RINGS WITH PERIODIC ADDITIVE GROUP IN WHICH ALL SUBRINGS ARE IDEALS

Thesis by

Robert Leroy Kruse

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1964

ACKNOWLEDGEMENTS

To my advisor, Professor Richard A. Dean, without whose helpful suggestions and guidance, much patience, and many real kindnesses my work would have been impossible, I wish first to express my gratitude. To my other instructors I also wish to express my appreciation, and especially to Professor Robert P. Dilworth, whose early guidance in my thesis research and whose continuing interest in my work has been most helpful. To the Woodrow Wilson National Fellowship Foundation and to the National Science Foundation for fellowship support, and to the California Institute for the opportunity to teach during my graduate study, I am most grateful.

ABSTRACT

A ring in which every subring is a two sided ideal is called a v-ring. This dissertation is a classification of all v-rings with periodic additive group. It is first shown that a ring is a v-ring with periodic additive group if and only if it is the restricted ring direct sum of v-rings whose additive groups are p-groups for different primes p. Such rings are called p-v-rings. It is next shown that a p-v-ring must be nil, or be isomorphic to the ring of rational integers mod p^n for some $n > 1$, or be isomorphic to the direct sum of the prime field of p elements and a nil p-v-ring.

The classification of nil p-v-rings constitutes the major part of this dissertation. Nil p-v-rings containing elements of unbounded additive order are first characterised. Redei has shown that for any element x of a nil p-v-ring either (I) x^2 is a natural multiple of x or (II) px^2 is a natural multiple of x although x^2 is not a natural multiple of x. Because of this result it is possible to study a nil p-v-ring possessing a bound on the additive orders of its elements by decomposing the ring into an additive group direct sum of cyclic groups. It is shown that aside from elements in the annihilator of the ring, there is a decomposition of the ring with at most two generators of type (I) and three of type (II). The possible defining relations for these nil p-v-rings are enumerated.

I. INTRODUCTION

A ring in which every subring is an ideal will be called a v-ring (from the German Vollidealring). The problem of determining all v-rings--described by F. Szász [1] as "ein schweres und bisher noch ungelöstes Problem der Algebra"--was first considered by L. Redei [2] who exhibited all v-rings generated by a single element as the homomorphs of the ring of polynomials with constant term zero over the rational integers determined by certain products of certain specified ideals. Further work with v-rings has been done by F. Szász and P. A. Freĭdman. Szász's work is with special cases which will not be discussed here. Freĭdman's work is directed toward a somewhat different problem but leads in particular to a determination of semi-simple v-rings and v-rings with torsion free additive group. The following are some of Freĭdman's relevant results [3, Theorems 8, 9, 10]: The radical of a v-ring is the set of nilpotent elements of the ring. A ring is a semi-simple v-ring if and only if it is isomorphic to a direct sum $(\mathfrak{Z}/M) \oplus N\mathfrak{Z}$ where $\mathfrak{Z}$ is the ring of rational integers and M is a square free integer dividing N (possibly $M = 1$ or $N = 0$). A v-ring with torsion free additive group is null or is a subring of the ring of rational integers.

V-rings with periodic additive group will be characterized here. Except for a few well known theorems all needed results will be proved here in complete detail. By Theorem 1 the problem is reduced to the consideration of rings whose additive groups are p-groups (p-rings), and by Theorem 2 to the consideration of nil p-rings. Theorem 3 isolates the v-rings among the nil p-rings containing elements of unbounded characteristic. The remainder of the dissertation is a classification of those v-rings which are nil p-rings containing only elements of bounded characteristic.

It should first be noted that a necessary and sufficient condition for a ring to be a v-ring is that every subring generated by a single element be an ideal, and that subrings and homomorphs of v-rings are again v-rings.

Natural examples of v-rings are the null rings and the ring of rational integers. It is not possible for a v-ring with periodic additive group to differ too much from these examples. Theorem 2 shows that the non-nil part of a v-ring with periodic additive group can be nothing more than a homomorph of the rational integers. It will be shown that a v-ring which is a nil p-ring must be the direct sum of a null ring and one of several very special rings listed explicitly in Theorems 4 - 9. These special rings have the property that when (at most) one subring generated by a single element is removed, then the p^{th} multiple of every product in the ring is zero.

II. NOTATION AND DEFINITIONS

A ring will be called a v-ring if every subring is an ideal. The term "ideal" will always mean two sided ideal. A ring will be called a p-ring if its additive group is a p-group, and a ring which is both a v-ring and a p-ring will be called a p-v-ring.

If $\mathcal{A}$ is a subset of elements of a ring let $\langle \mathcal{A} \rangle$ denote the subring generated by $\mathcal{A}$, and $\{\mathcal{A}\}$ the additive subgroup generated by $\mathcal{A}$. $\mathcal{A} \oplus \mathcal{B}$ or $\sum \oplus \mathcal{A}_i$ will denote a restricted ring direct sum, while $\mathcal{A} \dotplus \mathcal{B}$ or $\sum \dotplus \mathcal{A}_i$ will denote a restricted additive group direct sum.

An element y will be said to have exponent $r = \exp y$ if $y^r = 0$, $y^{r-1} \neq 0$. The characteristic $n = \text{char}\ \mathcal{A}$ of a set of elements $\mathcal{A}$ is the smallest positive integer n for which $nx = 0$ for all $x \in \mathcal{A}$ if such an integer exists. Otherwise $\text{char}\ \mathcal{A} = 0$. If $\mathcal{A} = \{x\}$ we write char x = char $\mathcal{A}$.

Script letters $\mathcal{A}$, $\mathcal{R}$, ... will denote rings, groups, or sets. $\mathfrak{Z}$ will denote the ring of rational integers. Capital letters A, B, C, ... will denote rational integers used as coefficients; A, ..., Q structure constants determined by the ring; R, S, T coefficients which may be arbitrarily specified; U, V, W, X unknowns in equations. Small letters a through d, g through n will be integers used as exponents; p and q will be primes; e, f, and u through z will be elements of a ring.

III. REDUCTION TO NIL p-RINGS

Theorem 1. A ring $\mathcal{R}$ is a v-ring with periodic additive group if and only if $\mathcal{R}$ is the restricted ring direct sum of p-v-rings $\mathcal{R}_p$ for different primes p.

Proof: If $\mathcal{R}$ is any ring with periodic additive group it is well known that $\mathcal{R}$ is the restricted group direct sum of its p-components $\mathcal{R}_p$. If $x \in \mathcal{R}_p$ has characteristic p^n, then $p^n xy = p^n yx = 0$ for all $y \in \mathcal{R}$ so $\mathcal{R}_p$ is an ideal and thus $\mathcal{R}$ is the restricted ring direct sum of the $\mathcal{R}_p$. Since subrings of v-rings are v-rings, if $\mathcal{R}$ is a v-ring then the $\mathcal{R}_p$ are p-v-rings.

Now assume that $\mathcal{R}$ is the restricted ring direct sum of p-v-rings for different primes p. It will be sufficient to show that each subring $\langle y \rangle$ generated by a single element y is an ideal. Let $y = \sum_{p \in \mathcal{P}} x_p$ where $x_p \in \mathcal{R}_p$ and $\mathcal{P}$ is a finite set of primes. Let char $x_p = n_p$. If $q \in \mathcal{P}$ let M be a solution to the congruences $M \equiv 1 \pmod{n_q}$, $M \equiv 0 \pmod{n_p}$ if $p \in \mathcal{P}$ $p \neq q$. Since each n_p is a power of p such a solution exists by the Chinese Remainder Theorem. Then $My = x_q$ so $\langle y \rangle = \bigcup_{p \in \mathcal{P}} \langle x_p \rangle$ is the union of ideals of direct summands and so is itself an ideal in $\mathcal{R}$.

We shall need the following classical result:

Lemma 1 (Koethe and Dickson): If the quotient ring $\mathcal{R}/\mathcal{N}$, where $\mathcal{N}$ is a nil ideal, contains an idempotent, then $\mathcal{R}$ contains an idempotent.

Proof: If x is in an idempotent coset of the quotient ring let $x' = x^2 - x$ and let $n(x) = \exp x'$. Choose e in the idempotent coset so that $n(e)$ is minimal. We show that $e' = 0$, so that e is an idempotent. For consider $f = e + e' - 2ee'$. f is in the same coset as e, and $f' = f^2 - f = 4e'^3 - 3e'^2$ would have exponent strictly less than $n(e)$ unless $e' = 0$.

The following lemma is due to P. A. Freĭdman. The proof is new.

Lemma 2. The radical of a p-v-ring is the set of nilpotent elements of the ring. A semi-simple p-v-ring is isomorphic to the field of p elements.

Proof: Let $\mathcal{R}$ be a p-v-ring and $\mathcal{N}$ the set of nilpotent elements of the ring. We first show that $\mathcal{N}$ is an ideal. If $x \in \mathcal{N}$, $y \in \mathcal{R}$ then $xy, yx \in \langle x \rangle \subseteq \mathcal{N}$. If $x, y \in \mathcal{N}$ choose m, n so that $x^m = y^n = 0$. Then each term of $(x-y)^{m+n-1}$ contains at least m x's or n y's. Since $xy^k \in \langle x \rangle$, $x^k y \in \langle y \rangle$ it follows that $(x-y)^{m+n-1} = 0$, so $x - y \in \mathcal{N}$ and $\mathcal{N}$ is an ideal.

Now suppose $\mathcal{R}$ is a p-v-ring with no nilpotent elements. If $x \in \mathcal{R}$ let char $x = p^n$. Then $(px)^n = 0$, so $n = 0, 1$. Suppose $x \neq 0$. Since $\langle x^2 \rangle$ is an ideal in $\langle x \rangle$, it follows that $x^3 = xx^2 = A_2x^2 + A_4x^4 + \ldots + A_kx^k$ for some polynomial, $0 \leq A_j < p$. We show that for some s $x^s \in \langle x^{s+1} \rangle$. If $A_2 = 0$ then $s = 3$. If $A_2 \neq 0$ choose B so that $BA_2 \equiv 1 \pmod{p}$. Then $x^2 = Bx^3 + \ldots$ so $s = 2$. Let $x^s = B_1x^{s+1} + \ldots + B_mx^{s+m}$. To obtain an idempotent one could formally divide both sides by x^s. We shall in fact show that $e = (B_1x + \dots + B_mx^m)^s$ is a non-zero idempotent. Since $ex^{s^2} = x^{s^2} \neq 0$ we have $e \neq 0$. Write $e = B_1^s x^s + f(x)x^s$ where $f(x)$ is a polynomial in x. Then $(B_1x + \dots + B_mx^m)^{s+1} = (B_1^s x^s + f(x)x^s)(B_1x + \dots + B_mx^m) = B_1^s x^s + f(x)x^s = e$. By induction $e^2 = e$.

If $\mathcal{R}$ contained another idempotent f, then either $\langle e\rangle \cap \langle f\rangle \neq 0$, from which it follows that $\langle e\rangle = \langle f\rangle$ and $e = f$, or else $\langle e\rangle \cap \langle f\rangle = 0$, and since $e + f$ is the only idempotent in $\langle e + f\rangle$ it follows that $e = e(e + f) = e + f$, so $f = 0$. Thus $\mathcal{R}$ is isomorphic to the field of p elements, and the Lemma is proved.

<u>Theorem 2</u>. A ring is a p-v-ring if and only if it is isomorphic to a ring $\mathcal{R}$ satisfying one of the following conditions:

(1) $\mathcal{R}$ is a nil p-v-ring.

(2) $\mathcal{R} = \mathfrak{F} \oplus \mathcal{N}$ where $\mathfrak{F}$ is the field of p elements and $\mathcal{N}$ is a nil p-v-ring.

(3) $\mathcal{R} = \mathfrak{Z}/\langle p^n\rangle$ where $\mathfrak{Z}$ is the ring of rational integers and $n > 1$.

<u>Proof</u>: Rings satisfying (1) and (3) are evidently p-v-rings. To show that a ring $\mathcal{R}$ satisfying (2) is a p-v-ring consider the subring $\langle u+x\rangle$ where $u \in \mathfrak{F}$, $x \in \mathcal{N}$. Let $r = \exp x$. Then $(u+x)^r = u^r$ and $\langle u\rangle = \langle u^r\rangle$ so $\langle u+x\rangle = \langle u\rangle \cup \langle x\rangle$ is the join of ideals of direct summands and so is itself an ideal in $\mathcal{R}$.

Now assume that $\mathcal{R}$ is a p-v-ring which is not nil. Let

$\mathcal{M}$ be the radical of $\mathcal{R}$. By Lemma 2 $\mathcal{R}/\mathcal{M}$ contains an idempotent, and then by Lemma 1 $\mathcal{R}$ contains an idempotent e. The Pierce decomposition gives us $\mathcal{R} = \langle e \rangle + \mathcal{N}$ where $\mathcal{N}$ is the two sided annihilator of e and for any y, $y = (ey+ye-eye) + (y-ey-ye+eye)$. If $\mathcal{N}$ were not nil then as above it would contain an idempotent. But then $\mathcal{R}/\mathcal{M}$ would not satisfy Lemma 2.

Let char $e = p^n$. If $n = 1$ then $\mathcal{R}$ satisfies condition (2). If $n > 1$ consider the ideal $\langle pe+x \rangle$ where $x \in \mathcal{N}$. $e(pe+x) = pe = V_1(pe+x) + V_2(p^2e+x^2) + \ldots + V_t(p^te+x^t)$ so $pe = V_1pe + V_2p^2e + \ldots + V_tp^te$ so $V_1 \not\equiv 0 \pmod{p}$. Also $V_1x + V_2x^2 + \ldots + V_tx^t = 0$ so $x \in \langle x^2 \rangle$ and since x is nilpotent we have $x = 0$. Thus $\mathcal{N} = 0$ and so (3) holds.

IV. NIL p-v-RINGS OF UNBOUNDED CHARACTERISTIC

<u>Lemma 3</u>: If y is an element of a nil p-v-ring then $y^3 \in \{y^2\}$.

<u>Proof</u>: Let k be the minimal positive integer such that $y^k = My^{k-1}$ for some M. Let $\exp y = r$. Then $y^{r-k}y^k = 0 = My^{r-1}$ so p divides M. Since $\langle y^2\rangle$ is an ideal in $\langle y\rangle$ we have $y^3 = yy^2 = A_2y^2 + A_4y^4 + \ldots + A_{r-1}y^{r-1}$. If $k \leq 3$ there is nothing to prove. If $k \geq 4$ then $y^{k-4}y^3 = A_2y^{k-2} + A_4y^k + \ldots = A_2y^{k-2} + (A_4M + A_6M^3 + \ldots)y^{k-1}$. Since p divides M there is a B such that $B(1 - A_4M - \ldots) \equiv 1 \pmod{\text{char } y}$. But then $y^{k-1} = BA_2y^{k-2}$, contradicting the minimality of k.

<u>Corollary</u>: A ring is a nil p-v-ring only if for all x, y in the ring there are U, V, U', V' such that $xy = Ux + Vx^2 = U'y + V'y^2$.

<u>Lemma 4</u>: Let $\mathcal{R}$ be a nil p-v-ring of unbounded characteristic. If $x \in \mathcal{R}$ then $px^2 = 0$. If $x, y \in \mathcal{R}$ then $xy \in \{x^2\} \cap \{y^2\}$.

