PACIFIC JOURNAL OF MATHEMATICS
Vol. 31, No. 1, 1969

ON THE SUBRING STRUCTURE OF FINITE NILPOTENT RINGS

ROBERT L. KRUSE AND DAVID T. PRICE

This paper studies the nilpotent ring analogues of several well-known results on finite p-groups. We first prove an analogue for finite nilpotent p-rings [a ring is called a p-ring if its additive group is a p-group] of the Burnside Basis Theorem, and use this to obtain some information on the automorphism groups of these rings. Next we obtain Anzahl results, showing that the number of subrings, right ideals, and two-sided ideals of a given order in a finite nilpotent p-ring is congruent to 1 mod p. Finally, we characterize the class of nilpotent p-rings which have a unique subring of a given order.

The analogy between nilpotent groups and nilpotent rings which motivates the results of this paper is the replacement of group commutation by ring product. A nilpotent ring, of course, is itself a group under the circle composition $x \circ y = x + y + xy$ but the structure of this group implies little about the invariants to be studied here, as shown by the examples in the last section of the paper.

All rings considered here are associative. The reader may verify, however, that all results of §§ 1–3 hold without the assumption of associativity, with the exception of (3.3). The unqualified word "ideal" means two-sided ideal. The letter p always denotes a prime number. If $\mathfrak{R}$ is a ring, we denote the additive group of $\mathfrak{R}$ by $\mathfrak{R}^+$. The *order* of a ring $\mathfrak{R}$, denoted $|\mathfrak{R}|$, is the order of the group $\mathfrak{R}^+$; the *index* of a subring $\mathfrak{S}$ in a ring $\mathfrak{R}$, denoted $[\mathfrak{R}:\mathfrak{S}]$, is the index of $\mathfrak{S}^+$ in $\mathfrak{R}^+$. A ring is called *null* if all products are 0. A ring $\mathfrak{R}$ is called *nilpotent* of *exponent* e if all products of e elements from $\mathfrak{R}$ are 0, but not all products of $e-1$ elements are 0. The *characteristic* of a finite ring is the maximum of the additive orders of its elements. The smallest ideal containing ideals $\mathfrak{S}$ and $\mathfrak{T}$ is denoted $\mathfrak{S}+\mathfrak{T}$.

We shall need the following elementary results:

(1.1) Let $\mathfrak{R}$ be a ring with periodic additive group. The primary decomposition of $\mathfrak{R}^+$ decomposes $\mathfrak{R}$ into a ring direct sum of p-rings.

Hence, in studying finite rings, it is sufficient to consider only p-rings.

(1.2.) Let $\mathfrak{J}$ be a maximal ideal of a nilpotent p-ring $\mathfrak{R}$. Then $[\mathfrak{R}:\mathfrak{J}] = p$, $\mathfrak{R}^2 \subseteq \mathfrak{J}$, and $p\mathfrak{R} \subseteq \mathfrak{J}$.

(1.3) Let $\mathfrak{S}$ be a proper subring of a finite nilpotent ring $\mathfrak{R}$. Then there is a maximal ideal of $\mathfrak{R}$ which contains $\mathfrak{S}$.

(1.4) If $\mathfrak{M}$ and $\mathfrak{N}$ are nonzero, nonempty subsets of a nilpotent ring, then $\mathfrak{M}$ is not contained in $\{\mu\nu \mid \mu \in \mathfrak{M}, \nu \in \mathfrak{N}\}$.

(1.5) A nilpotent ring of order p^n contains an ideal of every possible order p^i, $0 \leqq i \leqq n$.

2. **Burnside Basis Theorem.** The *Frattini subring* $\Phi_{\mathfrak{R}}$ of a ring $\mathfrak{R}$ is defined to be the intersection of the maximal ideals of $\mathfrak{R}$, provided such exist. Otherwise, $\Phi_{\mathfrak{R}} = \mathfrak{R}$. A set of elements of a ring $\mathfrak{R}$ *generates* a subring $\mathfrak{S}$ if $\mathfrak{S}$ is the smallest subring of $\mathfrak{R}$ containing all the elements.

THEOREM 2.1. *Let $\mathfrak{R}$ be a finite nilpotent p-ring. Then $\mathfrak{A} = \mathfrak{R}/\Phi_{\mathfrak{R}}$ is a null ring, and $\mathfrak{A}^+$ is elementary abelian. Let $[\mathfrak{R}: \Phi_{\mathfrak{R}}] = p^d$. Then any set of elements of $\mathfrak{R}$ which generates $\mathfrak{R}$ contains a subset of d elements, $\{\theta_1, \cdots, \theta_d\}$, which generates $\mathfrak{R}$. In the canonical homomorphism of $\mathfrak{R}$ onto $\mathfrak{A}$ the elements $\theta_1, \cdots, \theta_d$ map onto a basis of $\mathfrak{A}^+$. If, conversely, $\theta_1 + \Phi_{\mathfrak{R}}, \cdots, \theta_d + \Phi_{\mathfrak{R}}$ form a basis of $\mathfrak{A}^+$, then $\theta_1, \cdots, \theta_d$ generate $\mathfrak{R}$.*

Proof. By (1.2) $\mathfrak{A}$ is a null ring and $\mathfrak{A}^+$ is elementary abelian. Thus the images under the canonical homomorphism $\mathfrak{R} \to \mathfrak{A}$ of any generating set for $\mathfrak{R}$ must contain a basis for $\mathfrak{A}^+$. Let $\{\theta_1, \cdots, \theta_d\}$ be a set of elements whose images form a basis for $\mathfrak{A}^+$. Suppose $\theta_1, \cdots, \theta_d$ generate a proper subring of $\mathfrak{R}$. By (1.3) this subring is contained in a maximal ideal $\mathfrak{J}$, which contains $\Phi_{\mathfrak{R}}$. Thus

$$\theta_1 + \Phi_{\mathfrak{R}}, \cdots, \theta_d + \Phi_{\mathfrak{R}}$$

are in $\mathfrak{J}/\Phi_{\mathfrak{R}}$, which is proper in $\mathfrak{A}$. This contradicts the assumption that the images of $\theta_1, \cdots, \theta_d$ form a basis of $\mathfrak{A}^+$. This completes the proof.

REMARK 1. Theorem 2.1 implies that a finite nilpotent p-ring contains a unique maximal subring (= ideal) if and only if it is generated by a single element. A ring [an associative algebra] generated by one element we call a *power ring* [*power algebra*], since the additive group of the ring [the underlying vector space of the algebra] is spanned by the generator and its powers. Whereas a group generated by one element is completely determined by its order, the same is not true for power rings. In fact, even specification of

the additive group and the exponent of the ring are not generally sufficient to determine a nilpotent power ring up to isomorphism. There is, of course, only one nilpotent power algebra of a given dimension over any field. Note, finally, that all nilpotent power rings [algebras] are finite [finite-dimensional].

REMARK 2. It is frequently convenient to use the observation that $\Phi_{\mathfrak{R}} = \mathfrak{R}^2 + p\mathfrak{R}$ for every finite nilpotent p-ring $\mathfrak{R}$. To prove this, observe that (1.2) implies $\mathfrak{R}^2 + p\mathfrak{R} \subseteq \Phi_{\mathfrak{R}}$, while $\mathfrak{F} = \mathfrak{R}/(\mathfrak{R}^2 + p\mathfrak{R})$ is a null ring and $\mathfrak{F}^+$ is elementary abelian, so the intersection of the maximal subrings of $\mathfrak{F}$ is 0, which means $\Phi_{\mathfrak{F}} = 0$, so $\Phi_{\mathfrak{R}} \subseteq \mathfrak{R}^2 + p\mathfrak{R}$.

