TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 331, Number 1, May 1992

THE STRUCTURE OF RINGS IN SOME VARIETIES WITH DEFINABLE PRINCIPAL CONGRUENCES

G. E. SIMONS

ABSTRACT. We study varieties of rings with identity that satisfy an identity of the form $xy = yp(x, y)$, where every term of the polynomial p has degree greater than one. These varieties are interesting because they have definable principal congruences and are residually small. Let $\mathscr{V}$ be such a variety. The subdirectly irreducible rings in $\mathscr{V}$ are shown to be finite local rings and are completely described. This results in structure theorems for the rings in $\mathscr{V}$ and new examples of noncommutative rings in varieties with definable principal congruences. A standard form for the defining identity is given and is used to show that $\mathscr{V}$ also satisfies an identity of the form $xy = q(x, y)x$. Analogous results are shown to hold for varieties satisfying $xy = q(x, y)x$.

1. INTRODUCTION

The concept of definable principal congruences originated in universal algebra. A variety $\mathscr{V}$ of (universal) algebras has definable principal congruences if there is a first-order formula in the language of $\mathscr{V}$ that defines principal congruences for all algebras in $\mathscr{V}$. There are a number of results connecting definable principal congruences with the number of subdirectly irreducible algebras in a variety, and with the existence of a finite basis for a variety. For example, McKenzie [M78] proved that a variety (of finite type) with definable principal congruences and a bound on the size of its subdirectly irreducible algebras is finitely axiomatizable and used this result to prove that paraprimal varieties are finitely axiomatizable. It was shown by Tulipani [T] that a variety with definable principal congruences has definable n-generated congruences for every positive integer n.

An interesting question that has stimulated further work is whether the variety generated by a finite algebra must have definable principal congruences. This has been investigated by several authors for different kinds of algebras. McKenzie [M78] showed that the only varieties of lattices with definable principal congruences are the two varieties of distributive lattices (all distributive lattices, all one-element lattices). Building on earlier work of Burris and Lawrence [BL79], Baker [B] showed that a locally finite variety of groups has definable

Received by the editors February 5, 1990.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 16A48; Secondary 08B99, 16A10, 16A38, 16A44.

Key words and phrases. Definable principal congruences, varieties of rings, subdirectly irreducible rings, finite local rings, residually small varieties.

0002-9947/92 $1.00 + $.25 per page

principal congruences if and only if it satisfies the identity $[x, y, x] = 1$. More recently, Kiss [K] has developed an algorithm that determines whether a congruence distributive variety generated by a finite algebra has definable principal congruences.

Less is known about varieties of rings with definable principal congruences. Since any variety of commutative rings has definable principal congruences, our interest is focussed on noncommutative rings in varieties with definable principal congruences. Burris and Lawrence [BL79] gave an example of a noncommutative ring that cannot be in any variety with definable principal congruences. Earlier work on varieties of rings with definable principal congruences [S83, S86] has shown that in a variety with definable principal congruences, rings that have certain 'nice' structural conditions, such as primitivity or primeness, must be commutative. However, an example of a noncommutative ring in a variety with definable principal congruences was given in [S83] and more examples appear in this paper.

This paper deals with the structure of rings in varieties that satisfy an identity of the form $xy = yp(x, y)$, where all terms of the polynomial p have degree greater than one. This condition on p excludes the variety of all commutative rings. These varieties have definable principal congruences and are also residually small, that is, there is a bound on the size of the subdirectly irreducible rings in the variety. We find the subdirectly irreducible rings in such a variety and use this information to get a structure theorem for the finite and semiperfect rings in the variety. We also obtain a standard form for the defining identity. This allows us to show that any such variety also satisfies an identity of the form $xy = p(x, y)x$. Similar results hold for varieties satisfying this form of identity.

2. Preliminaries

This section presents some results that are needed later and introduces notation used throughout the paper.

Throughout, the term 'ring' will mean 'ring with identity' and the term 'algebra' is used in its ring-theoretic sense. Since all our rings have an identity, the language of rings used is $\{+, -, \cdot, 0, 1\}$. The term 'polynomial' refers to a polynomial in this language. These can be regarded as (ordinary) polynomials in noncommuting indeterminates with integer coefficients. If R is a ring, then we use $V(R)$ for the variety of rings generated by R, $J(R)$ for the Jacobson radical of R, $P(R)$ for the prime radical of R, $Z(R)$ for the centre of R, $C(R)$ for the commutator ideal of R (the ideal generated by all commutators $[x, y]$ $(= xy - yx)$ in R), $\mathrm{Nil}(R)$ for the upper nil radical of R (the unique largest nil ideal of R) and $U(R)$ for the multiplicative group of units of R. If the context is clear, we often use just the abbreviations J, P, Z, or C. The two-sided ideal generated by an element $x \in R$ is denoted by either RxR or (x).

