commutative group all of whose nonzero elements have order 2, and the quaternions; see Zassenhaus [1]. So again the norm of G is the direct sum of its p-components, but, different from Case 2, N_2 is not commutative. N_2 is, in fact, the direct sum of the quaternions and a commutative group all of whose nonzero elements have order 2. N_2 contains a unique nonzero element w such that $w = 2x$ for some $x \in N_2$. (w) is therefore a characteristic subgroup of N_2. Since N_2 is normal in G, (w) is normal in G. Adding this to the fact that $o(w) = 2$ shows that $w \in Z(G)$. Baer [2] proved that when the norm of a group is hamiltonian, the following four statements must hold: G contains no elements of infinite order; G contains no elements whose order is divisible by 8; all elements of G whose order is divisible by 4 are of the form $z + v$, where v commutes with every element in N_2 and $z \in N_2$ with $o(z) = 4$; all elements of G whose orders are not divisible by 4 commute with every element in N_2. Hence, if the commutator $[a, x] = -a - x + a + x$ for some $a \in G$ and some $x \in N_2$ is different from 0, $a = z + v$, where v commutes with N_2 and $z \in N_2$ with $o(z) = o(x) = 4$. To see this, recall the structure of N_2. Therefore, when $[a, x] \neq 0$ for $a \in G$ and $x \in N_2$, there exists a $z \in N_2$ such that $[a, x] = [z, x] = w$. Since we established earlier that $w \in Z(G)$, $N_2 \leqq Z_2(G)$. We can apply the argument of Case 2 to the complement of N_2 in $N(G)$ to show that the complement is contained in $Z_3(G)$. Since $N(G)$ equals the direct sum of N_2 and its complement, $N(G) \leqq Z_3(G)$, and the proof of the theorem is complete.

Since the norm $N(G)$ as the intersection of all normalizers of all subgroups of G is a normal subgroup of G, G induces a group of automorphisms on $N(G)$.

THEOREM 5.2. *The group of automorphisms induced by the group G on its norm is nilpotent of class* 2.

Proof. Let S denote the group of automorphisms induced by G on $N(G)$. If $N(G)$ contains an element of infinite order, then $N(G) = Z(G)$ (see Baer [1, 3]); then $S = 1$, and there is nothing to prove. Assume that every element in the norm of G has finite order.

Case 1. $N(G)$ is commutative.

Then $N(G)$ equals the direct sum of N_p. For the prime p, let S_p = all $a \in S$ such that $a = 1$ on N_q for every prime $q \neq p$. N_p is a characteristic subgroup of $N(G)$ for every prime p, and $N(G)$ is characteristic in G; so N_p is normal in G. By using Lemma 1.1, we have S_p is precisely the group of automorphisms induced by G on N_p. N_p, S_p is a norm pair and therefore, by Theorem 1.1, is a norm-like pair. If $N_p \leqq Z(G)$, $S_p = 1$. If N_p is not contained in the center of G, then N_p has bounded order by Theorem 1.1, and we can apply Theorem 4.2 to obtain S_p is nilpotent of class 2. Using Lemma 1.1, we see that S is the direct product of its p-components S_p, and therefore S itself must be nilpotent of class 2.

Case 2. $N(G)$ is hamiltonian.

Recall the structure of hamiltonian groups stated in Case 3 of Theorem 5.1 to see that $N(G)$ is again the direct sum of N_p. For $p \neq 2$, we can argue as in Case 1 to obtain S_p is nilpotent of class 2. Let C = the centralizer of N_2 in G. Since N_2 is a normal subgroup of G, C is normal also. Let Q be the quaternions. Using Baer's result on groups with hamiltonian norm cited in Case 3 of Theorem 5.1, we see that $G = Q + C$. $C \cap Q = 2Q$. S_2 is isomorphic to $G/C = (Q + C)/C$ is isomorphic to $Q/Q \cap C = Q/2Q$ = the 4-group. So S_2 is commutative. Since commutativity was not needed in the proof of Lemma 1.1, we can again apply Lemma 1.1 to obtain S equals the direct product of S_p. Since S_p is nilpotent of class 2 for $p \neq 2$, and since S_2 is commutative, S is of class 2.

We can connect and sharpen Theorems 5.1 and 5.2 with the following theorem.