As an application of Theorem 2.1, we shall now derive some information about the group of automorphisms of a finite nilpotent p-ring.

THEOREM 2.2. *Let $\mathfrak{R}$ be a nilpotent ring of order p^n, and let $[\mathfrak{R}: \Phi_{\mathfrak{R}}] = p^d$. Then the order of the automorphism group of $\mathfrak{R}$ divides $p^{d(n-d)}\Theta(p^d)$, where*

$$\Theta(p^d) = (p^d - 1)(p^d - p) \cdots (p^d - p^{d-1}) .$$

The order of the group of automorphisms of $\mathfrak{R}$ which fix $\mathfrak{R}/\Phi_{\mathfrak{R}}$ elementwise divides $p^{d(n-d)}$.

Proof. This result, due to P. Hall for p-groups, follows in the same way as § 1.3 of [2].

If $\mathfrak{F}$ is an ideal of a ring $\mathfrak{R}$, we now define $\mathrm{Aut}(\mathfrak{R}; \mathfrak{F})$ to be the group of all automorphisms of $\mathfrak{R}$ which leave $\mathfrak{R}/\mathfrak{F}$ fixed elementwise. For $\mathfrak{R}$ a finite nilpotent p-ring we shall obtain a bound on the class of the p-group $\mathscr{P} = \mathrm{Aut}(\mathfrak{R}; \Phi_{\mathfrak{R}})$. These results are analogues of those obtained by H. Liebeck [4] for p-groups.

THEOREM 2.3. *Let $\mathfrak{R}$ be a finite p-ring, nilpotent of exponent e, for which $\Phi_{\mathfrak{R}} \neq 0$. Let $\mathfrak{R}^i/\mathfrak{R}^{i+1}$ have characteristic p^{m_i}, $i = 1, \cdots, e-1$. Then the class of $\mathscr{P} = \mathrm{Aut}(\mathfrak{R}; \Phi_{\mathfrak{R}})$ does not exceed*

$$\lambda(\mathfrak{R}) = \left(\sum_{i=1}^{e-1} m_i\right) - 1 .$$

This theorem will follow by induction from the next result.

THEOREM 2.4. *Let $\mathfrak{R}$ be a finite p-ring, nilpotent of exponent e, for which $\Phi_{\mathfrak{R}} \neq 0$. Let $\mathfrak{R}^{e-1}$ have characteristic p^m and let $\mathfrak{N} = p^{m-1}\mathfrak{R}^{e-1}$. Then*

(i) *the ideal $\mathfrak{N}$ is elementwise fixed by $\mathscr{P} = \mathrm{Aut}(\mathfrak{R}; \Phi_{\mathfrak{R}})$.*

(ii) $\mathscr{Z} = \mathrm{Aut}(\mathfrak{R}; \mathfrak{N})$ *is in the center of* $\mathscr{P}$.

(iii) $\mathscr{Z}$ *has order* p^{rd}, *where* p^r *is the order of* $\mathfrak{N}$, *and* $p^d = [\mathfrak{R}: \Phi_{\mathfrak{R}}]$.

(iv) $\mathscr{P}/\mathscr{Z}$ *is isomorphic to the subgroup* $\mathscr{Q}$ *of automorphisms from* $\mathrm{Aut}(\mathfrak{R}/\mathfrak{N}; \Phi_{\mathfrak{R}}/\mathfrak{N})$ *which can be extended to* $\mathfrak{R}$.

The proof of (2.4) requires three lemmas, the first of which is obvious.

LEMMA 2.5. *Let* $\mathfrak{R}$ *be a ring and* α *an automorphism of* $\mathfrak{R}$. *If* $\{\theta_1, \cdots, \theta_d\}$ *is a generating set for* $\mathfrak{R}$, *then* α *is completely determined by the values of* $\theta_i^\alpha, 1 \leqq i \leqq d$. *If* $\mathfrak{I}$ *is an ideal of* $\mathfrak{R}$ *then* $\alpha \in \mathrm{Aut}(\mathfrak{R}; \mathfrak{I})$ *if and only if* $\theta_i^\alpha - \theta_i \in \mathfrak{I}, 1 \leqq i \leqq d$.

LEMMA 2.6. *With* $\mathfrak{R}$ *as in* (2.4), *if* $\alpha \in \mathscr{P}$ *and* $\theta \in \mathfrak{R}^i$ *for some* i, $1 \leqq i \leqq e-1$, *then* $\theta^\alpha - \theta \in p\mathfrak{R}^i + \mathfrak{R}^{i+1}$.

Proof. The lemma is true for $i = 1$, since $\Phi_{\mathfrak{R}} = p\mathfrak{R} + \mathfrak{R}^2$ and $\alpha \in \mathrm{Aut}(\mathfrak{R}; \Phi_{\mathfrak{R}})$. Assume the result for $i < j$. Let $\theta \in \mathfrak{R}^j$. Express θ as a sum of products

$$\theta = \sum_r \pi_r \rho_r$$

where the $\pi_r \in \mathfrak{R}^{j-1}$, $\rho_r \in \mathfrak{R}$. Then $\theta^\alpha = \sum \pi_r^\alpha \rho_r^\alpha = \sum (\pi_r + \sigma_r)(\rho_r + \tau_r)$, where, by induction hypothesis, $\sigma_r \in p\mathfrak{R}^{j-1} + \mathfrak{R}^j$ and $\tau_r \in p\mathfrak{R} + \mathfrak{R}^2$. Thus $\theta^\alpha - \theta = \sum (\sigma_r \rho_r + \pi_r \tau_r + \sigma_r \tau_r) \in p\mathfrak{R}^j + \mathfrak{R}^{j+1}$.

LEMMA 2.7. *With the notation of* (2.4), *every automorphism* $\zeta \in \mathscr{Z}$ *leaves* $\Phi_{\mathfrak{R}}$ *elementwise fixed.*

Proof. For any $\theta \in \mathfrak{R}$, $\theta^\zeta - \theta \in \mathfrak{N}$. Thus from $p\mathfrak{N} = 0$ follows $0 = p(\theta^\zeta - \theta) = (p\theta)^\zeta - p\theta$, so $\mathscr{Z}$ fixes $p\mathfrak{R}$ elementwise. Similarly, since $\mathfrak{N}\mathfrak{R} = \mathfrak{R}\mathfrak{N} = 0$, $\mathscr{Z}$ fixes $\mathfrak{R}^2$, hence $\Phi_{\mathfrak{R}} = \mathfrak{R}^2 + p\mathfrak{R}$, elementwise.

Proof of (2.4). (i) Suppose $\theta \in \mathfrak{N}$ and $\alpha \in \mathscr{P}$. Then $\theta = p^{m-1}\psi$ for some $\psi \in \mathfrak{R}^{e-1}$, and so, by (2.6),

$$\theta^\alpha - \theta = p^{m-1}(\psi^\alpha - \psi) \in p^{m-1}(p\mathfrak{R}^{e-1} + \mathfrak{R}^e) = 0 .$$

(ii) Let $\theta \in \mathfrak{R}$, $\alpha \in \mathscr{P}$, and $\zeta \in \mathscr{Z}$. Then

$$\begin{aligned}(\theta^\alpha)^\zeta &= (\theta + \rho)^\zeta \text{ for some } \rho \in \Phi_{\mathfrak{R}} \\ &= \theta^\zeta + \rho \text{ by (2.7)} \\ &= \theta + \rho + \sigma \text{ for some } \sigma \in \mathfrak{N} ,\end{aligned}$$

while

$$(\theta^{\zeta})^{\alpha} = (\theta + \sigma)^{\alpha} = \theta^{\alpha} + \sigma[\text{by (i)}] = \theta + \sigma + \rho\ .$$

Thus $\alpha\zeta = \zeta\alpha$.