<u>Proof</u>: If $x \in \mathcal{R}$ then $x(px) = Upx + Vp^2x^2$ so $(1-pV)px^2 = Upx$ so $px^2 \in \{x\}$. Let $\text{char } x = p^r$ and choose $z \in \mathcal{R}$ so that $\text{char } z = p^{2r}$. If $\{x\} \cap \{z\} = 0$ then $x(px + p^rz) = px^2 = U(px + p^rz) + Vp^2x^2$ so p^r divides U so $px^2 = Vp^2x^2$ and so $px^2 = 0$. On the other hand suppose $p^{r+j}z = Ap^jx$ for some j, $A \not\equiv 0 \pmod p$. Then $x(Apx - p^{r+1}z) = Apx^2 = U(Apx - p^{r+1}z) + V(A^2p^2x^2) = V(A^2p^2x^2)$ so again $px^2 = 0$.

Now assume that $x, y \in \mathcal{R}$. Let $\text{char } x = p^r$, $\text{char } y = p^s$, and $t > \max(r,s)$. Choose $z \in \mathcal{R}$ so that $\text{char } z = p^{2t}$. First suppose $\{z\} \cap \langle x\rangle = 0$. Then $(x + p^tz)y = xy = U(x + p^tz) + Vx^2$ so p^t divides U and so $xy \in \{x^2\}$. Next suppose $p^{2t+j-r}z = Ap^jx$, $A \not\equiv 0\ (p)$. Then $(Ax - p^{2t-r}z)y = Axy = V(A^2x^2)$ so again $xy \in \{x^2\}$. Finally suppose $p^{2t-1}z = Ap^{r-1}x + Bx^2$, $x^2 \notin \{x\}$. If $A \equiv 0$ (p) then $(x+p^t z)y = xy = (UB+V)x^2$ so $xy \in \{x^2\}$. If $A \not\equiv 0$ (p) then $(Ax-p^{2t-r}z)y = Axy = (-UB+VA^2)x^2$ so $xy \in \{x^2\}$. Thus in every case we have shown that $xy \in \{x^2\}$. Similarly it can be shown that $xy \in \{y^2\}$.

The following lemma is well known.

Lemma 5: If $p \neq 2$ and $P(S,T)$ is a quadratic polynomial in two variables which mod p is not constant in either variable, then for some integers S, T we have $P(S,T) \equiv 0 \pmod p$.

Proof: We may assume that $P(S,T)$ is in standard form $P(S,T) = AS^a + BT^b + C$. If $a = 1$ or $b = 1$ the result is immediate. Otherwise write $P(S,T) = 0$ as $AS^2 = -BT^2 - C$. The left hand side takes on $(p+1)/2$ values--obtained from the $(p-1)/2$ quadratic residues and zero--while the right hand side also takes on $(p+1)/2$ values, so there is one in common.

Theorem 3: A p-ring of unbounded characteristic is a nil p-v-ring if and only if it is isomorphic to a ring $\mathcal{R}$ satisfying one of the following conditions, where $\mathcal{N}$ is a p-ring of unbounded characteristic which annihilates $\mathcal{R}$:

(1) $\mathcal{R} = \mathcal{N}$.

(2) $\mathcal{R} = \langle x \rangle \cup \mathcal{N}$, $px, x^2 \in \mathcal{N}$, char $x^2 = p$.

(3) $\mathcal{R} = \langle x,y \rangle \cup \mathcal{N}$, $px, py, x^2 \in \mathcal{N}$. char $x^2 = p$, $y^2 = Ax^2$, $A \not\equiv 0 \pmod p$, $xy = Fx^2$, $yx = F'x^2$, $T^2+T(F+F')+A \not\equiv 0 \pmod p$ for any integer T.

Proof: Rings satisfying (1) are obviously v-rings. We show that rings satisfying (3) are v-rings. A trivial modification of the argument shows that rings satisfying (2) are v-rings. It is enough to show that each subring $\mathcal{S} = \langle Sx+Ty+u \rangle$, $u \in \mathcal{N}$, is an ideal. If p divides S and p divides T then $Sx+Ty+u \in \mathcal{N}$ and thus $\mathcal{S}$ is an ideal. Otherwise $x^2 \in \mathcal{S}$ since $(Sx+Ty+u)^2 = (S^2+ST(F+F')+T^2A)x^2$ which is not zero since $T^2+T(F+F')+A$ is never zero. But all products are in $\{x^2\}$ so $\mathcal{S}$ is an ideal.

Conversely suppose $\mathcal{R}$ is a nil p-v-ring of unbounded characteristic. Let $\mathcal{N}$ be the two sided annihilator of $\mathcal{R}$. By Lemma 4 if $w \in \mathcal{R}$ then $pw \in \mathcal{N}$, and $w \in \mathcal{N}$ if and only if $w^2 = 0$. If $\mathcal{R} = \mathcal{N}$ then (1) holds. Otherwise there is an $x \in \mathcal{R}$, $x \notin \mathcal{N}$ (so char $x^2 = p$). If $\mathcal{R} = \langle x \rangle \cup \mathcal{N}$ then (2) holds, so assume there is some $y \in \mathcal{R}$, $y \notin \langle x \rangle \cup \mathcal{N}$. If $xy \neq 0$ or $yx \neq 0$ then since $xy, yx \in \{x^2\} \cap \{y^2\}$ we have $y^2 = Ax^2$ for some $A \not\equiv 0$ (mod p). If $xy = yx = 0$ then by Lemma 4 $x(x+y) = x^2 \in \{(x+y)^2\} = \{x^2+y^2\}$ so $y^2 = Ax^2$. Let $xy = Fx^2$, $yx = F'x^2$. If for some T $T^2+T(F+F')+A \equiv 0$ (mod p) then for that T $(y+Tx)^2 = 0$, so $y = (-Tx) + (y+Tx)$ is in $\langle x \rangle \cup \mathcal{N}$, a contradiction.

If $\mathcal{R} = \langle x,y \rangle \cup \mathcal{N}$ then (3) holds. Suppose there were some $z \in \mathcal{R}$, $z \notin \langle x,y \rangle \cup \mathcal{N}$. As above $z^2 = Bx^2$, $B \not\equiv 0$ (mod p), $xz + zx = (H+H')x^2$, $yz + zy = (K+K')x^2$. By Lemma 5 (or directly if $p = 2$) for suitable S and T $S^2+T^2A+S(H+H')+T(K+K')+ST(F+F')+B \equiv 0$ (mod p). For this S and T it follows that $(z+Sx+Ty)^2 = 0$, so $z \in \langle x,y \rangle \cup \mathcal{N}$.

V. NIL p-v-RINGS OF BOUNDED CHARACTERISTIC

The determination of nil p-v-rings of bounded characteristic will proceed as follows. It is first shown by Theorem 4 that any element of a nil p-v-ring has some multiple which generates the same additive subgroup and which satisfies one of two specified conditions. Elements satisfying these conditions will be called elements of types I and II. A p-ring of bounded characteristic may decompose as an additive group direct sum of finite cyclic subgroups (see, e.g. [4], p. 17). The generators of the cyclic direct summands can be taken to be of types I and II, and rings which have decompositions with only a finite number of type II generators are first considered. For convenience in the proofs the number of type II generators is assumed to be minimal, but the proofs provide a proceedure for obtaining a decomposition with the minimal number, starting with any finite number. Lemma 7 shows that rings with more than two type I generators with square not zero are not v-rings. The number of type I generators with square not zero is assumed to be minimal. By Theorems 5, 6, 7, and 8 nil p-v-rings of bounded characteristic having 0, 1, 2, and 3 generators of type II are in turn enumerated. Theorem 9 then shows that there are no nil p-v-rings whose minimal decompositions involve more than three type II generators, and if a nil p-v-ring has an infinite number of type II generators Theorem 9 outlines a procedure for obtaining a decomposition with only a finite number.

The following theorem is due to L. Redei [2]. The proof given here is new.

<u>Theorem 4</u>. A ring $\langle y\rangle$ generated by one element will be a nil p-v-ring if and only if there is some $x \in \{y\}$, $\langle x\rangle = \langle y\rangle$, satisfying one of the following conditions:

I. $x^2 = p^m x$, $p^{m+n}x = 0$ for suitable integers $m > 0$, $n \geq 0$.

II. $px^2 = p^m x$, $p^{m+n}x = 0$ for suitable integers $m > 0$, $n \geq 0$, $x^2 \notin \{x\}$. If $m = 1$ then $n = 0$ and $x^3 = 0$. If $m > 1$ then $x^3 = p^{2m-2}x$.

<u>Proof</u>: Suppose $\langle y\rangle$ is a nil p-v-ring. $\langle py\rangle$ is an ideal, so $py^2 = Upy + Vp^2y^2$ by the corollary to Lemma 3, and thus $p(1-pV)y^2 = pUy$. Let M be the minimal positive integer such that $My^2 = Ny$ for some N. Since p^2 does not divide $p(1-pV)$ either $M = 1$ or $M = p$. Let $N = Qp^m$ where p does not divide Q, and let S be a solution to the congruence $QS \equiv 1$ (mod char y). Let $x = Sy$. Then either $x^2 = p^m x$ or $px^2 = p^m x$. Note that $m > 0$, for $m = 0$ and x nilpotent implies $x = 0$. Let char x = p^{m+n}. If $x^2 = p^m x$ then condition I holds, so assume $px^2 = p^m x$, $x^2 \notin \{x\}$.

Suppose $m = 1$. Let r = exp x. Then $0 = px^r = (px^2)x^{r-2} = px^{r-1} = \ldots = px$ so $n = 0$. Since $x^3 \in \{x^2\}$ and $px^2 = 0$ it follows that $x^3 = 0$. Thus II holds.

Suppose $m > 1$. Let r = exp x, and let $x^3 = Kp^t x^2$. Multiplying by x^{r-3} shows that $t > 0$, so $x^3 = Kp^{m+t-1}x$. Then $x(x^2 - p^{m-1}x) = x^3 - p^{2m-2}x = U(x^2 - p^{m-1}x) + V(x^2 - p^{m-1}x)$. But $(x^2 - p^{m-1}x)^2 = Kp^{2m+t-2}x - Kp^{2m+t-2}x - p^{3m-3}x + p^{3m-3}x = 0$ and since

$x^2 \notin \{x\}$ it follows that p divides U, and $p(x^2 - p^{m-1}x) = 0$, so $x^3 - p^{2m-2}x = 0$, and thus condition II holds.

To show conversely that rings satisfying I and II are v-rings it suffices to show that each subring $\langle Ap^a x + Bx^2 \rangle$ generated by one element is an ideal, where p does not divide A and $0 \leq B < p$. Choose C so that $AC \equiv 1$ (mod char x).

I. $x(Ap^a x+Bx^2) = Ap^{m+a}x + Bp^m x^2 = p^m(Ap^a x+Bx^2)$.

II, $m = 1$. If $a > 0$ then $x(Ap^a x+Bx^2) = 0$. If $a = 0$ then $x(Ap^a x + Bx^2) = Ax^2 = C(Ax+Bx^2)^2$.

II, $m > 1$. If $a > 0$ then $x(Ap^a x+Bx^2) = p^{m-1}(Ap^a x+Bx^2)$. If $a = 0$ then $x(Ax+Bx^2) = Ax^2 + Bp^{2m-2}x = C(Ax+Bx^2)^2 - BCp^{2m-2}(Ax+Bx^2)$.

<u>Corollary</u>. If x and y are elements of a nil p-v-ring then $p(xy) \in \{x\} \cap \{y\}$.

Some special notation and several special techniques will be needed for the calculations to follow.

From now on whenever the symbol $\{\mathfrak{a}\}$ or $\langle \mathfrak{a} \rangle$ is used it will be assumed that $\{\mathfrak{a}\}$ is the restricted direct sum of the cyclic subgroups generated by the elements of $\mathfrak{a}$.

Let x and y be group direct sum generators, $x \neq y$. Since $\{x\} \cap \{y\} = 0$, by the corollary to Theorem 4 we have $p(xy) = p(yx) = 0$. The elements of characteristic p in a p-ring together with 0 form an algebra over the field of p elements. If u is of type I it is evident that $p^{a+b-1}u$ is a basis for the elements of characteristic p in $\langle u \rangle$, where $u^2 = p^a u$ and $p^{a+b}u = 0$. If x is of type II it is easy to show that $x^2 - p^{j-1}x$ and

$p^{j+k-1}x$ constitute a basis, where $px^2 = p^j x$ and $p^{j+k}x = 0$. If $k = 0$ we shall often use the alternative basis x^2, $p^{j-1}x$. Since products of distinct group direct sum generators are in this algebra, almost all calculations will be done in the field of p elements, and all relations among coefficients are to be interpreted as congruences mod p unless stated otherwise.

In what follows, in order to determine relations among the generators, certain subrings, say $\langle y \rangle$, will be considered. By the corollary to Lemma 3 the statement $xy \in \langle y \rangle$ is equivalent to showing that there are integers U, V such that $xy = Uy + Vy^2$.

Another standard technique will be to replace a type II generator x by a type I generator of the form x+Ty. When this is done it must always be that char y $\leq$ char x (and it will always be assumed that $\{x\} \cap \{y\} = 0$) so that $\{x+Ty\} \cap \{y\} = 0$.

Henceforth the symbols u, v, w will denote group direct sum generators of type I, and x, y, z group direct sum generators of type II. The following relations will hold:

$u^2 = p^a u,\ p^{a+b}u = 0, \quad v^2 = p^c v,\ p^{c+d}v = 0, \quad w^2 = p^g w,\ p^{g+h}w = 0$

$px^2 = p^j x,\ p^{j+k}x = 0, \quad py^2 = p^m y,\ p^{m+n}y = 0, \quad pz^2 = p^r z,\ p^{r+s}z = 0.$

The generators are named so that $a \geq c \geq g$, $j \geq m \geq r$, and if $a = c$ then $b \geq d$, and similarly for all pairs selected from a, c, g or from j, m, r. This leads to a natural division of the calculations: one case is, say, $a + b > c$, the other $a = c$, $b=d=0$.

The results to follow are stated in "if and only if" terms, but the proofs are given in only one direction. The converse proofs follow immediately from Theorem 10.

VI. NIL p-v-RINGS WITH NO TYPE II GENERATORS

Lemma 6. The ring <u,v> is a nil p-v-ring if and only if $d = 0$ or $a > c$, $d = 1$.

Proof: Suppose that $d > 1$. Then $v(u + pv) = p^{c+1}v = U(u + pv) + V(p^a u + p^{c+2}v)$ for suitable U, V. Then p^a divides U while p^{c+1} does not divide U and so $c \geq a$. By assumption $a \geq c$ so $a = c$. Then $b \geq d > 1$. $v(pu + pv) = p^{c+1}v = U(pu + pv) + V(p^{c+2}u + p^{c+2}v)$. U and V must be chosen to make $(Up + Vp^{c+2})u = 0$. But then $(Up + Vp^{c+2})v = 0$, contradicting $d > 1$. Suppose now that $d = 1$ and $a = c$. Then $b \geq d = 1$. $v(u + v) = p^c v = U(u + v) + V(p^c u + p^c v)$. U and V must be chosen to make $(U + Vp^c)u = 0$. But then $(U + Vp^c)v=0$, contradicting $d = 1$.

Lemma 7: A ring <u,v,w> is a nil p-v-ring if and only if one of the following conditions holds:

(1) $d = h = 0$.