The fundamental criterion for determining whether a variety of rings has definable principal congruences is given in the following theorem.

Theorem 2.1 [BL79]. *If K is a class of rings, then $V(K)$ has definable principal congruences if and only if K satisfies an identity of the form*

$$\sum_{i=1}^{n} x_i y z_i = \sum_{i=1}^{k} r_i(\overline{x}, y, \overline{z}) y s_i(\overline{x}, y, \overline{z})$$

where n *and* k *are integers,* $n > k \geq 1$, $\overline{x} = (x_1, \ldots, x_n)$, $\overline{z} = (z_1, \ldots, z_n)$ *and* $r_i(\overline{x}, y, \overline{z})$, $s_i(\overline{x}, y, \overline{z})$, $1 \leq i \leq k$, *are polynomials.*

If a variety $\mathscr{V}$ of rings has definable principal congruences, then it satisfies an identity of the form given in the theorem and a first-order formula defining principal ideals (congruences) in $\mathscr{V}$ would be

$$\phi(x, y) := \exists x_1, \ldots, x_k, z_1, \ldots, z_k \left(x = \sum_{i=1}^{k} x_i y z_i \right).$$

If $R \in \mathscr{V}$ and $x, y \in R$, then $x \in RyR$ if and only if $\phi(x, y)$ holds. If R is a commutative ring then $V(R)$ has definable principal congruences, since $\sum_{i=1}^{2} x_i y z_i = 1y(\sum_{i=1}^{2} x_i z_i)$.

If a variety $\mathscr{V}$ of rings has definable principal congruences, then any ring $R \in \mathscr{V}$ will generate a variety with definable principal congruences, since $V(R) \subseteq \mathscr{V}$. Thus most of our results are stated for rings generating varieties with definable principal congruences. Some of the principal results about the structure of such rings are summarized in the following results. These results appear in [S83, S86].

Theorem 2.2. *Let* R *be a nontrivial ring. Then* $V(M_n(R))$ *does not have definable principal congruences if* $n \geq 2$.

This result is the key ingredient in proving most of the parts of the following theorem.

Theorem 2.3. *Let* R *be a ring. If* $V(R)$ *has definable principal congruences then*

(i) R *is a polynomial identity (PI) ring;*

(ii) *if* R *is primitive, then* R *is a field;*

(iii) *if* R *is semiprime, then* R *is commutative;*

(iv) *if* R *is an algebra over a field, then all idempotents of* R *are in the centre of* R;

(v) *if* R *is an algebra over an infinite field, then* R *is commutative.*

From these results, we can deduce the following theorem on the structure of any ring in a variety with definable principal congruences.

Theorem 2.4. *Suppose that* $\mathscr{V}$ *is a variety of rings with definable principal congruences and that* $R \in \mathscr{V}$. *Let* N *be the set of nilpotent elements of* R. *Then* N *is a two-sided ideal of* R, $N = \mathrm{Nil}(R)$, $C(R) \subseteq P(R) = N \subseteq J(R)$ *and* $R/J(R)$ *is a subdirect product of fields in* $\mathscr{V}$.

Proof. Since $\mathscr{V}$ has definable principal congruences, R/P is commutative, so $C \subseteq P$ and thus C is a nil ideal. Then N/C is an ideal of the commutative ring R/C, so N is a two-sided ideal of R. Clearly, N is the largest possible nil ideal of R, so $N = \mathrm{Nil}(R)$ and $N \subseteq J$. Since R is a PI-ring, $P = \mathrm{Nil}(R) = N$ [P, p. 40]. Finally, R/J is a subdirect product of its primitive images, which must be fields which are in $\mathscr{V}$. □

Corollary 2.5. *If $\mathscr{V}$ is a variety of rings with definable principal congruences, $R \in \mathscr{V}$ and $J(R)$ is nilpotent, then $J(R) = \mathrm{Nil}(R) = P(R) = \{x \in R | x$ is nilpotent$\}$.*

Corollary 2.6. *If $\mathscr{V}$ is a variety of rings with definable principal congruences and F is the (relatively) free ring in $\mathscr{V}$, then $J(F) = \{x \in F | x$ is nilpotent$\}$.*

Proof. Since F is a PI-ring, $J(F) = \mathrm{Nil}(F)$ [Ro, p. 134]. □

The following theorem is used in the next section of this paper, but is presented here because it can be applied in situations other than the one considered there.