(iii) Let $\theta_1, \cdots, \theta_d$ generate $\mathfrak{R}$, and $\psi_1, \cdots \psi_d$ be arbitrary elements of $\mathfrak{R}$. Then the mapping

$$(*) \qquad \theta_i \to \theta_i + \psi_i,\ i = 1, \cdots, d\ ,$$

defines an automorphim $\zeta \in \mathscr{Z}$. But every automorphism $\zeta \in \mathscr{Z}$ induces a mapping of the form (*). Thus $|\mathscr{Z}| = p^{rd}$.

(iv) Let $\alpha \in \mathscr{P}$. Defining $(\theta + \mathfrak{N})^{\alpha} = \theta^{\alpha} + \mathfrak{N}$ for all $\theta \in \mathfrak{R}$ gives, by (i), a homomorphism f of $\mathscr{P}$ into $\mathscr{Q}$. If $(\theta + \mathfrak{N})^{\alpha} = \theta + \mathfrak{N}$, all θ, then $\theta^{\alpha} - \theta \in \mathfrak{N}$, so $\alpha \in \mathscr{Z}$. Thus the kernel of f is $\mathscr{Z}$. Now consider an automorphism $\beta' \in \mathscr{Q}$. Let β be an extension of β' to $\mathfrak{R}$, $\beta \in \mathscr{P}$. Then $f\beta \in \mathscr{Q}$, and for $\theta \in \mathfrak{R}$, $(\theta + \mathfrak{N})^{f\beta} = \theta^{\beta} + \mathfrak{N} = (\theta + \mathfrak{N})^{\beta'}$ so the homomorphism f is onto $\mathscr{Q}$. This completes the proof of (2.4).

Proof of (2.3). $\lambda(\mathfrak{R}) = 0$ implies $e = 2$ and $m_1 = 1$, hence $\Phi_{\mathfrak{R}} = 0$, contrary to assumption. If $\lambda(\mathfrak{R}) = 1$, then either $e = 2, m_1 = 2$, or else $e = 3, m_1 = m_2 = 1$. In either case, for $\mathfrak{N} = p^{m_{e-1}^{-1}}\mathfrak{R}^{e-1}$, $\mathfrak{N} = \Phi_{\mathfrak{R}}$. Hence, by (ii) of (2.4), $\mathscr{P}$ is abelian. We now use induction on $\lambda(\mathfrak{R})$. Let $\mathfrak{N} = p^{m_{e-1}^{-1}}\mathfrak{R}^{e-1}$. By (2.4) $\mathscr{Z} = \text{Aut}\,(\mathfrak{R}; \mathfrak{N})$ is central in $\mathscr{P}$ and $\mathscr{P}/\mathscr{Z}$ is isomorphic to a subgroup $\mathscr{Q}$ of $\text{Aut}\,(\mathfrak{R}/\mathfrak{N}; \Phi_{\mathfrak{R}}/\mathfrak{N})$. Since $\lambda(\mathfrak{R}/\mathfrak{N}) = \lambda(\mathfrak{R}) - 1 < \lambda(\mathfrak{R})$, by induction hypothesis the class of $\mathscr{Q}$ does not exceed $\lambda(\mathfrak{R}/\mathfrak{N})$. Thus the class of $\mathscr{P}$ does not exceed $\lambda(\mathfrak{R}) = \lambda(\mathfrak{R}/\mathfrak{N}) + 1$.

REMARK. The bounds given in Theorems 2.2 and 2.3 are attained by the free nilpotent rings of characteristic p with two or more generators.

3. Enumeration results.

The results of this section depend upon the following lemma, which is essentially the enumeration principle of Philip Hall ([2], Th. 1.4).

LEMMA 3.1. *Let* $\mathfrak{U}$ *be a finite p-group,* $\mathscr{M}$ *the set of maximal subgroups of* $\mathfrak{U}$ *which contain a fixed subgroup* $\mathfrak{B} \neq \mathfrak{U}$. *Let* $\mathscr{C}$ *be any class whose members are subsets of* $\mathfrak{U}$, *and let each member of* $\mathscr{C}$ *be contained in at least one member of* $\mathscr{M}$. *Let* $n(M)$ *be the number of members of* $\mathscr{C}$ *which are contained in* M *for each* $M \in \mathscr{M}$. *Then the number of members of* $\mathscr{C}$ *is congruent to* $\sum_{M \in \mathscr{M}} n(M)$ (mod p).

THEOREM 3.2. *Let* $\mathfrak{R}$ *be a nilpotent ring of order* p^n. *Let* $\mathfrak{S}$ *be a subring of* $\mathfrak{R}$, *of order* p^s. *Then for* $s \leqq t \leqq n$, *the number of*

subrings of $\mathfrak{R}$ *of order* p^t *which contain* $\mathfrak{S}$ *is congruent to* 1 (mod p).

Proof. If $\mathfrak{S} = \mathfrak{R}$, the result is trivial. Suppose $\mathfrak{S} \neq \mathfrak{R}$. We proceed by induction on n. Let $\mathscr{M}$ be the set of maximal subgroups of $\mathfrak{R}^+$ which contain $\mathfrak{B}^+ = (\mathfrak{S} + \mathfrak{R}^2)^+$. By (1.2) and (1.3), $\mathscr{M}$ is non-empty. Letting $\mathscr{C} = \{\mathfrak{S}\}$ in (3.1), we see that the number of members of $\mathscr{M}$ is congruent to 1 (mod p). If $t = n$, the result is trivial. Suppose $t < n$. Let $\mathscr{C} = \{\mathfrak{T} \mid \mathfrak{S} \subseteq \mathfrak{T}, |\mathfrak{T}| = p^t, \mathfrak{T}$ is a subring of $\mathfrak{R}\}$. By (1.3) and (1.2) each $\mathfrak{T} \in \mathscr{C}$ is contained in some $M \in \mathscr{M}$. Let $n(M)$ be the number of members of $\mathscr{C}$ contained in M, for each $M \in \mathscr{M}$. By induction, $n(M) \equiv 1 \pmod{p}$. Hence, by (3.1), the number of members of $\mathscr{C}$ is congruent to 1 (mod p).

It is well known that the number of normal subgroups of a given order in a finite p-group is congruent to 1 (mod p). For rings there are several analogous results.

THEOREM 3.3. *Let* $\mathfrak{B}$ *be a right module of order* p^n *of a nilpotent ring* $\mathfrak{R}$. *The number of submodules of* $\mathfrak{B}$ *of order* p^k, $0 \leqq k \leqq n$, *is congruent to* 1 (mod p).

THEOREM 3.4. *Let* $\mathfrak{J}$ *be a right ideal of order* p^m *of a nilpotent ring* $\mathfrak{R}$ *of order* p^n. *The number of right ideals of* $\mathfrak{R}$ *of order* p^k *which contain* $\mathfrak{J}$ (*which are contained in* $\mathfrak{J}$), $m \leqq k \leqq n$ $(0 \leqq k \leqq m)$, *is congruent to* 1 mod p.