(2) $d = 1$, $h = 0$, $a > c$.

(3) $d = 0$, $h = 1$, $c > g$.

Proof: Since Lemma 6 must hold for each of the subrings <u,v>, <u,w>, and <v,w> we may assume that $a > c > g$ and $d = h = 1$. But then $w(u + v + w) = p^g w = U(u + v + w) + V(p^a u + p^c v + p^g w)$. Since $\{u\} \cap \{v,w\} = 0$ it follows that p^a divides U so $p^g w = V(p^c v + p^g w)$. But $p^c v \notin \{w\}$ so p divides V and so $p^g w = 0$, a contradiction.

Theorem 5. A nil p-v-ring generated with additive group direct sum by elements of type I must be isomorphic to a ring $\mathcal{R}$ satisfying one of the following conditions, where $\mathcal{N}$ is a null p-ring and $u^2 = p^a u$, $p^{a+b} u = 0$, $v^2 = p^c v$, $p^{c+d} v = 0$:

(1) $\mathcal{R} = \mathcal{N}$.

(2) $\mathcal{R} = \langle u \rangle \oplus \mathcal{N}$. If $b > 1$ then char $\mathcal{N} \leq p^a$.

(3) $\mathcal{R} = \langle u \rangle \oplus \langle v \rangle \oplus \mathcal{N}$, $a > c$, $b > 0$, $d = 1$, and char $\mathcal{N} \leq p^a$.

Proof: This follows directly from Lemmas 6 and 7.

VII. NIL p-v-RINGS WITH ONE TYPE II GENERATOR

Throughout this section we shall let $ux = Fp^{a+b-1}u$ and $xu = F'p^{a+b-1}u$, where $0 \le F, F' < p$. If $F \ne 0$ or $F' \ne 0$ then $\langle u \rangle \cap \langle x \rangle \ne 0$. Because the elements of characteristic p form an algebra it follows that $\langle u \rangle \cap \langle x \rangle$ is generated by $p^{a+b-1}u = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$ for some A, B. Then $A \ne 0$, since otherwise $\{u\} \cap \{x\} \ne 0$.

In considering rings containing generators of both types I and II it will become apparent that dividing the calculations into two cases is advantageous. If the generators are called u and x the cases are $a \ge j$ and $j > a$. This leads to the grouping of Lemmas 8 and 9, Lemmas 11, 12, 13, and Lemmas 14, 15.

Lemma 8: Assume that $a \ge j$. Then $\langle u,x \rangle$ is a nil p-v-ring if and only if $k = 0$ and one of the following conditions holds:

(1) $ux = xu = 0$.

(2) $a + b > j$, $x^2 = Ap^{a+b-1}u$, $A \ne 0$, $ux = Fp^{a+b-1}u$, $xu = F'p^{a+b-1}u$.

(3) $a = j$, $b = 0$, $p^{a-1}u = Ax^2 + Bp^{j-1}x$, $A \ne 0$, $ux = Fp^{a-1}u$, $xu = F'p^{a-1}u$, $B + A(F + F') = 0$.

Proof: Suppose that $k > 0$. $x(p^k x+u) = p^{j+k-1}x + F'p^{a+b-1}u = U(p^k x+u) + V(p^k x+u)^2 = U'(p^{j+k-1}x + p^{j-1}u) + Vp^a u$, since p^{j+k-1} divides the coefficient of x in the left side and in the V term, so p^{j-1} exactly divides U. In fact $U' \equiv 1 \pmod p$. From the equation and from $a \ge j$ it follows that $a = j$, $b = 0$, and $F' = 1$. Similarly $F = 1$. Then $p^{a-1}u = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$, $A \ne 0$.
Then $u(Ax-u) = Ap^{a-1}u = U(Ax-u) + V(Ax-u)^2 = U'(Ap^{j-1}x - p^{a-1}u) +$

$U''Ap^{j+k-1}x + VA(Ax^2-2p^{a-1}u)$ where $U = U'p^{j-1} + U''p^{j+k-1}$. Since the left member is in $\langle u\rangle$ the right member must be also, and so $U' = -AV$, $U'' = BV$. Then $Ap^{a-1}u = VA(1-2+1)p^{a-1}u = 0$, a contradiction. Thus $k = 0$.

We may assume $ux \neq 0$ or $xu \neq 0$ or else (1) holds. To be definite assume $ux \neq 0$ (if $xu \neq 0$ and $ux = 0$ reverse all products in what follows). Then $\langle u\rangle \cap \langle x\rangle \neq 0$ so $p^{a+b-1}u = Ax^2 + Bp^{j-1}x$ for some $A \neq 0$, B. If $a + b > j$ then (2) holds or else $B \neq 0$. But $B \neq 0$ implies $u(p^{a+b-j}u-Bx) = -BFp^{a+b-1}u = U(p^{a+b-1}u - Bp^{j-1}x) + VB^2x^2$ so, for some X, $V = AX$, $U = -B^2X$, so $-BFp^{a+b-1}u = X(B^2-B^2)u = 0$, a contradiction. Thus if $a + b > j$ then (2) holds. Assume that $a = j$, $b = 0$. If $B + A(F+F') \neq 0$ let $T[B+A(F+F')] = -1$. Then $u(x+Tu) = Fp^{a-1}u = U(p^{j-1}x+Tp^{a-1}u) + V(x^2+T(F+F')p^{a-1}u)$. Then $V = AX$, $U = BX$ so $Fp^{a-1}u = X(1+T[B+A(F+F')])p^{a-1}u = 0$, a contradiction. Thus (3) holds.

<u>Lemma 9</u>: Assume that $j > a$. Then $\langle u,x\rangle$ is a nil p-v-ring if and only if one of the following conditions holds:

(1) $b = 0$, $ux = xu = 0$.

(2) $b = 1$, $p^a u = A(x^2-p^{j-1}x) + Bp^{j+k-1}x$, $A \neq 0$, $ux = Fp^a u$, $xu = F'p^a u$, and $1 + T[A(F+F')+(Bp^k-A)p^{j-a-1}] + T^2A$ is never 0.

(3) $b = 2$, $j = a+1$, $k = 0$, $p^{a+1}u = Ax^2$, $A \neq 0$, ux, $xu \in \{p^{a+1}u\}$.

<u>Proof</u>: Suppose first that $b = 0$. Then $(u+px)x = Fp^{a-1}u + p^jx \in \langle u+px\rangle$ and $p^{j-1}(u+px) = p^jx \in \langle u+px\rangle$ so $Fp^{a-1}u \in \langle u+px\rangle$. But $p(Fp^{a-1}u) = 0$ and since $(u+px)^2 = p^{j+1}x = p^j(u+px)$ the only elements

of characteristic p in <u+px> are multiples of $p^{j+k-2}u + p^{j+k-1}x$, so $F = 0$. Similarly $F' = 0$, and so (1) holds.

Now assume that $b > 0$. $\langle u\rangle \cap \langle x\rangle \neq 0$ since if that were so then $x(u+x) = x^2 = U(u+x) + V(p^a u + x^2)$, which cannot be solved for U and V. If $j+k > a+1$ then Lemma 6 on $\langle px,u\rangle$ shows that $b = 1$.

If $b = 1$ let $p^a u = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$, $A \neq 0$. Since

$$(x+Tu)^2 = [1+T(F+F'+T)A]x^2 + [T(F+F'+T)(Bp^k - A)]p^{j-1}x$$
$$p^{j-1}(x+Tu) = [TAp^{j-a-1}]x^2 + [1+Tp^{j-a-1}(Bp^k - A)]p^{j-1}x$$

it follows that the generator x may be replaced by the type I generator x+Tu if the determinant formed by the four coefficients is ever 0. Thus (2) holds.

Finally suppose $b > 1$. We have shown that $j = a+1$, $k = 0$. Let $p^{a+b-1}u = Ax^2 + Bp^{j-1}x$, $A \neq 0$. Consider $\langle u,x\rangle/\langle p^{a+b-1}u\rangle$. In the quotient ring $x^2 \equiv -A^{-1}Bp^{j-1}x$ so $\langle \bar{x}\rangle$ is of type I. If $B \neq 0$ then Lemma 6 cannot hold for this quotient ring. Thus $B = 0$. Then $u(pu+x) = (p^{a+1} + Fp^{a+b-1})u = Up^{a+2}u + V(p^{a+2} + A^{-1}p^{a+b-1})u$ shows that $b = 2$, and so (3) holds.

<u>Lemma 10</u>: Either $\langle u\rangle \cap \langle x\rangle = 0$ or $\langle v\rangle \cap \langle x\rangle = 0$.

<u>Proof</u>: If $p^{a+b-1}u \in \langle x\rangle$ and $p^{c+d-1}v \in \langle x\rangle$ then $\{p^{a+b-1}u, p^{c+d-1}v\} = \{x^2 - p^{j-1}x,\ p^{j+k-1}x\}$ so $p^{j+k-1}x \in \{u,v\}$, a contradiction.

<u>Lemma 11</u>: Assume that $a \geq c \geq j$. Then <u,v,x> is a nil p-v-ring if and only if $k = 0$ and one of the following conditions holds:

(1) $d = 0$, $ux = xu = vx = xv = 0$.

(2) $d = 0$, $a+b > c$, $\langle v\rangle \cap \langle x\rangle = 0$, $x^2 = Ap^{a+b-1}u$, $A \neq 0$, $ux = Fx^2$,

$xu = F'x^2$.

(3) $d = 1$, $a > c$, $\langle u\rangle \cap \langle x\rangle = 0$, $x^2 = Ap^c v$, $A \neq 0$, $xv = Fp^c v$, $vx = F'p^c v$, and $1+T(F+F')+T^2 A$ is never zero.

(4) $p = 2$ or $p = 3$, $d = 1$, $a = c+1$, $b = 0$, $\langle u\rangle \cap \langle x\rangle = \langle v\rangle \cap \langle x\rangle = 0$, $x^2 = Ap^c u - p^c v$, $A \neq 0$.

(5) $p = 2$, $d = 1$, $a = c+1$, $b = 0$, $\langle v\rangle \cap \langle x\rangle = 0$, $x^2 = 2^c u$, ux, $xu \in \{x^2\}$, $ux \neq xu$.

<u>Proof</u>: Lemma 6 on $\langle u,v\rangle$ shows that $d = 0$ or else $a > c$, $d = 1$. Lemma 8 on $\langle u,x\rangle$ shows that $k = 0$. First suppose $ux = xu = vx = xv = 0$. If $d = 0$ then (1) holds, so assume that $a > c$, $d = 1$. Writing $U = U'p^{\alpha} - p^a V$ one sees that $v(u+v+x) = p^c v = U'(p^{a+b-1}u + p^{a+b-1}v) + V(p^c v + x^2)$, from which it follows that $x^2 = Ap^{a+b-1}u + Bp^c v$ for some A, B not both zero. Let $R \neq 0$, $S \neq 0$. Then $v(Rp^{a+b-c-1}u+Sv+x) = Sp^c v = U(Rp^{a+b-1}u+Sp^c v) + V(Ap^{a+b-1}u+(B+S^2)p^c v)$. This is solvable only if the determinant $R(B+S^2)-AS$ is never zero for $R \neq 0$, $S \neq 0$. This implies either $A = 0$, $B+S^2$ is never 0, which is case (3), or else $p = 2$ or $p = 3$, $B = -1$, $A \neq 0$. Then $v(u+v+x)$ is not in $\langle u+v+x\rangle$ unless $a+b = c+1$. Thus (4) holds. If not all of ux, xu, vx, xv are zero then $\langle u\rangle \cap \langle x\rangle \neq 0$ or $\langle v\rangle \cap \langle x\rangle \neq 0$.

Suppose $\langle u\rangle \cap \langle x\rangle \neq 0$. By Lemma 10 $\langle v\rangle \cap \langle x\rangle = 0$. If $a = c$, $b = d = 0$ then $x(u+v) = xu = U(u+v)$ so $ux = xu = 0$ and so (1) holds. Thus assume that $a+b > c$. We may assume that (2) of Lemma 8 holds in $\langle u,x\rangle$ so $x^2 = Ap^{a+b-1}u$, $A \neq 0$. If $d = 0$ then (2) holds. Suppose $a > c$ and $d = 1$. If it were true that $a+b > c+1$ then it would follow that $v(Ap^{a+b-c-1}u+v+x) = p^c v = U(Ap^{a+b-1}u+p^c v) + V(p^c v +$

$Ap^{a+b-1}u)$, which is not solvable. Thus $a = c+1$, $b = 0$, $d = 1$. If there is an integer T for which $T(F+F'+AT) \neq 0$ then for that T we have $v(u+T(F+F'+AT)v+Tx) = T(F+F'+AT)p^c v = U[p^c u+T(F+F'+AT)p^c v] + V[T(F+F'+AT)][T(F+F'+AT)p^c v+p^c u]$ cannot be solved. Thus $p = 2$, $A = F+F' = 1$, and so (5) holds.

Finally suppose $\langle u\rangle \cap \langle x\rangle = 0$, $\langle v\rangle \cap \langle x\rangle \neq 0$. If $d = 0$ then $x(u+v) = xv = U(u+v) + Vp^a u$ so p^a divides U and since $a \geq c$ it follows that $xv = vx = 0$ and so (1) holds. If $d = 1$ then we may assume that (2) of Lemma 8 holds in $\langle v,x\rangle$, and then $x^2 = Ap^c v$, $A \neq 0$, $vx = Fp^c v$, $xv = F'p^c v$. But $(v+Tx)^2 = [1+T(F+F')+T^2 A]p^c v$ is never zero since the number of type I generators with square not zero is assumed to be minimal, and so (3) holds.

<u>Lemma 12</u>: Assume that $a \geq j > c$. Then $\langle u,v,x\rangle$ is a nil p-v-ring if and only if $k = 0$ and one of the following conditions holds:

(1) $d = 0$, $xv = vx = 0$, $\langle u,x\rangle$ satisfies Lemma 8.

(2) $d = 1$, $\langle u\rangle \cap \langle x\rangle = 0$, $p^c v = Ax^2$, $A \neq 0$, $vx = Fp^c v$, $xv = F'p^c v$, and $1+T(F+F')A+T^2 A$ is never zero.

<u>Proof</u>: Lemma 6 on $\langle u,v\rangle$ shows that $d = 0$ or $d = 1$. Lemma 8 on $\langle u,x\rangle$ shows that $k = 0$. Lemma 9 on $\langle v,x\rangle$ shows that if $d = 0$ then $xv = vx = 0$ so (1) holds, while if $d = 1$ then $p^c v = Ax^2+Bp^{j-1}x$ for some $A \neq 0$, B, $vx = Fp^c v$, $xv = F'p^c v$, and $1+T[A(F+F')+Bp^{j-c-1}] +T^2 A$ is never 0. Lemma 10 then asserts that $\langle u\rangle \cap \langle x\rangle = 0$. From $v(u+x) = vx = U(u+x) + V(p^a u+x^2)$ we obtain (since p^a divides U so $vx = Vx^2$) either $F = F' = 0$ or $B = 0$. If $B = 0$ then (2) holds. If $B \neq 0$, $F = F' = 0$, then $x(u+v+x)$ is not in $\langle u+v+x\rangle$.