THEOREM 5.3. *Where $N(G)$ is hamiltonian, $N(G) \leqq Z_2(G)$ if and only if the group of automorphisms S induced on $N(G)$ by G is commutative; where $N(G)$ is a commutative group containing no elements of infinite order and $2N_2 = 0$, $N(G) \leqq Z_2(G)$ if and only if S is commutative.*

Proof. Assume $N(G)$ is hamiltonian. By Theorem 3.1, $N_p \leqq Z_2(G)$ if and only if S_p is commutative for $p \neq 2$. For $p = 2$, S_p was shown to be commutative in Case 2 of Theorem 5.2, and $N_p \leqq Z_2(G)$ was shown in Case 3 of Theorem 5.1. Since S equals the direct product of S_p, and $N(G)$ equals the direct sum of N_p, the first part of the theorem is established. Now assume $N(G)$ is commutative and contains no elements of infinite order and that $2N_2 = 0$. S_2 thus contains elements of maximum order. If S_2 contains 2 such which are disjoint, then, by Lemma 4.1, $N_2 = F_2 = Z_2(G) \cap N_2$; this

in turn implies, by Theorem 3.1, that S_2 is commutative. If S_2 does not contain 2 elements of maximum order which are disjoint, then all $N_2(1 - a)$ are equal for $a \neq 1 \in S_2$, since $2N_2 = 0$. Then $N_2(1 - S_2) \leqq F(S_2) = Z(G) \cap P$. This implies, by Corollary 3.1, that S_2 is commutative. $N_2(1 - S_2) \leqq Z(G)$ is equivalent to $N_2 \leqq Z_2(G)$. Therefore, in either case, $N_2 \leqq Z_2(G)$, and S_2 is commutative. For $p \neq 2$, $N_p \leqq Z_2(G)$ if and only if S_p is commutative, by Theorem 3.1. So again S is commutative if and only if $N(G) \leqq Z_2(G)$.

By examining the proof just completed and by recalling that, by Baer [1, 3], if the norm contains an element of infinite order, then the norm equals the center, we see there is only one obstacle to the theorem: $N(G) \leqq Z_2(G)$ if and only if S is commutative. This obstacle is the prime 2 and the restriction it imposes on the sufficiency of the desired theorem. This restriction is exemplified by Theorem 3.1.

Section VI

Theorem 1.1 establishes that norm pairs P, S are norm-like pairs and, if $S \neq 1$, P has bounded order. A trivial example of the converse is provided by the norm-like pair P, S with $S = 1$. Theorem 6.1 gives sufficient conditions for norm-like pairs to be norm pairs.

THEOREM 6.1. *If P, S is a norm-like pair such that P has bounded order p^m with $p \neq 2$ and such that S contains elements of maximum order which are disjoint, then P, S is a norm pair.*

Proof. The problem is to construct a group G such that $P \leqq N(G)$, P is normal in G, and G induces exactly the group of automorphisms S on P. If $S = 1$, let $G = P$. If $S \neq 1$, S contains 2 elements of maximum order which are disjoint. From Lemma 4.1 and the second remark of Section IV, there exists an $x \in P$ such that $x(1 - c)$ generates $P(1 - c)$ for every $c \in S$. By the first remark of Section IV and Lemma 2.3, S is a commutative group of bounded order, and therefore S has a basis b_i. Let G be the group formed by adjoining x_i to P with the following properties: x_i induces b_i on P, $x_i + x_j = x_j + x_i$, and $p^m x_i = x(1 - b_i)$. G contains P as a normal subgroup, and induces exactly S as automorphism group on P. Therefore, we need only show that $P \leqq N(G)$. The general element of G has the form $y + a$ with $y \in P$ and a a finite sum of x_i, where a given x_i may occur more than once. If $a \in G$ induces the automorphism a on P, then $a + y = y + a + y(1 - a)$ since P is commutative. Since $p^m P = 0$ and p is not divisible by 2,

$$p^m(a + y) = p^m a + p^m y + y(1 - a) + 2y(1 - a) + \cdots + (p^m - 1)y(1 - a) = p^m a + (p^m - 1)p^m/2 \cdot y(1 - a) = p^m a.$$

By Corollary 3.2,

$$1 - cd = 1 - c + c - cd = (1 - c) + (1 - d)c = (1 - c) + (1 - d)$$

for every c and d in S. Therefore, if $a = x_1 + \cdots + x_k$,

$$p^m a = x(1 - b_1) + \cdots + x(1 - b_k) = x(1 - \prod_i b_i),$$

and the automorphism $a = \prod_i b_i$ since x_i induces b_i. Since $x(1 - a)$ generates $P(1 - a)$ and $p^m a = p^m(a + y)$, $P(1 - a) \leqq (a + y)$. Since $a + y$ was a general element of G, we have, for every $z \in P$ and every $w \in G$, $z(1 - w) = z - w - z + w \in (w)$. This is equivalent to $P \leqq N(G)$ since every element of G has finite order.

Bibliography

Reinhold Baer

1. *Der Kern, eine charakteristische Untergruppe*, Compositio Math., vol. 1 (1934), pp. 254–283.
2. *Gruppen mit hamiltonschem Kern*, Compositio Math., vol. 2 (1935), pp. 241–246.
3. *Zentrum und Kern von Gruppen mit Elementen unendlicher Ordnung*, Compositio Math., vol. 2 (1935), pp. 247–249.
4. *Norm and Hypernorm*, Publ. Math. Debrecen, vol. 4 (1956), pp. 347–350.

Hans Zassenhaus

1. *Theory of groups*, New York, 1949.

University of Illinois
Urbana, Illinois
Argonne National Laboratory
Lemont, Illinois