THEOREM 3.5. *Let* $\mathfrak{J}$ *be a two-sided ideal of order* p^m *of a nilpotent ring* $\mathfrak{R}$ *of order* p^n. *The number of two-sided ideals of* $\mathfrak{R}$ *of order* p^k *which contain* $\mathfrak{J}$ (*which are contained in* $\mathfrak{J}$), $m \leqq k \leqq n$ $(0 \leqq k \leqq m)$, *is congruent to* 1 mod p.

The proofs of these results are similar to that of (3.2).

REMARK 1. No analogue of the theorem of Kulakoff seems to hold for nilpotent rings. For example, the rings with basis α, β, such that $p^2\alpha = p^2\beta = 0$, $\alpha^2 = -\beta^2 = p\alpha$, and $\alpha\beta = \beta\alpha = 0$, have $3p + 1$ subrings of order p^2 if $p \neq 2$, and 5 if $p = 2$.

REMARK 2. Note that the Anzahl theorems fail to hold for non-nilpotent p-rings. For example, consider the ring $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2$, where $\mathfrak{R}_1$ is generated by an element α of characteristic p with $\alpha^2 = \alpha$, and $\mathfrak{R}_2$ is generated by an element β of characteristic p with $\beta^2 = 0$. Then $\mathfrak{R}_1$ and $\mathfrak{R}_2$ are the only two subrings (and ideals) of order p, and $2 \not\equiv 1$ (mod p) for any prime p.

4. **Nilpotent p-rings with only one subring of a given order.** It is well-known that a finite p-group $\mathfrak{G}$ which contains only one subgroup $\mathfrak{S}$ of a given order, $1 \neq \mathfrak{S} \neq \mathfrak{G}$, must be cyclic, or else $|\mathfrak{S}| = 2$ and $\mathfrak{G}$ is generalized quaternion [1; 131–132]. This section obtains a characterization of nilpotent rings and (associative) algebras satisfying the analogous condition. Although the algebra result could be obtained as a corollary to the ring result, we shall give an independent proof to illustrate the general ideas used while avoiding much detail required for the ring proof. The result for algebras is

THEOREM 4.1. *A nilpotent algebra $\mathfrak{U}$ over a field $\mathfrak{F}$ contains only one subalgebra $\mathfrak{S}$ of some given finite dimension, $0 \neq \mathfrak{S} \neq \mathfrak{U}$, if and only if one of the following conditions holds:*

(1) $\dim \mathfrak{S} = \dim \mathfrak{U} - 1$ *and* $\mathfrak{U}$ *is a power algebra.*

(2) $\dim \mathfrak{S} = 1, \dim \mathfrak{U} \geqq 3, \mathfrak{U}^2 = \mathfrak{S}, \mathfrak{U}^3 = 0$, *and* $\varphi \in \mathfrak{U}, \varphi^2 = 0$ *implies* $\varphi \in \mathfrak{S}$.

REMARK 1. An algebra $\mathfrak{U}$ such that $\dim \mathfrak{U}^2 = 1$, $\mathfrak{U}^3 = 0$, and $\varphi \in \mathfrak{U}$, $\varphi^2 = 0$ implies $\varphi\mathfrak{U} = \mathfrak{U}\varphi = 0$, is called "almost-null." It may be of interest to note that a nil algebra has the property that every subalgebra is an ideal if and only if the algebra is almost-null (see Kruse [3]). Thus almost-null algebras seem in one way analogous to the quaternion group of order 8, which plays a key role both in the determination of p-groups with a unique subgroup of order p, and in the determination of groups in which all subgroups are normal.

REMARK 2. The classification of the finite-dimensional algebras $\mathfrak{U}$ over a field $\mathfrak{F}$ satisfying (2) of (4.1) is closely related to the study of quadratic forms over $\mathfrak{F}$. Let $\mathfrak{U}$ have a basis $\{\alpha_1, \alpha_2, \cdots, \alpha_n, \beta\}$ with $\beta \in \mathfrak{U}^2$, and choose $a_{ij} \in \mathfrak{F}$, $1 \leqq i, j \leqq n$, so that $\alpha_i\alpha_j = a_{ij}\beta$. Then condition (2) requires that the quadratic form

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}x_ix_j$$

have no nontrivial zero $(x_1, x_2, \cdots, x_n)$. Let us note that when $\mathfrak{F}$ is a finite field, then every quadratic form in three variables has a nontrivial zero, so if $\mathfrak{F}$ is finite then $\dim \mathfrak{U} = 3$. On the other hand, over each finite field there exists a quadratic form in two variables with no nontrivial zero, so algebras satisfying (2) always occur when $\mathfrak{F}$ is finite.

Finally, we note that an arbitrary almost-null algebra must either be null, or isomorphic to the direct sum of a null algebra and either a power algebra of dimension 2 or an algebra satisfying (2).

Proof of (4.1). It is easy to check that nilpotent algebras satisfy-

ing (1) or (2) have unique subalgebras of the dimensions indicated. For the converse we shall first establish two lemmas.

LEMMA 4.2. *If* $\mathfrak{U}$ *is a nilpotent algebra of dimension* 4, *over a field* $\mathfrak{F}$, *then* $\mathfrak{U}$ *has more than one subalgebra of dimension* 2.

Proof. If $\dim \mathfrak{U}^2 = 3$, then $\mathfrak{U}$ is a power algebra, generated by one element α. Then all subalgebras generated by $\alpha^2 + x\alpha^3$ for different $x \in \mathfrak{F}$ are distinct and all have dimension 2. If $\dim \mathfrak{U}^2 \leqq 1$ then $\mathfrak{U}/\mathfrak{U}^2$ is null, and $\mathfrak{U}$ contains more than one subalgebra of dimension 2. Thus we can suppose that $\dim \mathfrak{U}^2 = 2$, and $\mathfrak{U}^2$ is the only subalgebra of $\mathfrak{U}$ of dimension 2. It follows, for any $\varphi \in \mathfrak{U}$, $\varphi \in \mathfrak{U}^2$, that $\varphi^3 \neq 0$. Since $\dim \mathfrak{U}^2 = 2$, there are elements $\alpha, \beta \in \mathfrak{U}$ which are linearly independent mod $\mathfrak{U}^2$, so $\{\alpha, \beta, \alpha^2, \alpha^3\}$ is a basis for $\mathfrak{U}$. Choose $x, y \in \mathfrak{F}$ so that $\alpha\beta = x\alpha^2 + y\alpha^3$ and let $\beta' = \beta - x\alpha - y\alpha^2$. Then $\beta' \in \mathfrak{U}^2$, and $\alpha\beta' = 0$. Let $\beta'^2 = u\alpha^2 + v\alpha^3$, $u, v \in \mathfrak{F}$. Then $0 = (\alpha\beta')\beta' = u\alpha^3$ so $u = 0$. Then $\beta'^3 = 0$ and $\beta' \in \mathfrak{U}^2$, a contradiction.

LEMMA 4.3. *Let* $\mathfrak{U}$ *be a nilpotent algebra with a unique subalgebra* $\mathfrak{S}$ *of dimension* 1, *and let* $\varphi \in \mathfrak{U}$. *If* $\varphi^2 = 0$ *then* $\varphi \in \mathfrak{S}$. *If* $\varphi \notin \mathfrak{S}$, *then* $0 \neq \varphi^2 \in \mathfrak{S}$.