<u>Lemma 13</u>: Assume that $j > a \geq c$. Then $\langle u,v,x\rangle$ is a nil p-v-ring if and only if one of the following conditions holds:

(1) $d = 0$, $xv = vx = 0$, $\langle u,x\rangle$ satisfies Lemma 9.

(2) $d = 1$, $b = 0$, $j > a > c$, $\langle u\rangle \cap \langle x\rangle = 0$, and $\langle v,x\rangle$ satisfies condition (2) of Lemma 9.

<u>Proof</u>: By Lemma 6 $d = 0$ or $a > c$, $d = 1$. If $d = 0$ then by Lemma 9 $xv = vx = 0$ and so (1) holds. If $d = 1$ then $\langle v,x\rangle$ satisfies (2) of Lemma 9 so by Lemma 10 $\langle u\rangle \cap \langle x\rangle = 0$ and thus (2) holds.

<u>Lemma 14</u>: Assume that $a \geq c \geq g \geq j$. Then $\langle u,v,w,x\rangle$ is a nil p-v-ring if and only if one of the following conditions holds:

(1) $h = 0$, w annihilates $\langle u,v,w,x\rangle$, and $\langle u,v,x\rangle$ satisfies Lemma 11.

(2) $h = 1$, $d = 0$, $c > g$, $\langle u\rangle \cap \langle x\rangle = \langle v\rangle \cap \langle x\rangle = 0$, and $\langle u,w,x\rangle$ satisfies condition (3) of Lemma 11.

<u>Proof</u>: If $h = 0$ then Lemma 11 on $\langle u,w,x\rangle$ shows that w annihilates $\langle u,v,w,x\rangle$ and so (1) holds. If $h > 0$ then Lemma 7 on $\langle u,v,w\rangle$ shows that $h = 1$, $d = 0$, and $c > g$. Lemma 11 on $\langle u,w,x\rangle$ shows that $x^2 \in \{u,w\}$ and on $\langle v,w,x\rangle$ shows that $x^2 \in \{v,w\}$ so $x^2 \in \{w\}$, and thus (3) of Lemma 11 holds in $\langle u,w,x\rangle$. Thus (2) of the conclusion holds.

<u>Lemma 15</u>: Assume that $j > g$. Then $\langle u,v,w,x\rangle$ is a nil p-v-ring if and only if one of the following conditions holds:

(1) $h = 0$, w annihilates $\langle u,v,w,x\rangle$, $\langle u,v,x\rangle$ satisfies Lemma 11, 12, or 13.

(2) $h = 1$, $a \geq j$, $c > g$, $d = 0$, $k = 0$, $\langle u\rangle \cap \langle x\rangle = \langle v\rangle \cap \langle x\rangle = 0$, and

$\langle u,w,x\rangle$ satisfies condition (2) of Lemma 12.

(3) $j > a \geq c > g$, $h = 1$, $b = 0$, $d = 0$, $\langle u\rangle \cap \langle x\rangle = \langle v\rangle \cap \langle x\rangle = 0$ and $\langle u,w,x\rangle$ satisfies (2) of Lemma 13.

<u>Proof</u>: If $h = 0$ then by Lemma 9 w annihilates x so (1) holds. If $h > 0$ then by Lemma 7 $h = 1$, $c > g$, and $d = 0$. If $a \geq j$ then (2) holds, while if $j > a$ then (3) holds.

<u>Theorem 6</u>: If a nil p-v-ring has an additive group direct sum decomposition with a minimum of one generator of type II then the ring is isomorphic to a ring $\mathcal{R}$ satisfying one of the following conditions, where $\mathcal{N}$ is a (null) p-ring annihilating $\mathcal{R}$, x is of type II, $px^2 = p^j x$, $p^{j+k}x = 0$, u and v are of type I, $u^2 = p^a u$, $p^{a+b}u = 0$, $v^2 = p^c v$, $p^{c+d}v = 0$, and $\langle \ldots \rangle$ is assumed to be the additive group direct sum of the cyclic groups generated by the enclosed elements.

(1) $\mathcal{R} = \{x\} \dotplus \mathcal{N}$, $x^2 - p^{j-1}x$ is any element of $\mathcal{R}$ which annihilates $\mathcal{R}$, char $(x^2 - p^{j-1}x) = p$. If $k > 0$ then char $\mathcal{N} < p^j$.

(2) $\mathcal{R} = \{u\} \dotplus \{x\} \dotplus \mathcal{N}$, $b > 0$, $a \geq j$, $k = 0$, $x^2 - p^{j-1}x$ is any element of $\mathcal{R}$ not in $\{x\}$ which annihilates $\mathcal{R}$, char $(x^2 - p^{j-1}x) = p$, $ux = xu = 0$, char $\mathcal{N} \leq p^a$.

(3) $\mathcal{R} = \langle u,x\rangle \oplus \mathcal{N}$, $a+b > j$, $k = 0$, $x^2 = Ap^{a+b-1}u$, $A \neq 0$, ux, $xu \in \{x^2\}$. If $b = 0$ then char $\mathcal{N} < p^a$. If $b > 1$ then char $\mathcal{N} \leq p^a$. If $b = 1$ let $ux = Fx^2$, $xu = F'x^2$. Then $1 + T(F+F'+T)A$ is never zero.

(4) $\mathcal{R} = \langle u,x\rangle \oplus \mathcal{N}$, $a = j$, $b = k = 0$, $p^{a-1}u = Ax^2 + Bp^{j-1}x$, $A \neq 0$, $ux = Fp^{a-1}u$, $xu = F'p^{a-1}u$, $B+A(F+F') = 0$, and char $\mathcal{N} < p^j$.

(5) $\mathcal{R} = \langle u,x\rangle \oplus \mathcal{N}$, $j > a$, $b = 1$, $p^a u = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$, $A \neq 0$, $ux = Fp^a u$, $xu = F'p^a u$, $1+T[A(F+F')+Bp^k-A)p^{j-a-1}]+T^2A$ is never zero. Either $k = 0$, $A = B$ or char $\mathcal{N} < p^j$.

(6) $\mathcal{R} = \langle u,x\rangle \oplus \mathcal{N}$, $j = a+1$, $b = 2$, $k = 0$, $p^{a+1}u = Ax^2$, $A \neq 0$, ux, $xu \in \{x^2\}$, and char $\mathcal{N} < p^j$.

(7) $\mathcal{R} = \langle u\rangle \oplus \langle v,x\rangle \oplus \mathcal{N}$, $a \geq j$, $a > c$, $d = 1$, $k = 0$, $x^2 = Ap^c v$, $A \neq 0$, $vx = Fp^c v$, $xv = F'p^c v$, $1+T(F+F')+T^2A$ is never zero. If $b > 0$ then char $\mathcal{N} \leq p^a$.

(8) $p = 2$ or $p = 3$, $\mathcal{R} = \langle u,v,x\rangle \oplus \mathcal{N}$, $a = c+1 > j$, $b = 0$, $d = 1$, $k = 0$, $x^2 = Ap^c u - p^c v$, $A \neq 0$, $ux = xu = vx = xv = 0$, char $\mathcal{N} \leq p^c$.

(9) $p = 2$, $\mathcal{R} = \langle v\rangle \oplus \langle u,x\rangle \oplus \mathcal{N}$, $a = c+1 > j$, $b = 0$, $d = 1$, $k = 0$, $x^2 = 2^c u$, ux, $xu \in \{x^2\}$, $ux \neq xu$, and char $\mathcal{N} \leq 2^c$.

Proof: This is just a summary of the results in the lemmas of this section.

VIII. NIL p-v-RINGS WITH TWO TYPE II GENERATORS

If x and y are type II generators then $\langle x\rangle \cap \langle y\rangle$ is a zero, one, or two dimensional algebra over the field of p elements. Lemma 16 shows that a zero dimensional intersection is impossible, so the calculations to follow are usually divided into two cases according to the dimension of the intersection.

Lemma 16: If $\langle x,y\rangle$ is a nil p-v-ring then $\langle x\rangle \cap \langle y\rangle \neq 0$.

Proof: If $\langle x\rangle \cap \langle y\rangle = 0$ then $xy = yx = 0$ and so $x(x+y) = x^2 = U(x+y) + V(x^2+y^2)$, which cannot be solved for U and V.

Lemma 17: Assume that $\langle x\rangle \cap \langle y\rangle$ is one dimensional. Then $\langle x,y\rangle$ is a nil p-v-ring if and only if $n = 0$ and one of the following conditions holds:

(1) $y^2 = Bp^{j+k-1}x$, $B \neq 0$, $xy = Fy^2$, $yx = F'y^2$. If $j = m$ then $k=1$.

(2) $y^2 = A(x^2-p^{j-1}x) + Bp^{j+k-1}x$, $A \neq 0$, $xy = Fy^2$, $yx = F'y^2$, and $1+T(F+F'+T)A$ is never zero. If $j = m$ then $k = 0$ and $A = B$.

(3) $p = 2$, $j = m > 1$, $k = 0$, $xy = yx = 0$, and $2^{m-1}y = x^2+2^{j-1}x$ or $2^{j-1}x = y^2+2^{m-1}y$.

(4) $p = 2$, $j = m > 1$, $k = 0$, $xy = yx = \begin{cases} x^2 = 2^{m-1}y+Ay^2 \text{ or} \\ y^2 = 2^{j-1}x+Ax^2 \end{cases}$ $A = 0,1$.

Note that replacing x or y by the generator x+y makes rings of case (3) satisfy (4) and rings of case (4) satisfy (3).

Proof: If $j+k > m$ applying Lemma 8 to $\langle px,y\rangle$ shows that $n = 0$. If $j = m$, $k = 0$ then by assumption $n = 0$. We are given that $\langle x\rangle \cap \langle y\rangle$ is one dimensional.

First suppose $y^2 \notin \langle x\rangle \cap \langle y\rangle$, so that $\langle x\rangle \cap \langle y\rangle$ is generated by $w = p^{m-1}y + Cy^2 = A(x^2-p^{j-1}x) + Bp^{j+k-1}x$ for some A,B,C.

Let $xy = Fw$, $yx = F'w$. Then $x(Tx+y) = Tx^2+Fw = U[Tp^{j-1}x + p^{j-1}y] + V[T^2x^2 + T(F+F')w + y^2]$. Suppose that $j > m$. Then $p^{j-1}y = 0$ so p divides V since $y^2 \notin \langle x\rangle$. Then $Tx^2+Fw \in \{p^{j-1}x\}$ for all $T \neq 0$. From this it follows that $p = 2$, $F = A = 1$. Similarly $F' = 1$. But then $x(2x+y)$ is not in $\langle 2x+y\rangle$. Thus we may assume that $j = m$. Consider $(x+Ty)y = Fw + Ty^2 = U[p^{j-1}x + Tp^{m-1}y] + V[x^2+T(F+F')w + T^2y^2]$. The left side is in $\langle y\rangle$ so the right side must be, so for some X we have $U = DX+pU'$, $V = AX$, where $D = Bp^k-A$. Then $Fw + Ty^2 = X([1+DT+AT(F+F')]w + [-DCT+AT^2]y^2)$. Since w and y^2 are by assumption independent but the left side must be dependent on the right side for all $T \neq 0$ it follows that the determinant $T[1+FDC]+T^2[D+AF']$ is zero for all T. Thus one holds:

(A) $1+FDC = D+AF' = 0$ (B) $p = 2$, $1+FDC = D+AF' = 1$.

One of these conditions must also hold with F and F' interchanged. It then follows that $F = F'$. If (A) holds then $F = F' \neq 0$ and $A \neq 0$, and then $T = -A^{-1}F^{-1}$ makes the w term on the right zero, whereas the w term on the left is not zero. Thus (B) holds. If $D = 0$ then $A = F = F' = 1$ and since $0 = D = B2^k-1$ it follows that $k = 0$, $B = 1$, and so (4) holds. Assume that $D = 1$. If $A = 0$ then $k = 0$, $B = 1$ and then $C \neq 0$ (otherwise $\{y\} \cap \{x\} \neq 0$) so $F = F' = 0$ and thus (3) holds. If $A = 1$ then $F = F' = 0$; so if $C = 0$, $k = 0$ then (3) holds, while if $C = 1$ then $(x+y)y \notin \langle x+y\rangle$, and if $C = 0$, $k > 0$ then $x(2x+y) \notin \langle 2x+y\rangle$.

Now assume that $y^2 \in \langle x\rangle$, so $y^2 = A(x^2-p^{j-1}x) + Bp^{j+k-1}x$ for some A, B, $xy = Fy^2$, $yx = F'y^2$. If $j > m$ then $p^{j-1}(x+Ty) = p^{j-1}x$

and $(x+Ty)^2 = [1+T(F+F'+T)A]x^2 + [T(F+F'+T)(Bp^k-A)]p^{j-1}x$. Since x cannot be replaced by a type I generator it follows that $1+T(F+F'+T)A$ is never zero. Thus (1) or (2) holds. If $j = m$, $k > 0$ then from $x(px+y) = p^jx + Fy^2 = Up^{j+1}x + V(p^{j+1}x+y^2)$ one sees that $k = 1$, $y^2 = Bp^jx$, and so (1) holds. Finally, if $j = m$ and $k = 0$ then by interchanging x and y one sees by the above that either $x^2 \in \langle y\rangle$ or (3) or (4) holds. If $x^2 \in \langle y\rangle$ then $y^2 = Ax^2$, $A \neq 0$, and since x cannot be replaced by a generator of the form $x+Ty$ with square zero, it follows that $1+T(F+F'+T)A$ is never zero. Thus (2) holds.

<u>Lemma 18</u>: Assume that $\langle x\rangle \cap \langle y\rangle$ is two dimensional. Let $\alpha = x^2-p^{j-1}x$ and $\beta = p^{j+k-1}x$. Then $\langle x,y\rangle$ is a nil p-v-ring if and only if $n = 0$, $xy = F\alpha + G\beta$, $yx = F'\alpha + G'\beta$, $y^2 = A\alpha + B\beta$, $p^{m-1}y = C\alpha + D\beta$, $C \neq 0$, $AD \neq BC$, and one of the following holds:

(1) $j > m$, $A = 0$, $F = F' = 0$.

(2) $j > m$, $A \neq 0$, $xy, yx \in \{y^2\}$, and $1+T(F+F')+T^2A$ is never 0.

(3) $j = m+1$, $k = 0$, $A = 0$, and $F = -F' \neq 0$.

(4) $j = m$, $k > 0$, $A \neq 0$, $xy-p^{m-1}y$, $yx-p^{m-1}y \in \{y^2\}$, and $1+T(F+F'-C)+T^2A$ is never zero.

(5) $j = m$, $k = 1$, $A = 0$, $F + F' = C$.

(6) $j = m$, $k = 0$, and $1+T[D-C+F+F']+T^2[A+D(F+F')-C(G+G')]+T^3[AD-BC]$ is never zero.

Note that rings satisfying conditions (1) and (2) are homomorphs of rings satisfying (1) and (2) of Lemma 17.

<u>Proof</u>: If $j+k > m$ applying Lemma 8 to $\langle px,y\rangle$ shows that $n = 0$.