Proof. If $\varphi^2 = 0$ then either $\varphi = 0$ or φ generates a subalgebra of dimension 1, which by hypothesis must be $\mathfrak{S}$. Thus $\varphi \in \mathfrak{S}$. Suppose $\varphi \notin \mathfrak{S}$, and let e be the natural number such that $\varphi^e = 0$ but $\varphi^{e-1} \neq 0$. By the above argument $e \geqq 3$. If $e \geqq 4$ then $(\varphi^{e-2})^2 = 0$ so $\varphi^{e-2} \in \mathfrak{S}$. But $\mathfrak{S}$ is an ideal, so nilpotence of $\mathfrak{U}$ implies $\mathfrak{U}\mathfrak{S} = 0$, so $\varphi\varphi^{e-2} = 0$, contradicting the definition of e. Thus $e = 3$. Then $(\varphi^2)^2 = 0$ so $0 \neq \varphi^2 \in \mathfrak{S}$.

Proof of 4.1, *continued.* Let $\mathfrak{U}$ be a nilpotent algebra with a unique subalgebra $\mathfrak{S}$ of a given dimension, $0 \neq \mathfrak{S} \neq \mathfrak{U}$. If $\dim \mathfrak{U} = \dim \mathfrak{S} + 1$, then $\mathfrak{U}$ is a power algebra, and condition (1) of the conclusion holds. If $\dim \mathfrak{U} \geqq \dim \mathfrak{S} + 2 \geqq 4$ then, by the algebra analogue of (1.5), $\mathfrak{U}$ contains a subalgebra $\mathfrak{B}$ with $\dim \mathfrak{B} = \dim \mathfrak{S} + 2$, and an ideal $\mathfrak{J}$ with $\dim \mathfrak{J} = \dim \mathfrak{S} - 2$. Then the algebra $\mathfrak{B}/\mathfrak{J}$ fails to satisfy (4.2). Hence we can suppose $\dim \mathfrak{S} = 1$, $\dim \mathfrak{U} \geqq 3$.

Next we show that $\mathfrak{U}^2 = \mathfrak{S}$. Choose $\varphi, \psi \in \mathfrak{U}$. By (4.3), φ^2, ψ^2, and $(\varphi + \psi)^2$ are in $\mathfrak{S}$. Thus $\varphi\psi + \psi\varphi \in \mathfrak{S}$. Hence $0 = \varphi(\varphi\psi + \psi\varphi) = \varphi\psi\varphi$, since $\varphi^2 \in \mathfrak{S}$ and $\mathfrak{S}\mathfrak{U} = 0$. Thus $(\varphi\psi)^2 = 0$, so by (4.3) $\varphi\psi \in \mathfrak{S}$. Thus $\mathfrak{U}^2 \subseteqq \mathfrak{S}$. $\mathfrak{U}^2 \neq 0$ is trivial, so $\mathfrak{U}^2 = \mathfrak{S}$. (4.3) now implies directly that $\mathfrak{U}$ satisfies (2) of (4.1). Thus the proof is complete.

We now turn to the analogous problem for rings. We shall

establish the following:

THEOREM 4.4. *A nilpotent p-ring* $\mathfrak{R}$ *contains only one subring* $\mathfrak{S}$ *of a given order,* $0 \neq \mathfrak{S} \neq \mathfrak{R}$, *if and only if* $\mathfrak{R}$ *and* $\mathfrak{S}$ *satisfy one of the following conditions:*

(1) $\mathfrak{R}^+$ *is cyclic or quasi-cyclic.*

(2) $[\mathfrak{R}: \mathfrak{S}] = p$. $\mathfrak{R}$ *is a power ring.*

(3) $|\mathfrak{S}| = p$. *Let* $\mathfrak{U} = \{\varphi \in \mathfrak{R} \mid p\varphi = 0\}$. *Then* $\mathfrak{U}^+$ *has rank 2 or 3,* $\mathfrak{U}^2 = \mathfrak{S}$, *and* $\varphi \in \mathfrak{U}$, $\varphi^2 = 0$ *implies* $\varphi \in \mathfrak{S}$. *There is, moreover, an ideal* $\mathfrak{C}$ *of* $\mathfrak{R}$ *such that* $\mathfrak{R} = \mathfrak{C} + \mathfrak{U}$, $\mathfrak{C} \cap \mathfrak{U} = \mathfrak{S}$, *and* $\mathfrak{C}^+$ *is cyclic or quasi-cyclic.*

(4) $|\mathfrak{S}| = p^2$. $|\mathfrak{R}| = p^4$, $\mathfrak{R}^+$ *has type* (2,2), *and, if* $\varphi \in \mathfrak{R}$ *with* $p\varphi \neq 0$, *then* $p\varphi^2 = 0$ *and* φ^2 *is not a natural multiple of* φ.

REMARK. A description of the "exceptional" nilpotent p-ring $\mathfrak{R}$ satisfying (3) or (4) may be completed in terms of generators and relations as follows:

(3) Let $\mathfrak{S}$ be generated by an element σ. Then $p\sigma = 0$ and $\sigma\mathfrak{R} = \mathfrak{R}\sigma = 0$. If $\mathfrak{C}^+$ is quasi-cyclic, then $\mathfrak{C}\mathfrak{R} = \mathfrak{R}\mathfrak{C} = 0$. The subring $\mathfrak{U}$ satisfies one of the following conditions:

(a) $\mathfrak{U}^+$ has a basis σ, β, and $\beta^2 \neq 0$.

(b) $\mathfrak{U}^+$ has a basis σ, β_1, β_2. Let $\beta_i\beta_j = B_{ij}\sigma$ for suitable integers B_{ij}, $i, j = 1, 2$. Then $B_{11}X^2 + (B_{12} + B_{21})XY + B_{22}Y^2 \equiv 0 \pmod{p}$ for integers X and Y implies $X \equiv Y \equiv 0 \pmod{p}$.

(4) Let $\mathfrak{R}^+$ have a basis α_1 and α_2. Then $\alpha_i\alpha_j = A_{ij}p\alpha_1 + B_{ij}p\alpha_2$ for suitable integers A_{ij}, B_{ij}, $i, j = 1, 2$, and

$$B_{11}X^3 + (A_{11} + B_{12} + B_{21})X^2 + (B_{22} + A_{12} + A_{21})X + A_{22} \equiv 0 \pmod{p}$$

has no integer solution X.

Since, over the field of p elements, there are both quadratic forms in two variables which have no nontrivial zeroes, and irreducible cubic polynomials, rings satisfying (3) and (4) occur nontrivially for all primes p.

Proof of 4.4. It is easy to see that nilpotent p-rings satisfying (1)–(4) have unique subrings of the orders indicated. An infinite nilpotent p-ring which contains only one subring $\mathfrak{S}$ of a given (finite) order clearly satisfies one of (1)–(4) if and only if each of its finite subrings which properly contains $\mathfrak{S}$ also does. Thus for the converse we consider only finite rings. As a notational convenience, let $\mathscr{Z}(n, s)$ denote the class of nilpotent rings of order p^n which contain only one subring, generically denoted $\mathfrak{S}$, of order p^s. If $\mathfrak{R} \in \mathscr{Z}(n, n-1)$, then the basis theorem (2.1) implies $\mathfrak{R}$ is a power ring. The rings in $\mathscr{Z}(n, 1)$

are studied in § 5. To characterize the rings in $\mathscr{U}(n, s), 1 < s < n-1$, we first determine those in $\mathscr{U}(4, 2)$, $\mathscr{U}(5, 2)$, and $\mathscr{U}(5, 3)$ and then proceed by induction. Several steps of the proof are separated as lemmas.