If $j = m$ and $k = 0$ then by assumption $r = 0$. $C \neq 0$ follows from $\{x\} \cap \{y\} = 0$. $AD \neq BC$ since y is not of type I. Consider

$$(x+Ty)^2 - p^{j-1}(x+Ty) = [1+T(F+F'-Cp^{j-m})+T^2A]\alpha + [T(G+G'-Dp^{j-m})+T^2B]\beta$$
$$p^{j+k-1}(x+Ty) = \qquad [TCp^{j+k-m}]\alpha + \qquad [1+TDp^{j+k-m}]\beta$$

Since x cannot be replaced by a type I generator of the form $x+Ty$ it follows that the determinant formed by the four coefficients above must never be zero. This, together with the relations on the exponents and on A implies the relations on the coefficients in conditions (2) through (6).

First suppose $j > m$ and $A = 0$. If $j = m+1$ and $k = 0$ then (1) or (3) holds. Otherwise $x(px+y) = p^j x + xy = Up^j x + V(p^{j+1}x + Bp^{j+k-1}x)$ shows that $xy \in \{x\}$, which means $F = 0$. Similarly $F' = 0$, and thus (1) holds.

Next suppose $j > m$ and $A \neq 0$. Then $p^{j+k-1}x = My^2 + Np^{m-1}y$ for some $M \neq 0$, $N \neq 0$. Then $x(p^{j+k-m}x - Ny) = -Nxy = U(p^{j+k-1}x - Np^{m-1}y) + V(N^2y^2) = (UM+VN^2)y^2$ so xy, $yx \in \{y^2\}$, and so (2) holds.

If $j = m$, $k > 0$, and $A \neq 0$ then $p^{j+k-1}x = My^2 + Np^{m-1}y$ for some $M \neq 0$, $N \neq 0$. Then $x(p^k x - Ny) = p^{j+k-1}x - Nxy = (UM+VN^2)y^2$ so $xy - p^{m-1}y$, $yx - p^{m-1}y \in \{y^2\}$, and so (4) holds.

If $j = m$, $k > 0$, and $A = 0$ then by the relations on the coefficients $F+F' = C$. Suppose $k > 1$. Then $x(p^{k-1}x+y) = p^{j+k-2}x + xy = U(p^{j+k-2}x + p^{m-1}y) + V(p^{j+2k-3}x + y^2)$. Multiplying by p shows that $U = 1 + pU'$ so $xy = p^{m-1}y + (\ldots)y^2$ so $F = C$. Similarly $F' = C$. But $F+F' = C$, so $C = 0$, which is impossible. Thus $k = 1$ and so condition (5) holds.

If $j = m$ and $k = 0$ then condition (6) holds.

Lemma 19: Assume that $a \geq j \geq m$ and that $\langle x\rangle \cap \langle y\rangle$ is one dimensional. Then $\langle u,x,y\rangle$ is a nil p-v-ring if and only if $k = n = 0$ and one of the following conditions holds:

(1) $ux = xu = uy = yu = 0$, $y^2 = Ax^2$, $A \neq 0$, $xy = Fx^2$, $yx = F'x^2$, and $1+T(F+F')+T^2A$ is never zero.

(2) $x^2, ux, xu, uy, yu \in \{p^{a+b-1}u\}$, $y^2 = Ax^2$, $A \neq 0$, $xy = Fx^2$, $yx = F'x^2$, and $1+T(F+F')+T^2A$ is never zero. If $a = j$ and $b = 0$ then $uy = -yu$ and $ux = -xu$.

(3) $a = j > m$, $b = 0$, $p^{a-1}u = Cy^2 = C(Ax^2 + Bp^{j-1}x)$, $A \neq 0$, $B \neq 0$, $C \neq 0$, $ux = Hp^{a-1}u$, $xu = H'p^{a-1}u$, $B + A(H+H') = 0$, $uy = -yu = Kp^{a-1}u$, $xy = Fy^2$, $yx = F'y^2$, and $1+T(F+F'+T)A$ is never zero.

(4) $p = 2$, $a = j > m$, $b = 0$, $2^{a-1}u = x^2 + 2^{j-1}x$, $ux, xu \in \{2^{a-1}u\}$, $ux \neq xu$, $xy, yx \in \{y^2\}$, $xy \neq yx$, $\langle u\rangle \cap \langle y\rangle = 0$, and either $y^2 = x^2$ or $y^2 = 2^{j-1}x$.

Replacing x by u+x in (4) interchanges the two subcases.

Proof: By Lemma 8 we have $k = n = 0$. By Lemma 17 one of the following conditions holds, where in (B) the original x and y may have been interchanged or one replaced by x+y.

(A) $y^2 = Ax^2 + Bp^{j-1}x$, $xy = Fy^2$, $yx = F'y^2$, $1+T(F+F'+T)A$ is never zero. If $j = m$ then $B = 0$.

(B) $p = 2$, $j = m > 1$, $xy = yx = 0$, and $2^{m-1}y = x^2 + 2^{j-1}x$.

By Lemma 8 one of the following conditions holds:

(C) $ux = xu = 0$.

(D) $a+b > j$, $p^{a+b-1}u = Cx^2$, $C \neq 0$, $ux, xu \in \{p^{a+b-1}u\}$.

(E) $a=j$, $b=0$, $p^{a-1}u=Cx^2+Dp^{j-1}x$, $ux=Hp^{a-1}u$, $xu=H'p^{a-1}u$, and $D+C(H+H')=0$.

First suppose that $\langle u\rangle \cap \langle x\rangle = 0$ and $j>m$. Then $y^2 \in \langle x\rangle$ so by Lemma 8 $uy=yu=0$. If $F\neq 0$ then $(u+x)y=Fy^2=Vx^2$ so $y^2=Ax^2$ and so (1) holds. Similarly if $F'\neq 0$ then (1) holds. If $F=F'=0$ then $(u+x+y)y=y^2=V(x^2+y^2)$ so again $y^2=Ax^2$ and so (1) holds.

Second suppose $\langle u\rangle \cap \langle x\rangle = \langle u\rangle \cap \langle y\rangle = 0$ and $j=m$. Condition (A) implies (1) of the conclusion, so suppose (B) holds. Then $(u+x+y)y=y^2=V(x^2+y^2)$ cannot be solved for V.

Third suppose $\langle u\rangle \cap \langle y\rangle = 0$ and $p^{a+b-1}u=Cx^2+Dp^{j-1}x$, $C\neq 0$. Condition (B) implies $p^{a+b-1}u=C(p^{m-1}y-p^{j-1}x)+Dp^{j-1}x$, which is impossible. Thus (A) holds. Also $AD\neq BC$. If $j=m$ then by (A) $y^2=Ax^2$, and $u(x+y)=ux=V(x^2+(F+F'+1)Ax^2)$. But $x^2\in\langle y\rangle$, $p^{a+b-1}u\notin\langle y\rangle$ so $ux=0$. Similarly $xu=0$, and so (1) holds. Thus we may assume that $j>m$.

Suppose $D=0$. Then $B\neq 0$, $C\neq 0$, and $(H+H')p^{a+b-j}=0$, so $(x+y+B^{-1}C^{-1}(A+1)p^{a+b-j}u)^2=(A+1)x^2+Bp^{j-1}x$, while $p^{j-1}(x+y+B^{-1}C^{-1}(A+1)p^{a+b-j}u)=B^{-1}((A+1)x^2+Bp^{j-1}x)$. Thus x may be replaced by a type I generator. Suppose on the other hand that $D\neq 0$. Then if either $a+b>j$ or $H+H'=0$ it follows that $(x-D^{-1}p^{a+b-j}u)^2=x^2$ and $p^{j-1}(x-D^{-1}p^{a+b-j}u)=-CD^{-1}x^2$, so again x may be replaced by a type I generator. Thus we may assume $D\neq 0$, $D+C(H+H')=0$, $a=j>m$, and $b=0$. Consider

$$(x+Su+Ty)^2=[1+SC(H+H')+T(F+F'+T)A]x^2+[SD(H+H')+T(F+F'+T)B]p^{j-1}x$$

$p^{j-1}(x + Su + Ty) = [SC]x^2 + [SD + 1]p^{j-1}x$.

If the determinant $S[(AD-BC)T(F+F'+T)] + [1+T(F+F'+T)A]$ is ever zero then x can be replaced by a type I generator. Since $AD-BC \neq 0$ this can be made zero for suitable S, T unless $p = 2$, $F+F' = 1$. Then (4) holds.

Fourth suppose $\langle u\rangle \cap \langle x\rangle = 0$, $\langle u\rangle \cap \langle y\rangle \neq 0$, and $j = m$. Interchanging x and y (which is possible unless (B) holds) gives $\langle u\rangle \cap \langle x\rangle \neq 0$, $\langle u\rangle \cap \langle y\rangle = 0$, $j = m$. This case has already been considered. It was shown that such rings satisfy (1), which is self-dual. Now suppose (B) holds. We show that (*) $a+b > j$ and $2^{a+b-1}u = y^2$. First suppose $uy \neq 0$. Then $u(x+y) = uy = Ux^2 + V(x^2+y^2)$ so $2^{a+b-1}u = y^2$. If $a+b > j$ then (*) holds so suppose $a = j$, $b = 0$. Then $(u+x)y = uy = U(y^2+2^{j-1}x) + Vx^2$ cannot be solved. Second assume that $uy = yu = 0$. If $a+b > j$ then $y(u+x+y) = y^2 = U(2^{a+b-1}u) + V(x^2+y^2)$ so $2^{a+b-1}u = y^2$ and (*) holds. If $a = j$ and $b = 0$ then $y(u+x+y) = y^2 = U(2^{a-1}u+x^2) + V(x^2+y^2)$ cannot be solved. Thus (*) always holds. Then $(x+y+2^{a+b-j}u)^2 = x^2 + y^2$, $2^{j-1}(x+y+2^{a+b-j}u) = x^2 + y^2$ and so x may be replaced by a type I generator.

Fifth suppose $p^{a+b-1}u = Cy^2 = CAx^2$, $A \neq 0$, $C \neq 0$. If $a+b > j$ then (2) holds. If $a = j$, $b = 0$ then by (C) or (E) we have $ux = -xu$. Let $uy = Kx^2$, $yu = K'x^2$. Since $(x+y+Su)^2 = [1+A+(F+F')A+S(K+K')]x^2$, x may be replaced by a type I generator unless $K+K' = 0$. Thus (2) holds.

Finally suppose $p^{a+b-1}u = Cy^2 = C(Ax^2 + Bp^{j-1}x)$, $A \neq 0$, $B \neq 0$,

$C \neq 0$. By (A) we have $j > m$. Let $ux = Hp^{a+b-1}u$, $xu = H'p^{a+b-1}u$, $uy = Kp^{a+b-1}u$, $yu = K'p^{a+b-1}u$. Assume first that $a+b > j$. Then $u(BCx-p^{a+b-j}u) = BCux = U(-ACx^2) + V(B^2C^2x^2)$ so $ux = 0$. Similarly $xu = yx = xy = 0$. Then $y(BCx+BCy-(A+1)p^{a+b-j}u) = BCy^2 = U(-Ap^{a+b-1}u -ACx^2) + V(B^2C^2x^2 + B^2C^2y^2) = (VB^2C^2-UAC)(x^2+y^2)$ cannot be solved. Thus $a = j$ and $b = 0$. Since $(x+Su+Ty)^2 = x^2 + [SC(H+H'+T(K+K'))+T(F+F')T^2]y^2$ and $p^{j-1}(x+Su+Ty) = -AB^{-1}x^2 + (B^{-1}+SC)y^2$ and x cannot be replaced by a type I generator, it follows that $C+AB^{-1}C(H+H'+T(K+K')) = 0$ for all T. Then $B+A(H+H') = 0$, $K+K' = 0$, and so condition (3) holds.

<u>Lemma 20</u>: Assume that $a \geq j \geq m$ and $\langle x\rangle \cap \langle y\rangle$ is two dimensional. Then $\langle u,x,y\rangle$ is a nil p-v-ring if and only if $k = n = 0$, $j > m$, $\langle u\rangle \cap \langle x\rangle = \langle u\rangle \cap \langle y\rangle = 0$, $y^2 = Ax^2$, $A \neq 0$, $xy = Fx^2$, $yx = F'x^2$, and $1+T(F+F')+T^2A$ is never zero.

<u>Proof</u>: Lemma 8 shows that $k = n = 0$. Lemma 10 shows that $\langle u\rangle \cap \langle x\rangle = \langle u\rangle \cap \langle y\rangle = 0$. Let $y^2 = Ax^2 + Bp^{j-1}x$, $xy = Fx^2 + Gp^{j-1}x$, $yx = F'x^2 + G'p^{j-1}x$. Since $a \geq j$ it follows that $(u+x)y = Fx^2 + Gp^{j-1}x = Vx^2$ so $G = 0$. Similarly $G' = 0$. Then $x(u+y) = Fx^2 = Vy^2$ so $B = 0$ or $F = F' = 0$. But if $F = F' = 0$ then $x(u+x+y) = x^2 = V(x^2+Ax^2+Bp^{j-1}x)$ so we always have $B = 0$. Condition (2) of Lemma 18 must hold, since condition (6) implies cubic $= [1+TD][1+T(F+F')+T^2A]$ is never zero, so $D = 0$, which contradicts $B = 0$, $AD \neq BC$. But condition (2) implies the conclusion of the Lemma.

<u>Lemma 21</u>: Assume that $j > a$. Then $\langle u,x,y\rangle$ is a nil p-v-ring

if and only if one of the following conditions holds:

(1) u annihilates $\langle u,x,y\rangle$ and $\langle x,y\rangle$ satisfies Lemma 17 or 18.

(2) $p=2$, $b=1$, $a\geq m$, $n=0$, $j=a+2$ and $k=0$ or $j=a+1$ and $k=1$, $\langle u\rangle \cap \langle y\rangle = 0$, $y^2 = 2^{j+k-1}x + 2^a u = x^2 + 2^{j-1}x + B2^{j+k-1}x$, xy, $yx \in \{y^2\}$, $xy \neq yx$, $ux = H2^a u$, $xu = H'2^a u$, $H+H' = 1+2^{j-a-1}$, and $\langle x\rangle \cap \langle y\rangle$ is one dimensional.

(3) $b=2$, $j=m=a+1$, $k=n=0$, $p^{a+1}u = Cy^2 = CAx^2$, $A\neq 0$, $C\neq 0$, ux, xu, uy, $yu \in \{x^2\}$, $xy = Fx^2$, $yx = F'x^2$, $1+T(F+F')+T^2A$ is never zero, and $\langle x\rangle \cap \langle y\rangle$ is one dimensional.

<u>Proof</u>: First suppose $\langle x\rangle \cap \langle y\rangle$ is two dimensional. Lemma 10 shows that $\langle u\rangle \cap \langle x\rangle = \langle u\rangle \cap \langle y\rangle = 0$. Lemma 9 shows that $b=0$, and thus (1) holds. From now on we assume that $\langle x\rangle \cap \langle y\rangle$ is one dimensional.

Suppose $j>a\geq m$. Lemma 11 on $\langle px,u,y\rangle$ shows that $b=0$ or $b=1$. If $b=0$ Lemma 9 shows that $ux=xu=0$ and Lemma 11 on $\langle px,u,y\rangle$ shows that $uy=yu=0$, so (1) holds. Assume that $b=1$. Case (5) of Lemma 11 on $\langle px,u,y\rangle$ implies $(px)y\neq 0$ or $y(px)\neq 0$, which is impossible, so either (3) or (4) holds.