4.5 *Let $\mathfrak{R}$ be a nilpotent p-ring for which $\mathfrak{R}^+$ has type $(n, 1)$. Then, for $1 < i < n$, $\mathfrak{R}$ has exactly $p+1$ ideals of order p^i.*

Proof. For $1 < i \leqq n+1$, $\mathfrak{B}_i = \{\varphi \in \mathfrak{R} \mid p^{i-1}\varphi = 0\}$ is an ideal of $\mathfrak{R}$ of order p^i. For $1 \leqq i < n$, $\mathfrak{C}_i = \{p^{n-i}\varphi \mid \varphi \in \mathfrak{R}\}$ is an ideal of $\mathfrak{R}$ of order p^i. Hence $\mathfrak{R}$ has at least two, so by the Anzahl theorem (3.5) at least $p+1$, ideals of order $p^i, 1 < i < n$. But these exhaust the subgroups of $\mathfrak{R}^+$ of order p^i.

4.6 *Suppose $\mathfrak{R}$ is a power ring, $\mathfrak{R} \in \mathscr{U}(n, s), 1 \leqq s < n-1$. Then $\mathfrak{R}^+$ is cyclic.*

Proof. First suppose $s = 1$. Let $\mathfrak{R}$ be generated by an element α, and let $\Phi = p\mathfrak{R} + \mathfrak{R}^2$. Let $\mathfrak{M} = \{\varphi \in \Phi \mid p\varphi = 0, \varphi \notin \mathfrak{S}\}$. If $\mathfrak{M}$ is nonempty, then by (1.4) there is some $\delta \in \mathfrak{M}$ such that $\delta\alpha \in \mathfrak{S}$. From $\delta \in \Phi$ follows $\delta = p\psi + \alpha\xi$, some $\psi, \xi \in \mathfrak{R}$. Then $\delta^2 = \delta(p\psi + \alpha\xi) = 0$, so δ generates a second subring of order p. Thus $\mathfrak{M}$ is empty and Φ^+ is cyclic. By (2.1), $[\mathfrak{R}: \Phi] = p$. If $\mathfrak{R}^+$ had type $(n-1, 1)$, then $\Phi = \{\varphi \in \mathfrak{R} \mid p^{n-2}\varphi = 0\}$, so Φ^+ would not be cyclic. Hence $\mathfrak{R}^+$ is cyclic, as desired.

We now proceed by induction on s. Suppose $s > 1$. Let $\mathfrak{J}$ be an ideal of order p of $\mathfrak{R}$. Applying the induction hypothesis to the power ring $\mathfrak{R}/\mathfrak{J}$ we find that $(\mathfrak{R}/\mathfrak{J})^+$ is cyclic. Hence either $\mathfrak{R}^+$ is cyclic or has type $(n-1, 1)$. But type $(n-1, 1)$ is excluded by (4.5).

4.7 *If $\mathfrak{R} \in \mathscr{U}(4, 2)$, then rank $\mathfrak{R}^+ \leqq 2$.*

Proof. $\mathfrak{R}^+$ cannot have rank 4 by Lemma 4.2, where $\mathfrak{F} = GF(p)$, the field of p elements. Suppose $\mathfrak{R}^+$ has rank 3, so $\mathfrak{R}^+$ has type $(2, 1, 1)$. Let $\mathfrak{T} = \{\varphi \in \mathfrak{R} \mid p\varphi = 0\}$. Since $|\mathfrak{T}| = p^3$, $\mathfrak{T}$ contains $\mathfrak{S}$, the unique subring of order p^2. It follows by (2.1) that $\mathfrak{T}$ is a power algebra over $GF(p)$, and so $\mathfrak{R}^+$ has a basis of the form $\{\varphi, \psi, \psi^2\}$ where φ has characteristic p^2, ψ and ψ^2 have characteristic p, and $\psi^3 = p\varphi$. Since $\psi^2 \in \mathfrak{R}^2$ and $\psi^3 \in \mathfrak{R}^2$, $|\mathfrak{R}^2| \geqq p^2$. By (4.6) $\mathfrak{R}$ is not a power ring, so $|\mathfrak{R}^2| \leqq p^2$. Thus $\mathfrak{R}^2 = \mathfrak{S}$, and $\mathfrak{S}^+$ has a basis $\{\psi^2, \psi^3\}$. Hence there are integers A, B such that $\varphi\psi = A\psi^2 + B\psi^3$. Let $\varphi' = \varphi - A\psi - B\psi^2$. Then $\varphi'\psi = 0$. Let $\varphi'^2 = C\psi^2 + D\psi^3$ for suitable integers C, D. Then $0 = \varphi'(\varphi'\psi) = \varphi'^2\psi = C\psi^3$ so $C \equiv 0 \pmod{p}$. Then $\varphi'^2 = Dp\varphi'$, so φ' generates a second subring of order p^2. Thus $\mathfrak{R}^+$ has rank at most 2.

4.8 *If* $\mathfrak{R} \in \mathscr{U}(5, s)$, $s = 2, 3$, *then* $\mathfrak{R}^+$ *is cyclic.*

Proof. Suppose rank $\mathfrak{R}^+ \geqq 3$. Then, for $s = 2$ (resp. for $s = 3$), we can find a subring $\mathfrak{U}$ of order p^4 (resp. an ideal $\mathfrak{J}$ of index p^4) with rank $\mathfrak{U}^+ \geqq 3$ (resp. rank $(\mathfrak{R}/\mathfrak{J})^+ \geqq 3$). This is impossible by (4.7), so rank $\mathfrak{R}^+ \leqq 2$.

Suppose rank $\mathfrak{R}^+ = 2$. By (4.5) $\mathfrak{R}^+$ has type $(3, 2)$. Let α and β, with $p^3\alpha = p^2\beta = 0$, be a basis for $\mathfrak{R}^+$. Since $p\alpha$ and $\{p^2\alpha, p\beta\}$ generate distinct subrings of order p^2, we have $s = 3$. Then $p\mathfrak{R} = \mathfrak{S}$. Moreover, $\mathfrak{R}^2 = \mathfrak{S}$, since otherwise $\mathfrak{R}$ is a power ring, which is excluded by (4.6). Let $\alpha^2 = Ap\alpha + Bp\beta$, $\beta^2 = Cp\alpha + Dp\beta$, $C \not\equiv 0 \pmod{p}$, $\alpha\beta = Ep\alpha + Fp\beta$. By replacing α by $\alpha' = \alpha - EC^{-1}\beta$, where $C^{-1}C \equiv 1 \pmod{p^2}$, we may assume that $E = 0$. Then $(\alpha^2)\beta = BCp^2\alpha$, while $\alpha(\alpha\beta) = 0$. Thus $B \equiv 0 \pmod{p}$, and α generates a second subring of order p^3.

Proof of (4.4), *continued.* If $\mathfrak{R} \in \mathscr{U}(4, 2)$, then by (4.5) and (4.7) either $\mathfrak{R}^+$ is cyclic or has type $(2, 2)$. If $\mathfrak{R}^+$ has type $(2, 2)$ and, for some $\varphi \in \mathfrak{R}$, $p\varphi \neq 0$ and φ^2 is a multiple of φ, then both $p\mathfrak{R}$ and the subring generated by φ have order p^2. Thus (4) of (4.4) holds.

Suppose $\mathfrak{R} \in \mathscr{U}(n, s)$ with $n > 5$, $1 < s < n - 1$. If $s = 2$ and rank $\mathfrak{R}^+ \geqq 2$, we can find a subring of order p^5 and rank $\geqq 2$, which contradicts (4.8). For $s > 2$ we proceed by induction on n. Let $\mathfrak{J}$ be an ideal of $\mathfrak{R}$ of order p. By induction hypothesis $(\mathfrak{R}/\mathfrak{J})^+$ is cyclic. $\mathfrak{R}^+$ cannot have type $(n - 1, 1)$ by (4.5), hence $\mathfrak{R}^+$ is cyclic.