Assume that (3) holds. Then $p^a u = Cy^2$, $uy = Ky^2$, $yu = K'y^2$, $1+T(K+K')+T^2C$ is never zero, and $j+k-1>a$. By Lemma 17 $y^2 = A(x^2-p^{j-1}x) + Bp^{j+k-1}x$, $xy = Fy^2$, $yx = F'y^2$, $1+T(F+F'+T)A$ is never zero, and $A\neq 0$. By Lemma 9 $ux = Hp^a u$, $xu = H'p^a u$, and $1+T[AC(H+H')+(Bp^k-A)Cp^{j-a-1}]+T^2AC$ is never zero. But then x can be replaced by a type I generator of the form $x+Sy+Tu$ for suitable S, T.

Assume that (4) holds. Then $y^2 = \pm p^{j+k-1}x - p^a u$, $\langle u\rangle \cap \langle y\rangle = 0$, $j+k = a+2$, and by Lemma 17 $y^2 = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$, $A \neq 0$ (for $A = 0$ implies $\{u\} \cap \{x\} \neq 0$). Then $p^a u = -A(x^2 - p^{j-1}x) + (\pm 1 - B)p^{j+k-1}x$. As above if $p = 3$ x may be replaced by a type I generator. If $p = 2$ by Lemmas 17 and 9 $xy, yx \in \{y^2\}$, $xy \neq yx$, $ux = H2^a u$, $xu = H'2^a u$, $H+H' = 1+2^{j-a-1}$. Thus (2) holds.

Next suppose that $j+k > m > a$. If $b = 0$ then by Lemma 9 condition (1) holds. If $b > 0$ then Lemma 12 on $\langle px,u,y\rangle$ shows that $b = 1$, $p^a u = Cy^2$, $C \neq 0$. Then cases (1) and (3) of Lemma 17 are impossible, and we may by changing x and y assume that (4) does not hold, so (2) holds. Then as above x may be replaced by a type I generator.

Suppose finally that $j = m > a$, $k = n = 0$. By Lemma 9 we have $b = 0$, 1, or 2. If $b = 0$ then (1) holds. If $b = 1$ then as above x may be replaced by a type I generator. If $b = 2$ then by Lemmas 9 and 17 it follows that (3) holds.

Lemma 22: Assume that $a \geq c \geq j \geq m$. Then $\langle u,v,x,y\rangle$ is a nil p-v-ring if and only if $k = n = 0$, $y^2 = Ax^2$, $xy = Fx^2$, $yx = F'x^2$, $1+T(F+F')+T^2A$ is never zero, and one of the following holds:

(1) $d = 0$, u and v annihilate x and y.

(2) $d = 0$, $b \neq 1$, $\langle v\rangle \cap \langle x,y\rangle = 0$, $x^2, ux, xu, uy, yu \in \{p^{a+b-1}u\}$. If $b = 0$ then $a > c$.

(3) $p = 2$, $d = 1$, $b = 0$, $a = c+1$, u and v annihilate x and y, $x^2 = 2^c u + 2^c v$.

Proof: First assume $d = 0$. Then one of (1) or (2), Lemma 11, holds in $\langle u,v,x\rangle$, and these imply that Lemma 20 or (1) or (2) of Lemma 19 holds in $\langle u,x,y\rangle$. These conditions together imply the relations on x and y, and also imply that (1) or (2) of the conclusion holds, except that (2) might hold with $b = 1$. But then for suitable S, T we would have $(u+Sx+Ty)^2 = 0$, contrary to the assumption that the number of type I generators with square not zero is minimal.

Now assume that $d > 0$. By Lemma 11 $d = 1$. If $\langle x\rangle \cap \langle y\rangle$ were two dimensional then by Lemma 10 $\langle u\rangle \cap \langle x\rangle = \langle v\rangle \cap \langle x\rangle = 0$, so (4) of Lemma 11 would hold in $\langle u,v,x\rangle$. But then $p^{m-1}y \in \{u,v,x\}$, a contradiction. Thus $\langle x\rangle \cap \langle y\rangle$ is one dimensional.

Since $d = 1$ it follows that $a > c$ so (3) and (4) of Lemma 19 do not hold in $\langle u,x,y\rangle$. Suppose (2) holds. Then $y^2 = Ax^2 \in \{u\}$ so (5) of Lemma 11 holds in $\langle u,v,x\rangle$, in $\langle u,v,y\rangle$, and in $\langle u,v,x+y\rangle$. Then $p = 2$, $ux \neq xu$, $uy \neq yu$, $u(x+y) \neq (x+y)u$. This is impossible, and so (1) of Lemma 19 holds in $\langle u,x,y\rangle$. Then (5) of Lemma 11 cannot hold in $\langle u,v,x\rangle$. If (3) of Lemma 11 holds then v may be replaced by a generator with square zero, which is assumed not to be possible. Thus (4) of Lemma 11 holds. First suppose $p = 3$. Let $y^2 = Ex^2 = E(A3^c u - 3^c v)$, $xy = Fx^2$, $yx = F'x^2$. Choose T so that $1+T(F+F')+T^2E = -1$. Then $v(v+Au+x+Ty) = 3^c v = U(A3^c u + 3^c v) + V(-A3^c u + 2(3^c v))$ cannot be solved. Thus $p = 2$, and so (3) of the conclusion holds.

<u>Lemma 23</u>: Assume that $j > c$. Then $\langle u,v,x,y\rangle$ is a nil p-v-ring if and only if one of the following conditions holds:

(1) $d = 0$, v annihilates x and y, $\langle u,x,y\rangle$ satisfies Lemma 19, 20, or 21.

(2) $p = 2$, $d = 1$, $b = k = n = 0$, $j = a+1 = c+2$, $\langle u\rangle \cap \langle v,x,y\rangle = 0$, and $\langle v,x,y\rangle$ satisfies condition (2), Lemma 21.

Proof: If $d = 0$ then by Lemma 21 on $\langle v,x,y\rangle$ it follows that v annihilates x and y, so (1) holds. If $d > 0$ then by Lemma 6 $d = 1$. First suppose $a \geq j$. By Lemma 12 on $\langle u,v,x\rangle$ we have $\langle u\rangle \cap \langle x\rangle = 0$ and $x^2 \in \{v\}$. Then $\langle v,x,y\rangle$ does not satisfy Lemma 21. On the other hand suppose $j > a$. By Lemma 13 we have $b = 0$, $j > a > c$. Then (2) of Lemma 21 must hold in $\langle v,x,y\rangle$, and so (2) of the conclusion holds.

Theorem 7: If the group direct sum decompositions of a nil p-v-ring involve a minimum of two type II generators, then under the notation of section V the ring is isomorphic to a ring $\mathcal{R}$ satisfying one of the following conditions, where $\mathcal{N}$ is a (null) p-ring annihilating $\mathcal{R}$:

(1) $\mathcal{R} = \{x,y\} \dotplus \mathcal{N}$, $j \geq m$, $n = 0$, $y^2 = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$, $xy = Fy^2$, $yx = F'y^2$, $1+T(F+F'+T)A$ is never zero, $x^2 - p^{j-1}x$ is any element of $\mathcal{R}$ not in $\{x\}$ with characteristic p which annihilates $\mathcal{R}$, char $\mathcal{N} < p^j$. If $j > m$ then $k \neq 0$ or $B \neq A$. If $j = m$ then $A = 0$, $B \neq 0$, and $k = 1$.

(2) $\mathcal{R} = \{u\} \dotplus \{x,y\} \dotplus \mathcal{N}$, $k = n = 0$, $a \geq j \geq m$, x and y are as in (1). If $b > 0$ then char $\mathcal{N} \leq p$. Also $A = B$.

(3) $\mathcal{R} = \langle u,x,y\rangle \oplus \mathcal{N}$, $a \geq j \geq m$, $k = n = 0$, $b \neq 1$, $y^2 = Ax^2$, $xy = Fx^2$, $yx = F'x^2$, $1+T(F+F')+T^2A$ is never zero, $\langle x\rangle \cap \langle y\rangle$ is

one dimensional, x^2, ux, xu, uy, yu $\in \{p^{a+b-1}u\}$. If $a = j$, $b = 0$ then $uy = -yu$, $ux = -xu$. If $b = 0$ then char $\mathcal{N} < p^a$. If $b > 1$ then char $\mathcal{N} \leq p^a$.

(4) $\mathcal{R} = \langle u,x,y\rangle \oplus \mathcal{N}$, $a = j > m$, $b = k = n = 0$, $p^{a-1}u = Cy^2 = C(Ax^2 + Bp^{j-1}x)$, $A \neq 0$, $B \neq 0$, $C \neq 0$, $ux = Hp^{a-1}u$, $xu = H'p^{a-1}u$, $B + A(H+H') = 0$, $uy = -yu = Kp^{a-1}u$, $xy = Fy^2$, $yx = F'y^2$, $1+T(F+F'+T)A$ is never zero, $\langle x\rangle \cap \langle y\rangle$ is one dimensional, and char $\mathcal{N} < p^j$.

(5) $\mathcal{R} = \langle u,x,y\rangle \oplus \mathcal{N}$, $j = m = a+1$, $b = 2$, $k = n = 0$, $p^{a+1}u = Cy^2 = CAx^2$, $A \neq 0$, $C \neq 0$, ux, xu, uy, yu $\in \{p^{a+1}u\}$ $xy = Fy^2$, $yx = F'y^2$, $1+T(F+F'+T)A$ is never zero, $\langle x\rangle \cap \langle y\rangle$ is one dimensional, and char $\mathcal{N} < p^j$.

(6) $p = 2$, $\mathcal{R} = \{x,y\} \dotplus \mathcal{N}$, $j = m > 1$, $k = n = 0$, $xy = yx = 0$, $y^2 = 2^{j-1}x + 2^{m-1}y$, x^2 is any element of $\mathcal{R}$ with characteristic 2 which annihilates $\mathcal{R}$, $x^2 \notin \{x\}$, char $\mathcal{N} < 2^j$.

(7) $p = 2$, $\mathcal{R} = \langle u,x,y\rangle \oplus \mathcal{N}$, $a \geq m$, $b = 1$, $n = 0$, $j = a+2$ and $k = 0$ or $j = a+1$ and $k = 1$, $\langle u\rangle \cap \langle y\rangle = 0$, $y^2 = 2^{j+k-1}x + 2^a u = x^2 + 2^{j-1}x + B2^{j+k-1}x$, xy, yx $\in \{y^2\}$, $xy \neq yx$, $ux = H2^a u$, $xu = H'2^a u$, $H+H' = 1 + 2^{j-a-1}$, $\langle x\rangle \cap \langle y\rangle$ is one dimensional, and char $\mathcal{N} < 2^j$.

(8) $p = 2$, $\mathcal{R} = \langle u,x,y\rangle \oplus \mathcal{N}$, $a = j > m$, $b = 0$, $2^{a-1}u = x^2 + 2^{j-1}x$, $y^2 = x^2$, ux, xu $\in \{2^{a-1}u\}$ $ux \neq xu$, xy, yx $\in \{y^2\}$, $xy \neq yx$, $\langle u\rangle \cap \langle y\rangle = 0$, and char $\mathcal{N} < 2^j$.

(9) $p = 2$, $\mathcal{R} = \langle u,v,x,y\rangle \oplus \mathcal{N}$, $a-1 = c \geq j \geq m$, $d = 1$, $b = k = n = 0$, $\langle u\rangle \cap \langle x\rangle = \langle u\rangle \cap \langle y\rangle = \langle v\rangle \cap \langle x\rangle = \langle v\rangle \cap \langle y\rangle = 0$, $x^2 = y^2 = 2^c u +$

$2^c v$, $\langle x\rangle \cap \langle y\rangle$ is one dimensional, and char $\mathcal{N} < 2^j$.

In the following cases, $\mathcal{R} = \langle x,y\rangle \oplus \mathcal{N}$, $n = 0$, $y^2 = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$, $p^{m-1}y = C(x^2 - p^{j-1}x)$, $xy = F(x^2 - p^{j-1}x) + Gp^{j+k-1}x$, $yx = F'(x^2 - p^{j-1}x) + G'p^{j+k-1}x$, $B \neq 0$, $C \neq 0$, and char $\mathcal{N} < p^j$.

(10) $j = m+1$, $k = 0$, $A = 0$, $F+F' = 0$.

(11) $j = m$, $k = 1$, $A = 0$, $F+F' = C$.

(12) $j = m$, $k > 0$, $A \neq 0$, $1+T(F+F'-C)+T^2A$ is never zero, and $xy-p^{m-1}y$, $yx-p^{m-1}y \in \{y^2\}$.

(13) $j = m$, $k = 0$, $1+T[F+F'-C]+T^2[A-C(G+G')]-T^3BC$ is never zero.

Proof: This is essentially a summary of the results in the lemmas of this section. In the last four cases above we have taken the special case $D = 0$, which is obtained from the general ring $\langle x,y\rangle$ with two dimensional intersection by making the change of generator $\bar{y} = y - Dp^{j-m+k}x$.

IX. NIL p-v-RINGS WITH THREE TYPE II GENERATORS

Lemma 24: A ring $\langle x,y,z\rangle$ is a nil p-v-ring if and only if $n = s = 0$ and one of the following conditions holds:

(1) $j+k > m$, $z^2 = Ey^2 = EBp^{j+k-1}x$, $E \neq 0$, $B \neq 0$, $xy = Fy^2$, $yx = F'y^2$, $xz = Hz^2$, $zx = H'z^2$, $yz = Kz^2$, $zy = K'z^2$, and $1+T(K+K'+T)E$ is never zero. If $j = m$ then $k = 1$.

(2) $j-1 = m > r$, $k = 0$, $z^2 = Ey^2 = EBp^{j-1}x$, $p^{m-1}y = Cx^2 + Dp^{j-1}x$, $B \neq 0$, $C \neq 0$, $E \neq 0$, $xy = Fx^2 + Gp^{j-1}x$, $yx = -Fx^2 + G'p^{j-1}x$, $F \neq 0$, $xz = Hz^2$, $zx = H'z^2$, $yz = Kz^2$, $zy = K'z^2$, and $1+T(K+K'+T)E$ is never zero.

(3) $j = m > r$, $k = 1$, $z^2 = Ey^2 = EBp^jx$, $p^{m-1}y = C(x^2-p^{j-1}x) + Dp^jx$, $B \neq 0$, $C \neq 0$, $E \neq 0$, $xy = F(x^2-p^{j-1}x) + Gp^jx$, $yx = F'(x^2-p^{j-1}x) + G'p^jx$, $F+F' = C$, $xz = Hz^2$, $zx = H'z^2$, $yz = Kz^2$, $zy = K'z^2$, and $1+T(K+K'+T)E$ is never zero.

(4) $j = m > r$, $k = 0$, $y^2 = Ax^2 + Bp^{j-1}x$, $p^{m-1}y = Cx^2 + Dp^{j-1}x$, $C \neq 0$, $AD \neq BC$, $z^2 = Ex^2 + E'p^{j-1}x$, $xy = Fx^2 + Gp^{j-1}x$, $yx = F'x^2 + G'p^{j-1}x$, $xz = Hz^2$, $zx = H'z^2$, $yz = Kz^2$, $zy = K'z^2$, $1+T(H+H'+T)E$ is never zero, $[S+D][S^2+A+T^2E+S(F+F')+TE(K+K')+STE(H+H')] \neq C[B+T^2E'+S(G+G')+TE'(K+K')+STE'(H+H')]$ for any S, T.

Proof: We shall consider two major cases, one when $j+k > m$ and the other when $j = m$ and $k = 0$.

First suppose that $j+k > m$. Lemma 19 or 20 on $\langle px,y,z\rangle$ shows that $n = s = 0$, $z^2 = Ey^2$, $yz = Kz^2$, $zy = K'z^2$, $E \neq 0$, and $1+T(K+K'+T)E$ is never zero. We now consider two cases.

(A) $\langle x\rangle \cap \langle y\rangle$ is one dimensional. By Lemma 17 $y^2 =$

$A(x^2-p^{j-1}x) + Bp^{j+k-1}x$, $xy = Fy^2$, $yx = F'y^2$, $1+T(F+F'+T)A$ is never zero, if $A = 0$, $j = m$ then $k = 1$, and if $A \neq 0$ then $j > m$. Assume that $A \neq 0$. By Lemma 17 or 18 on $\langle x,z\rangle$ we have $xz = Hz^2$, $zx = H'z^2$, and $1+T(H+H'+T)EA$ is never zero. It follows that for suitable S, T $(x+Sy+Tz)^2 \in \{x+Sy+Tz\}$ and so x may be replaced by a type I generator. On the other hand suppose that $A = 0$. Then (1) holds or else (3) or (5), Lemma 18, holds in $\langle x,z\rangle$. But if (3) holds then $x(y+z) \notin \langle x\rangle \cap \langle y+z\rangle$, while if (5) holds then $(x+y)z \notin \langle z\rangle \cap \langle x+y\rangle$.

(B) $\langle x\rangle \cap \langle y\rangle$ is two dimensional. By Lemma 10 $\langle x\rangle \cap \langle z\rangle = \langle y\rangle \cap \langle z\rangle = \{z^2\}$. Let $y^2 = A(x^2-p^{j-1}x) + Bp^{j+k-1}x$, $p^{m-1}y = C(x^2-p^{j-1}x) + Dp^{j+k-1}x$, $C \neq 0$, $AD \neq BC$, $xy = F(x^2-p^{j-1}x) + Gp^{j+k-1}x$, $yx = F'(x^2-p^{j-1}x) + G'p^{j+k-1}x$, $xz = Hz^2$, $zx = H'z^2$, and $1+T(H+H'+T)EA$ is never zero. One of conditions (1) through (5) of Lemma 18 must hold in $\langle x,y\rangle$. We consider each in turn:

(1) This is condition (1) of the conclusion.

(2) Since $j > m$, $A \neq 0$, it follows that for suitable S, T x may be replaced by the type I generator $x+Sy+Tz$.

(3) Since $p^{r-1}z \notin \langle x\rangle$ considering $x(y+z) \in \langle x\rangle \cap \langle y+z\rangle$ shows that $m > r$ and so condition (2) of the conclusion holds.

(4) As in (3) $m > r$. Then for suitable S, T x may be replaced by the type I generator $x+Sy+Tz$.

(5) As in (3) $m > r$. Then condition (3) of the conclusion holds.

Now for the second major case suppose $j = m$ and $k = 0$. From Lemma 17 or 18 $n = s = 0$. We shall consider in turn several cases obtained by applying Lemmas 17 and 18 to $\langle x,y\rangle$, and show that none of them can occur except (D), which leads to (4) of the conclusion. For convenience if $j = m = r$ and $k = n = s = 0$ we shall rename x, y, and z to insure that $\langle x\rangle \cap \langle z\rangle$ and $\langle y\rangle \cap \langle z\rangle$ are one dimensional.

(A) Lemma 17, (2). $y^2 = Ax^2$, $A \neq 0$, $xy = Fy^2$, $yx = F'y^2$, and $1+T(F+F'+T)A$ is never zero. If z^2, xz, zx, yz, $zy \in \{x^2\}$ then for suitable S, T we have $(x+Sy+Tz)^2 = 0$, and so x can be replaced by a type I generator. Otherwise Lemma 17 or 18 on $\langle x,z\rangle$ and on $\langle y,z\rangle$ shows that $j = m = r > 1$, so by assumption all intersections are one dimensional, $p = 2$, and $x^2 = y^2 = 2^{r-1}z + Az^2$, $A = 0,1$, $xy \neq yx$, $xz = zx = yz = zy = x^2$. Then $2^{m-1}y \notin \langle x\rangle$ so if $xy = x^2$ then $x(x+y+z) \notin \langle x+y+z\rangle$ while if $yx = x^2$ then $(x+y+z)x \notin \langle x+y+z\rangle$.

(B) Lemma 17, (3) or (4), $m > r$. Change x and y so that $2^{m-1}y = x^2+2^{j-1}x$, $xy = yx = 0$. Then $z^2 = 2^{m-1}y = x^2+2^{j-1}x$, xz, $zx \in \{z^2\}$, $xz \neq zx$. To be definite assume $xz = z^2$, $zx = 0$. Let $yz = Jy^2 + K2^{m-1}y$, $zy = J'y^2 + K'2^{m-1}y$, where if $\langle y\rangle \cap \langle z\rangle$ is one dimensional then $J = J' = 0$, while if $\langle y\rangle \cap \langle z\rangle$ is two dimensional then either $J = J' = 0$ or $m = r+1$, $J = -J'$. Then $(x+y)z = Jy^2 + (K+1)(x^2+2^{j-1}x) = Ux^2 + V(x^2+y^2)$. Since $y^2 \notin \langle x\rangle$ we have $V = J$. Since $2^{j-1}x \notin \{x^2\}$ we have $K = 1$. $z(x+y) = J'y^2 + K'(x^2+2^{j-1}x)$ so $K' = 0$. $z(x+y+z) = J'y^2+x^2+2^{j-1}x = Ux^2 + V(y^2+2^{j-1}x)$ so $J = J' = 1$. Then $y(x+y+z) \notin \langle x+y+z\rangle$.

(C) Lemma 17, (3) or (4), $m = r$. By assumption all intersections are one dimensional. If there is a pair of generators with squares equal then we may rename the generators so that $x^2 = y^2$. Then (A) holds, which was shown to be impossible for $m = r$. Thus (3) or (4) of Lemma 17 holds in $\langle x,y\rangle$, in $\langle x,z\rangle$, and in $\langle y,z\rangle$. Change x and y so that $2^{m-1}y = x^2+2^{j-1}x$, $xy = yx = 0$. Suppose $\langle x\rangle \cap \langle y\rangle \cap \langle z\rangle \neq 0$. Then $z^2 = 2^{m-1}y$, $xz = zx = yz = zy = z^2$. Then $x(y+z) \notin \langle y+z\rangle$. Thus $\langle x\rangle \cap \langle y\rangle \cap \langle z\rangle = 0$ and so by Lemma 17 on $\langle y,z\rangle$ one of the following holds:

(a) $z^2 = y^2+2^{m-1}y$. Then $(z+y)^2 = 2^{m-1}y \in \langle x\rangle$ so $\langle x,y,z\rangle = \langle x,y,z+y\rangle$ is not a v-ring.

(b) $z^2+2^{r-1}z = y^2$. Then $(z+y)^2 + 2^{r-1}(z+y) = 2^{m-1}y \in \langle x\rangle$ so $\langle x,y,z\rangle = \langle x,y,z+y\rangle$ is not a v-ring.

(c) $2^{r-1}z \in \langle y\rangle$.

Thus (c) holds, and dually $2^{r-1}z \in \langle x\rangle$, so $\langle x\rangle \cap \langle y\rangle \cap \langle z\rangle \neq 0$ and so $\langle x,y,z\rangle$ is not a v-ring.

(D) $m > r$, $\langle x\rangle \cap \langle y\rangle$ is two dimensional. By Lemma 10 $\langle x\rangle \cap \langle z\rangle$ and $\langle y\rangle \cap \langle z\rangle$ are one dimensional. Let $y^2 = Ax^2 + Bp^{j-1}x$, $p^{m-1}y = Cx^2 + Dp^{j-1}x$, $C \neq 0$, $AD \neq BC$, $xy = Fx^2 + Gp^{j-1}x$, $yx = F'x^2 + G'p^{j-1}x$. Since $j = m > r$ we have $z^2 \in \langle x\rangle$ so let $z^2 = Ex^2 + E'p^{j-1}x$, $xz = Hz^2$, $zx = H'z^2$, $yz = Kz^2$, $zy = K'z^2$. By Lemma 17 on $\langle x,z\rangle$ we have $1+T(H+H'+T)E$ is never zero. Since y cannot be replaced by a type I generator the determinant formed by the four coefficients below must never be zero: $(y+Sx+Tz)^2 = [A+S^2+T^2E+S(F+F')+TE(K+K')+STE(H+H')]x^2 + [B+T^2E'+S(G+G')+TE'(K+K')+STE'(H+H')]p^{j-1}x$. $p^{m-1}(y+Sx+Tz) = [C]x^2+$

$[D+S]p^{j-1}x$. Thus condition (4) of the conclusion holds.

(E) $m = r$, $\langle x\rangle \cap \langle y\rangle$ is two dimensional. By replacing y by the generator $\bar{y} = y - Dx$ we may assume that $D = 0$, so $B \neq 0$. By Lemma 10 $\langle x\rangle \cap \langle z\rangle$ and $\langle y\rangle \cap \langle z\rangle$ are one dimensional. If $p \neq 2$ then $z^2 \in \{x^2\}$, $z^2 \in \{y^2\}$, contradicting $B \neq 0$. Thus $p = 2$. We have $2^{m-1}y = x^2$, $y^2 = Ax^2 + 2^{j-1}x$. The condition on the cubic in Lemma 18 becomes $(F+F')+(G+G')+A = 1$. We shall consider several cases, showing that none of them is possible.

(a) $z^2 = x^2$. Then $z^2 = 2^{m-1}y$ so $yz = zy = z^2$, $xz+zx = z^2$ so we may assume $xz = z^2$, $zx = 0$. Suppose first that $A = 0$. Then $x(y+z) = (F+1)x^2+G2^{j-1}x = V(x^2+2^{j-1}x)$ since $2^{r-1}z \notin \langle x,y\rangle$. Thus $F+G = 1$. Considering $(y+z)x$ shows that $F' = G'$. Then $x(x+y+z) = Fx^2 + G2^{j-1}x = V((1+F+F')x^2 + (1+G+G')2^{j-1}x)$ so $F' = G' = 1$. Then considering $(x+y+z)x$ shows that $F = 0$, $G = 1$. Then $(x+y+z)y \notin \langle x+y+z\rangle$. Suppose on the other hand that $A = 1$. $x(y+z) = (F+1)x^2 + G2^{j-1}x = V2^{j-1}x$ and $(y+z)x = F'x^2 + G'2^{j-1}x$ show that $F = 1$, $F' = 0$. Since $(F+F')+(G+G')+A = 1$ we have $G+G' = 1$. Then $x(x+y+z) = x^2 + G2^{j-1}x = Vx^2$ so $G = 0$, $G' = 1$. Then $y(x+y+z) \notin \langle x+y+z\rangle$.

(b) $z^2 = 2^{j-1}x$. Then $xz = zx = z^2$. Suppose first that $A = 0$. Then $z^2 = y^2$ so we may assume $yz = z^2$, $zy = 0$. $x(y+z) = Fx^2 + (G+1)2^{j-1}x = V(2^{j-1}x)$ so $F = 0$. Similarly $F' = 0$. Then $G+G' = 1$. $x(x+y+z) = x^2 + (G+1)2^{j-1}x = V(x^2)$ so $G = 1$. Similarly $G' = 1$, contradicting $G+G' = 1$. On the other hand assume that $A = 1$. Then $z^2 = y^2 + 2^{m-1}y$ so $yz = zy$. Then $x(y+z) = Fx^2 + (G+1)2^{j-1}x = V(x^2)$ so $G = 1$. Similarly $G' = 1$. Then $F = F'$. Then $(x+y+z)^2 = 0$

so x may be replaced by a type I generator.

(c) $z^2 = x^2 + 2^{j-1}x$. Then $xz = zx$ and so $\bar{z} = z+x$ satisfies $\bar{z}^2 = 2^{j-1}x$, which is (b).

(d) $2^{r-1}z \in \langle x \rangle$. By Lemma 10 this is impossible.

(e) $z^2 + 2^{r-1}z = 2^{j-1}x$. Then $xz = zx = 0$. If $A = 1$ then $z^2 + 2^{r-1}z = y^2 + 2^{m-1}y$, which is impossible. Thus $A = 0$. Then $z^2 + 2^{r-1}z = y^2 = yz = zy$. $x(y+z) = Fx^2 + G2^{j-1}x = U[2^{m-1}(y+z) + (y+z)^2]$ since $z^2 + 2^{r-1}z$ is the only non-zero element in $\langle z \rangle \cap \langle x,y \rangle$. Then $Fx^2 + G2^{j-1}x = Ux^2$ so $G = 0$. Similarly $G' = 0$. Then $F+F' = 1$. Then $x(x+y+z) = (F+1)x^2 = U(2^{j-1}x+x^2)$, so $F = 1$. Similarly $F' = 1$, contradicting $F+F' = 1$.

(f) $z^2 + 2^{r-1}z = x^2$. Then $xz = zx$, and so $\bar{z} = z+x$ satisfies $(\bar{z})^2 + 2^{r-1}(\bar{z}) = 2^{j-1}x$, which is (e).

This completes the proof of Lemma 24.

<u>Theorem 8</u>: If the group direct sum decompositions of a nil p-v-ring involve a minimum of three type II generators, then under the notation of section V the ring is isomorphic to a ring $\mathcal{R}$ satisfying one of the following conditions, where $\mathcal{N}$ is a (null) ring annihilating $\mathcal{R}$, and char $\mathcal{N} < p^j$.

(1) $\mathcal{R} = \{x,y,z\} \dotplus \mathcal{N}$, $\langle x,y,z \rangle$ satisfies condition (1), Lemma 24, and $x^2 - p^{j-1}x$ is any element of $\mathcal{R}$ not in $\{x\}$ which annihilates $\mathcal{R}$, char $(x^2 - p^{j-1}x) = p$.

(2) $\mathcal{R} = \langle x,y,z \rangle \oplus \mathcal{N}$, $\langle x,y,z \rangle$ satisfies one of conditions (2), (3), (4), Lemma 24.

<u>Proof</u>: Consider a ring $\langle u,x,y,z \rangle$. Assume first that $a \geq j$.

If $\langle x\rangle \cap \langle y\rangle$ is one dimensional then Lemma 24 implies $y^2 \in \{x\}$ so $\langle u,x,y\rangle$ does not satisfy Lemma 19. If $\langle x\rangle \cap \langle y\rangle$ is two dimensional then Lemma 20 on $\langle u,x,y\rangle$ implies $j > m$, $y^2 = Ax^2$, so $\langle x,y,z\rangle$ does not satisfy Lemma 24.

Thus $a < j$. If $b > 0$ then Lemma 21 on $\langle u,x,y\rangle$ shows that $\langle x\rangle \cap \langle y\rangle$ is one dimensional and $y^2 \notin \{x\}$. Thus $\langle x,y,z\rangle$ does not satisfy Lemma 24. Thus $b = 0$, and by Lemma 21 u annihilates $\langle u,x,y,z\rangle$.

The proof of the Theorem is now immediate.

Theorem 9: If a nil p-v-ring has an additive group direct sum decomposition, then it has a decomposition involving no more than three type II generators.