5. **Nilpotent p-rings with one subring of order p.** In this section we shall show that a finite nilpotent p-ring $\mathfrak{R}$ which contains a unique subring $\mathfrak{S}$ of order p satisfies condition (3) of Theorem 4.4. Let $\mathfrak{S}$ be generated by an element σ. Then $p\sigma = 0$ and $\sigma\mathfrak{R} = \mathfrak{R}\sigma = 0$. Small Greek letters will denote elements of $\mathfrak{R}$. For ease of reference we restate the hypothesis that $\mathfrak{S}$ is the only subring of order p.

5.1 *If* $p\varphi = \varphi^2 = 0$, *then* $\varphi \in \mathfrak{S}$.

5.2 *Suppose* $p^a\varphi = 0$ *and* $p^{a-1}\varphi \notin \mathfrak{S}$, $a \geqq 1$. *Then* $a = 1$ *and* $\varphi^2 \in \mathfrak{S}$, $\varphi^2 \neq 0$.

Proof. By (5.1), $(p^{a-1}\varphi)^2 \neq 0$. This, with $p^a\varphi^2 = 0$, gives $2a - 2 < a$, so $a = 1$. Then φ together with $\mathfrak{S}$ generates an algebra over $GF(p)$, so (4.3) implies $\varphi^2 \in \mathfrak{S}$, $\varphi^2 \neq 0$.

LEMMA 5.3. *Let* a_1, a_2, a_3, *and* b *be elements of a ring such that* $pb = 0$ *and there are integers* A_{ij}, $0 \leqq A_{ij} < p$, $i, j = 1, 2, 3$, *such that*

$a_ia_j = A_{ij}b$. *Then there exist integers* $0 \leqq X_i < p$, $i = 1, 2, 3$, *not all* 0, *such that*

$$(X_1a_1 + X_2a_2 + X_3a_3)^2 = 0 .$$

Proof. This is equivalent to the well-known fact that a quadratic form in three variables over the field of p elements represents 0 non-trivially.

LEMMA 5.4. *Let* $\mathfrak{U} = \{\varphi \in \mathfrak{R} \mid p\varphi = 0\}$. *Then* $\mathfrak{U}^2 \subseteqq \mathfrak{S}$ *and one of the following conditions holds, according to the rank of* $\mathfrak{U}^+$:

(1) $\mathfrak{U} = \mathfrak{S}$.

(2) $\mathfrak{U}^+$ *has a basis* σ, β, *and* $\beta^2 \neq 0$.

(3) $\mathfrak{U}^+$ *has a basis* σ, β, γ, *and* $(X\beta + Y\gamma)^2 = 0$ *for integers* X *and* Y *implies* $X \equiv Y \equiv 0 \pmod{p}$.

Proof. Since $\mathfrak{S} \subseteqq \mathfrak{U}$, $\mathfrak{U}$ is an algebra over $GF(p)$ with a unique subalgebra of dimension 1. The result follows directly from (4.1) and (5.3).

In case $p\mathfrak{R} = 0$ we have $\mathfrak{R} = \mathfrak{U}$, and thus $\mathfrak{R}$ satisfies (3) of (4.4). If $p\mathfrak{R} \neq 0$, then, by (5.2), $\mathfrak{R}^+ = \mathfrak{C}^+ + \mathfrak{U}^+$ where $\mathfrak{C}^+$ is a cyclic p-group with $|\mathfrak{C}^+| > p$, and $\mathfrak{C}^+ \cap \mathfrak{U}^+ = \mathfrak{S}^+$. The rest of the proof is devoted to showing that $(\mathfrak{R}^2)^+ \subseteqq p\mathfrak{C}^+$. This implies that the set of elements of $\mathfrak{C}^+$ form a subring $\mathfrak{C}$, and thus (3) of (4.4) holds. Let α be a generator of $\mathfrak{C}^+$. The proof that $(\mathfrak{R}^2)^+ \subseteqq p\mathfrak{C}^+$ is divided into cases depending on the location of α^2 and on the rank of $\mathfrak{U}^+$, which of course equals the rank of $\mathfrak{R}^+$.

If $\mathfrak{U}^+$ has rank 1, then $\mathfrak{C} = \mathfrak{R}$, so (1) of (4.4) holds. Suppose $\mathfrak{U}^+$ has rank 2, with basis σ, β. If $\alpha^2 \notin p\mathfrak{C}^+$, then $(\mathfrak{R}^2)^+$ has rank 2 so (4.6) applies. Thus $\alpha^2 \in p\mathfrak{C}^+$. By (5.4) $\mathfrak{U}^2 \subseteqq \mathfrak{S}$, and $\mathfrak{S}^+ \subseteqq p\mathfrak{C}^+$. Finally, $\alpha\beta \in \mathfrak{S}$ and $\beta\alpha \in \mathfrak{S}$ by the nilpotence of α.

Thus we may assume that $\mathfrak{U}^+$ has rank 3, with basis σ, β, γ. If $(\mathfrak{R}^2)^+$ has rank 1, we are done. If $(\mathfrak{R}^2)^+$ has rank 3, then (4.6) applies. Thus assume $(\mathfrak{R}^2)^+$ has rank 2. Without loss of generality we may asssume $\beta \in \mathfrak{R}^2$. To complete the proof we make use of the following remark:

5.5 *Under the above assumptions, if* $\varphi \in \mathfrak{R}^2$, $p\varphi = 0$, *and* $\varphi\beta = 0$, *then* $\varphi \in \mathfrak{S}$.

Proof. Since $(\mathfrak{R}^2)^+$ has rank 2 and $\sigma, \beta \in \mathfrak{R}^2$, it follows that $\varphi =$

$X\sigma + Y\beta$, some integers X and Y. Thus $\varphi\beta = Y\beta^2$. Since $\beta^2 \neq 0$, $Y \equiv 0 \pmod{p}$. Thus $\varphi \in \mathfrak{S}$.

We now continue the proof. Since $\beta^2 \in \mathfrak{S}$, $0 = \alpha\beta^2 = (\alpha\beta)\beta$ so by (5.5) $\alpha\beta \in \mathfrak{S}$. Dually $\beta\alpha \in \mathfrak{S}$. By (5.4) $\mathfrak{U}^2 \subseteq \mathfrak{S}$. Since $\gamma\beta \in \mathfrak{S}$, $0 = \alpha(\gamma\beta) = (\alpha\gamma)\beta$ so, by (5.5), $\alpha\gamma \in \mathfrak{S}$. Dually $\gamma\alpha \in \mathfrak{S}$. Since $\alpha\beta \in \mathfrak{S}$, $0 = \alpha(\alpha\beta) = \alpha^2\beta$. Thus $\mathfrak{R}^2\beta = 0$. Choose any $\varphi \in \mathfrak{R}^2$. Since $(\mathfrak{R}^2)^+$ has rank 2, and $\beta \in \mathfrak{R}^2$, $\mathfrak{S} \subseteq \mathfrak{R}^2$, we can write $\varphi = pX_1\alpha + X_2\beta$ for some integers X_1 and X_2. Then $0 = \varphi\beta = (pX_1\alpha + X_2\beta)\beta = X_2\beta^2$. Since $\beta^2 \neq 0$, $X_2 \equiv 0 \pmod{p}$. Thus $\varphi \in p\mathfrak{C}^+$, so $(\mathfrak{R}^2)^+$ has rank 2.

6. Examples related to circle groups.[1] Every Jacobson radical ring is a group under the circle composition

$$x \circ y = x + y + xy ,$$

and every subring [two-sided ideal] of the ring is a subgroup [normal subgroup] of the circle group. In general, however, not all subgroups under circle are subrings, and normal subgroups, which may or may not be subrings, need not be ideals. In fact, a subgroup under circle is a subring if and only if it is also a subgroup under addition. We shall consider some examples which show that one cannot tell from the structure of the circle group alone which subgroups will or will not correspond to subrings.

6.1 *A fully invariant subgroup which is not a subring.* Let $\mathfrak{R}$ be the ring generated by an element φ of characteristic 8 with $\varphi^2 = 2\varphi$. The circle group $\mathfrak{C}$ of $\mathfrak{R}$ is abelian of order 8 and type (2, 1). The fully invariant subgroup of $\mathfrak{C}$ of elements of orders 1 and 2 in $\mathfrak{C}$ consists of $0, 3\varphi, 4\varphi$, and 7φ. These elements do not form a subring of $\mathfrak{R}$.

6.2 *Elementary abelian groups.* If $\mathfrak{R}$ is a radical ring whose additive and circle groups are elementary abelian p-groups, then all the additive and circle subgroups of a given order in $\mathfrak{R}$ are indistinguishable up to automorphisms of the groups. We shall, however, give examples of such rings in which the subring structure varies substantially.

Suppose $\mathfrak{R}$ is a radical ring such that $\mathfrak{R}^+$ is an elementary abelian p-group. Then the circle group $\mathfrak{C}$ of $\mathfrak{R}$ is elementary abelian if and only if $\mathfrak{R}$ is commutative and $\varphi^p = 0$ for all $\varphi \in R$. To prove this consider $\mathfrak{C}$ as the multiplicative group of elements $1 + \varphi$ where $\varphi \in \mathfrak{R}$ and 1 is an identity adjoined to $\mathfrak{R}$. Observe that $p\varphi = 0$ implies

[1] The authors wish to thank the referee and editor for encouraging the inclusion of this section.

$(1 + \varphi)^p = 1 + \varphi^p$, all $\varphi \in \mathfrak{R}$.

A ring whose additive group is an elementary abelian p-group may be considered as an algebra over $GF(p)$. We now describe some examples of rings $\mathfrak{R}$ whose additive and circle groups are elementary abelian. We denote a basis for $\mathfrak{R}$ as an algebra over $GF(p)$ by $\{\varphi_1, \cdots, \varphi_n\}$.

(a) *Null algebra*, $\mathfrak{R} = \mathfrak{Z}_n$. Define $\varphi_i\varphi_j = 0$ for all $i, j = 1, \cdots, n$. Every subgroup (under $+$ or $\circ$) of $\mathfrak{R}$ is an ideal.

(b) *Power algebra*, $\mathfrak{R} = \mathfrak{B}_n$. Assume $n < p$. $\mathfrak{B}_n$ is the unique power algebra of dimension n over $GF(p)$. $\mathfrak{B}_n$ may be defined by $\varphi_1^k = \varphi_k$, $1 \leqq k \leqq n$, $\varphi_1^{n+1} = 0$. By Theorem 2.1, $\mathfrak{B}_n$ contains only one subring of order p^{n-1}. For $1 \leqq k \leqq n-2$, $\mathfrak{B}_n$ contains only one ideal of order p^k, although more than one subring of order p^k.

(c) *Direct sum.* $\mathfrak{R} = \mathfrak{B}_m \oplus \mathfrak{Z}_{n-m}$, where $0 < m < n$ and $m < p$.

(d) *Almost-null algebras.* Assume $1 \leqq n \leqq 3$ and $p \neq 2$. $\mathfrak{R} = \mathfrak{U}$, where $\mathfrak{U}$ is a commutative ring whose structure is given in Lemma 5.4. 3 of 4.4. $\mathfrak{U}$ is called "almost-null," and its structure is typical both of nilpotent rings which have a unique subring of order p, and of nilpotent algebras in which all subalgebras are ideals.

6.3 *Remarks on commutative radical rings.* It is easy to find examples of commutative radical rings $\mathfrak{R}$ in which not every subring is an ideal. If $\mathfrak{C}$ is the circle group of $\mathfrak{R}$, then $\mathfrak{C}$ contains normal subgroups which correspond to subrings but not ideals. If, on the other hand, we start with the abelian group $\mathfrak{C}$, then the null ring whose additive group is $\mathfrak{C}$ also has circle group $\mathfrak{C}$, and every subgroup corresponds to an ideal. Every abelian group, moreover, appears as a circle group in this way.

In studying nilpotent rings one soon notices that the fruitful group analogy is between ring product and group commutation. Under this analogy an abelian group corresponds to a null ring, the center of a group to the annihilator of a ring, the lower central series of a group to the powers of a ring, etc.

6.4 *Three special rings.* We conclude by describing three nilpotent rings $\mathfrak{R}$ of order 16, each of which has an abelian circle group of type (2, 1, 1), but which differ in several other properties.

$\mathfrak{R} = \mathfrak{A}$ is generated by elements $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, each of characteristic 2, such that $\alpha_1^2 = \alpha_2$ and $\alpha_i\alpha_j = 0$ if $i \neq 1$ or if $j \neq 1$.

$\mathfrak{R} = \mathfrak{B}$ is generated by elements $\beta_1, \beta_2, \beta_3$, such that char $\beta_1 = 4$, char $\beta_2 =$ char $\beta_3 = 2$, $\beta_1^2 = 2\beta_1$, $\beta_2^2 = \beta_3$, $\beta_2\beta_3 = \beta_3\beta_2 = 2\beta_1$, and $\beta_1\beta_2 = \beta_2\beta_1 = \beta_1\beta_3 = \beta_3\beta_1 = \beta_3^2 = 0$.

$\mathfrak{R} = \mathfrak{C}$ is generated by elements γ_1 and γ_2 of characteristic 4 such that $\gamma_1^2 = \gamma_2$, $\gamma_1\gamma_2 = \gamma_2\gamma_1 = 2\gamma_1$, and $\gamma_2^2 = 2\gamma_2$.

Invariant	Value for $\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{C}$
Exponent of $\mathfrak{R}$: least integer e with $\mathfrak{R}^e = 0$	3	4	5
Number of generators required (see (2.1))	3	2	1
Number of subrings (ideals) of order 8	7	3	1
Number of subrings of order 4	11	3	3
Number of subrings of order 2	7	3	3
Number of ideals of order 4	11	3	1
Number of ideals of order 2	7	1	1
Order of $\mathfrak{R}^2$	2	4	8
Order of $\mathfrak{R}$ modulo its annihilator	2	8	8
Additive group type	(1, 1, 1, 1)	(2, 1, 1)	(2, 2)
Order of automorphism group of $\mathfrak{R}$	192	8	4

REFERENCES

1. W. Burnside, *Theory of groups of finite order*, Cambridge, 1911.
2. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2) **36** (1933), 29-95.
3. R. Kruse, *Rings in which all subrings are ideals, I*, Canad. J. Math. **20** (1968), 862-871.
4. H. Liebeck, *The automorphism group of finite p-groups*, J. Algebra **4** (1966), 426-32.

Received May 28, 1968. This work was supported by the United States Atomic Energy Commission.

SANDIA LABORATORY, ALBUQUERQUE, NEW MEXICO
WHEATON COLLEGE, WHEATON, ILLINOIS