Proof: We first show it is impossible to have a nil p-v-ring $\langle x,\ y,\ z,\ z^*\rangle$, $j \geq m \geq r \geq r^*$, $n = s = s^* = 0$. For suppose such existed. If $\langle x\rangle \cap \langle y\rangle$ were one dimensional then by Lemma 24 on $\langle x,y,z\rangle$ and on $\langle x,y,z^*\rangle$ we would have $\{z^{*2}\} = \{z^2\} = \{y^2\} = \{p^{j+k-1}x\}$. Then $\langle y,z,z^*\rangle$ does not satisfy Lemma 24 (in (4), $S = -D$ makes the cubic zero). Thus $\langle x\rangle \cap \langle y\rangle$ is two dimensional, so $\langle y\rangle \cap \langle z\rangle$ is one dimensional, so Lemma 24 on $\langle y,z,z^*\rangle$ implies $m > r$, $\{z^{*2}\} = \{z^2\} = \{p^{m-1}y\}$. Also $\langle x\rangle \cap \langle z\rangle$ is one dimensional so Lemma 24 on $\langle x,z,z^*\rangle$ implies $\{z^2\} = \{p^{j+k-1}x\}$. Thus $\{p^{m-1}y\} = \{p^{j+k-1}x\}$, which is impossible.

To show that a nil p-v-ring need not have an infinite number of type II generators recall that in the proofs of the preceding lemmas whenever a type II generator x was replaced by a type I generator of the form $x + Sy + Tz$ where y and z were of type II then it was always the generator of maximum characteristic which was replaced. Thus if a nil p-v-ring has more than three type II generators then by selecting three of minimum characteristic and taking linear combinations using only these three it follows that all other generators of type II may be replaced by generators of type I.

X. SUFFICIENCY OF CONDITIONS

Theorem 10: A nil p-v-ring which may be decomposed as an additive group direct sum of cyclic groups must, using the notation of section V, be isomorphic to a homomorph of a subring of one of the following rings $\mathcal{R}$. Conversely all homomorphs of subrings of the following rings are nil p-v-rings. $\mathcal{N}$ is a (null) p-ring which annihilates $\mathcal{R}$.

(1) $\mathcal{R} = \{u\} \dotplus \{x,y\} \dotplus \mathcal{N}$, $a \geq j \geq m$, $k = n = 0$, $ux = xu = uy = yu = 0$, $y^2 = Ax^2$, $xy = Fx^2$, $yx = F'x^2$, $1+T(F+F')+T^2A$ is never zero, x^2 is any element of $\mathcal{R}$ with characteristic p which annihilates $\mathcal{R}$. If $b > 0$ then char $\mathcal{N} \leq p^a$.

(2) $\mathcal{R} = \langle u,x \rangle \oplus \mathcal{N}$, $j = a+1$, $b = 1$, $p^a u = A(x^2 - p^{j-1}x) + Bp^{j+k-1}x$, $A \neq 0$, $ux = Hp^a u$, $xu = H'p^a u$, $1+T[A(H+H'+T) + (Bp^k - A)]$ is never zero, and char $\mathcal{N} < p^j$.

(3) $\mathcal{R} = \langle u,x,y \rangle \oplus \mathcal{N}$, $a = j > m$, $b = k = n = 0$, $p^{a-1}u = Cy^2 = C(Ax^2 + Bp^{j-1}x)$, $A \neq 0$, $B \neq 0$, $C \neq 0$, $ux = Hp^{a-1}u$, $xu = H'p^{a-1}u$, $B + A(H+H') = 0$, $uy = -yu \in \{p^{a-1}u\}$, $xy = Fy^2$, $yx = F'y^2$, $1+T(F+F'+T)A$ is never zero, and char $\mathcal{N} < p^j$.

(4) $\mathcal{R}$ satisfies Theorem 8.

(5) $\mathcal{R}$ satisfies (12) or (13) of Theorem 7.

(6) $p = 3$, $\mathcal{R}$ satisfies (8), Theorem 6.

(7) $p = 2$, $\mathcal{R}$ satisfies one of (9), Theorem 6, (6), (7), (8), or (9), Theorem 7.

Proof: It is not difficult to show that rings satisfying Theorems 5, 6, 7, and 8 satisfy the conclusion of the Theorem.

Since subrings and homomorphs of v-rings are again v-rings for the converse it is sufficient to show that rings satisfying conditions (1) through (7) are v-rings. To do this we need only show that a subring generated by a single element w is closed under multiplication by the generating elements u, v, x, y, z. Only multiplication on the left will be considered; multiplication on the right is similar. We consider each of conditions (1) through (7) in turn.

(1) If $b = 0$ then by the proof of Theorem 3 $\mathcal{R}$ is a v-ring. Assume that $b > 0$, so char $\mathcal{N} \leq p^a$. Let $w = Ru+Sx+Ty+n$, $n \in \mathcal{N}$. Then $uw = p^a w$. If p divides both S and T then $xw = yw = 0$, so $\langle w \rangle$ is an ideal. Otherwise, since $1+T(F+F')+T^2A$ is never zero we have $x^2 \in \{(Sx+Ty)^2\}$, $(Sx+Ty)^2 = w^2 - p^a Rw$, and certainly $xw, yw \in \{x^2\}$, so again $\langle w \rangle$ is an ideal.

(2) Let $w = Ru+Sx+n$, $n \in \mathcal{N}$. If p divides S it suffices to show that $Rp^a u \in \langle w \rangle$ and $Sp^{j-1}x \in \langle w \rangle$. If p also divides R then $p^{j-1}w = Sp^{j-1}x$, and $Rp^a u = 0$, so $\langle w \rangle$ is an ideal. If p does not divide R then $w^2 - Sp^{j-1}w = R^2 p^a u$, so $p^a u \in \langle w \rangle$. Then $p^{j-1}w = Rp^a u + Sp^{j-1}x$, so it follows that $\langle w \rangle$ is an ideal. Now suppose that p does not divide S. If p divides R it suffices to show that $x^2 \in \langle w \rangle$. But $w^2 = S^2 x^2$. Thus $\langle w \rangle$ is an ideal. If p divides neither R nor S then $1+T[A(H+H'+T)+(Bp^k-A)]$ never zero means that w is an element of type II. Thus both $x^2 - p^{j-1}x$ and $p^{j+k-1}x$ are in $\langle w \rangle$. Then $p^a u$ is in $\langle w \rangle$. Then x^2 is in $\langle w \rangle$ since $w^2 = S^2 x^2 + (\ldots)p^a u$. Thus $\langle w \rangle$ is an ideal.

(3) Let $w = Ru+Sx+Ty+n$, $n \in \mathfrak{N}$, and suppose first that p divides S. It suffices to show that $Rp^{a-1}u$ and Ty^2 are in $\langle w\rangle$. But $p^{a-1}w = Rp^{a-1}u$ and $w^2 = T^2y + (\ldots)Rp^{a-1}u$, so (since char $y^2 = p$) Ty^2 and $Rp^{a-1}u$ are in $\langle w\rangle$, so $\langle w\rangle$ is an ideal. Now suppose that p does not divide S. Then $Aw^2 + BSp^{j-1}w = [S^2+ST(F+F'+T)A]y^2 \neq 0$ since $1+T(F+F'+T)A$ is never zero, so y^2 is in $\langle w\rangle$. Then $p^{j-1}w - RCy^2 = Sp^{j-1}x$. Then x^2 is in $\langle w\rangle$, and it follows that $\langle w\rangle$ is an ideal.

(4) Let $w = Sx+Ty+Rz+n$, $n \in \mathfrak{N}$. First suppose that p does not divide S. If (1) of Lemma 24 holds then $p^{j+k-1}w = Sp^{j+k-1}x$ and $w^2 = S^2x^2 + (\ldots)p^{j+k-1}x$, from which it follows that $\langle w\rangle$ is an ideal. The conditions of Lemma 24 insure that x cannot be replaced by a type I generator of the form $x+Ty+Rz$, and so w is of type II. Then $x^2-p^{j-1}x$ and $p^{j+k-1}x$ are in $\langle w\rangle$. The only remaining verification to insure that $\langle w\rangle$ is an ideal is to show that in (3) x^2 is in $\langle w\rangle$. But $w^2 = S^2x^2+(\ldots)p^jx$, so x^2 is in $\langle w\rangle$ and so $\langle w\rangle$ is an ideal. Now suppose that p divides S. Suppose p also divides T. Then $xw = Sp^{j-1}x = p^{j-1}w$, or else (1) of Lemma 24 holds with $j = m$, $k = 1$, and p does not divide R, $m = r$. In that case $w^2 = R^2z^2 = R^2EBp^jx$, so again xw is in $\langle w\rangle$. To show that yw, zw are in $\langle w\rangle$ it suffices to show that Rz^2 is in $\langle w\rangle$. But $w^2 - Sp^{j-1}w = R^2z^2$, so $\langle w\rangle$ is an ideal. We may now suppose that p divides S, p does not divide T. We consider the cases of Lemma 24 separately. (1) $w^2 - Sp^{j-1}w = (Ty+Rz)^2$ so y^2 and thus yw, zw are in $\langle w\rangle$. If $j = m$ then also xw is in $\langle w\rangle$.

If $j > m$ then $xw = Sp^{j-1}x + (\ldots)y^2$, and $p^{j-1}w = Sp^{j-1}x$, so again $\langle w\rangle$ is an ideal. (2), (3) As in (1) y^2 is in $\langle w\rangle$. $p^{m-1}w = Sp^{j+k-2}x + Tp^{m-1}y$, so both y^2 and $p^{m-1}y$ are in $\langle w\rangle$. It follows that $\langle w\rangle$ is an ideal. (4) Since z^2 is in $\langle y\rangle$, $Ty+Rz$ is of type II, and $w^2 = (Ty+Rz)^2$, $p^{m-1}w = p^{m-1}(Ty+Rz) = Tp^{m-1}y$, it follows that y^2 and $p^{m-1}y$ are in $\langle w\rangle$, and from this that $\langle w\rangle$ is an ideal.

(5) This case is entirely similar to (4).

(6) Let $w = Ru+Sv+Tx+n$, $n \in \mathfrak{N}$, and suppose first that 3 divides T. If 3 also divides S then w annihilates $\mathfrak{R}$. Otherwise $vw = S3^c v = Sw^2$. Thus $\langle w\rangle$ is an ideal. Now suppose 3 divides S. Then $uw = vw = 0$, and $xw = Tx^2 = Tw^2$. Thus $\langle w\rangle$ is an ideal. Now suppose 3 divides R. Then $uw = 0$, $vw = S3^c v = 3^c w$, and $xw = Tx^2 = Tw^2 - TS3^c w$, so $\langle w\rangle$ is an ideal. Finally suppose that 3 divides none of R, S, T. Then $w^2 = 3^c v + x^2 = \pm 3^c u$, $3^c w = R3^c u + S3^c v$, so $3^c u$, $3^c v$, and x^2 are in $\langle w\rangle$, so $\langle w\rangle$ is an ideal.

(7) Theorem 6: (9). Let $w = Ru+Sv+Tx$. First suppose that 2 divides S. Since $vw = 0$, $uw = Tux$, $xw = Rxu + Tx^2$, and $2^c w = R2^c u$, we need only show that Tx^2 is in $\langle w\rangle$. If 2 does not divide R then $2^c w = x^2$ so $\langle w\rangle$ is an ideal. If 2 divides T then $Tx^2 = 0$ so $\langle w\rangle$ is an ideal. If 2 divides R but does not divide T then $w^2 = x^2$ so $\langle w\rangle$ is an ideal. Now suppose that 2 does not divide S. If 2 divides T then $w^2 = 2^c v$, $2^c w = R2^c u + 2^c v$, so $2^c v$ and $R2^c u$ are in $\langle w\rangle$, from which it follows that $\langle w\rangle$ is an ideal. If 2 divides R then $2^c w = 2^c v$ and $w^2 - 2^c v = Tx^2$, from which it follows that $\langle w\rangle$ is an ideal. Finally,

if 2 divides none of R,S,T then $w^2 = 2^c v + x^2 + ux + xu = 2^c v$, and $2^c w = 2^c u + 2^c v$, so $2^c v$ and $2^c u = x^2$ are in $\langle w\rangle$, so $\langle w\rangle$ is an ideal.

(7) Theorem 7: (6). Let $w = Rx+Sy+n$, $n \in \mathcal{N}$. If 2 divides R then $xw = 0$, $yw = Sy^2 = w^2$, and so $\langle w\rangle$ is an ideal. If 2 divides S then $yw = 0$, $xw = Rx^2 = w^2$, and so $\langle w\rangle$ is an ideal. If 2 divides neither R nor S then $yw = y^2 = 2^{j-1}w$, $xw = x^2 = w^2 + 2^{j-1}w$. Thus $\langle w\rangle$ is an ideal.

(7) Theorem 7: (7). Let $w = Ru+Sx+Ty+n$, $n \in \mathcal{N}$. It is sufficient to show that $R2^a u$, $S2^a u$, Sx^2, Sy^2, and Ty^2 are in $\langle w\rangle$. If 2 divides R and S then $w^2 = T^2y^2$, so $\langle w\rangle$ is an ideal. If 2 divides R but not S then $2^{j-1}w = S2^{j-1}x$, $w^2 = S^2x^2+(\ldots)2^{j-1}x$, from which it follows that all the above elements are in $\langle w\rangle$. If 2 divides S but not R then $w^2 = 2^a u + T^2y^2$ and $2^a w = 2^a u + S2^a x$, so $\langle w\rangle$ is an ideal unless $j = a+2$ and 4 does not divide S. Then $2^a w = y^2$, so again $\langle w\rangle$ is an ideal. Suppose 2 divides neither R nor S. Then $2^{j-1}w = 2^{j-1}x + 2^{j-1}u$ and $w^2 = x^2 + 2^{j-1}u$, so $x^2 - 2^{j-1}x$ and $2^{j+k-1}x$ are in $\langle w\rangle$, so $2^a u$ is in $\langle w\rangle$, so x^2 is in $\langle w\rangle$ and $\langle w\rangle$ is an ideal.

(7) Theorem 7: (8). Let $w = Ru+Sx+Ty+n$, $n \in \mathcal{N}$. It is sufficient to show that $R2^{a-1}u$, Sx^2, and Tx^2 are in $\langle w\rangle$. But $w^2 = RS2^{a-1}u + (S^2+ST+T^2)x^2$ and $2^{a-1}w = R2^{a-1}u + S2^{j-1}x = (R+S)2^{a-1}u + Sx^2$. It is now an easy matter to check that the above elements are in $\langle w\rangle$.

(7) Theorem 7: (9). This is similar to case (6) with $p = 3$ replaced by $p = 2$.

REFERENCES

[1] F. Szász. "Die Ringe, deren endlich erzeugbare echte Unterringe Hauptrechtsideale sind." *Acta. Math. Acad. Sci. Hungar.* 13(1962): 115 - 132.

[2] L. Redei. "Vollidealringe im Weiterin Sinn, I." *Acta. Math. Acad. Sci. Hungar.* 3(1952): 243 - 268.

[3] P. A. Freĭdman. "Kol'tsa s idealizatoriym usloviem, II." *Uchenye Zapiski Ural'skogo Gosudarstvennogo Universiteta.* 2(1959): 35 - 48.

[4] I. Kaplansky. *Infinite Abelian Groups.* Ann Arbor: University of Michigan Press, 1954.

For a complete bibliography of related papers see [1].