Theorem 2.7. *Let $\mathscr{V}$ be a variety of rings with definable principal congruences and let R be a subdirectly irreducible ring in $\mathscr{V}$ with nonzero characteristic. If $C(R)J(R) = 0$, then R has no nontrivial idempotents.*

Proof. Suppose that e is an idempotent of R other than 0 or 1. Then eJ is a two-sided ideal of R, since for $x \in R$ and $j \in J$ we have $(xe-ex)j \in CJ = 0$, so $xej = exj \in eJ$. Similarly $(1-e)J$ is a two-sided ideal of R and since $eJ \cap (1-e)J = 0$, either $eJ = 0$ or $(1-e)J = 0$, as R is subdirectly irreducible.

Without loss of generality, suppose that $eJ = 0$. Then Re is a two-sided ideal of R, since for $r \in R$ we have $e(er - re) \in eC \subseteq eJ = 0$ and so $er = e^2r = ere \in Re$. Since R is subdirectly irreducible with nonzero characteristic, it has characteristic p^k for some prime p and positive integer k. Then $p \in J$ and $ep = pe \in eJ = 0$, hence $Re \cap Rp = 0$. Since $Re \neq 0$, we must have $Rp = 0$. Therefore R has characteristic p. Then R is an algebra over the field $GF(p)$ and so all idempotents of R are central. Thus e is a nontrivial central idempotent, but this is impossible since R is subdirectly irreducible. Therefore R has no nontrivial idempotents. □

3. Subdirectly irreducible rings in varieties satisfying $xy = yp(x, y)$

For the rest of the paper we consider varieties of rings satisfying an identity of the form $xy = yp(x, y)$, where p is a polynomial in which every monomial (term) has degree greater than one. Throughout this and the following sections, $\mathscr{V}$ will denote a variety of rings satisfying an identity of this form. The reason for this restriction is two-fold: we do not want to consider the identity $xy = yx$, since all varieties of commutative rings have definable principal congruences, and secondly, work of McKenzie [M82] shows that this condition guarantees the existence of a bound on the size of the subdirectly irreducible rings in the variety.

It is clear that $\mathscr{V}$ has definable principal congruences, either by noting that it satisfies $x_1yz_1 + x_2yz_2 = 1 \cdot y \cdot (p(x_1, y)z_1 + p(x_2, y)z_2)$ and then using Theorem 2.1 or by observing that for any $R \in \mathscr{V}$ and $y \in R$, the two-sided principal ideal RyR equals the right ideal yR, so the statement $\phi(x, y) := \exists z(x = yz)$ defines principal ideals in $\mathscr{V}$.

Theorem 3.1. *Let $R \in \mathscr{V}$. Then $J(R) = \{x \in R | x^2 = 0\}$ and $J(R)^2 = 0$.*

Proof. Substituting x for y in the identity for $\mathscr{V}$ gives an identity of the form $x^2 = x^3 f(x)$. Then $x^2(1 - xf(x)) = 0$, so if $x \in J$, then $x^2 = 0$. Conversely, if $x^2 = 0$, Theorem 2.4 shows that $x \in J$. Therefore $J(R) = \{x | x^2 = 0\}$.

If $x \in J$ and $y \in R$, then xy and $x(1+y)$ are in J, so $(x(1+y))^2 = 0 = x^2 + (xy)^2 + x^2 y + xyx = xyx$. If both $x, y \in J$, then $xy = yp(x, y)$ and every monomial of $yp(x, y)$ contains either x^2, y^2 or yxy and hence is 0. Therefore $J^2 = 0$. □

Corollary 3.2. *If $R \in \mathscr{V}$ then $C(R)J(R) = J(R)C(R) = 0$.*

Proof. By Theorem 2.4 $C \subseteq J$, so $CJ \subseteq J^2 = 0$ and $JC \subseteq J^2 = 0$. □

Theorem 3.3. *There is a finite bound on the size of the fields in $\mathscr{V}$ and there is an integer $m > 1$ such that $x = x^m$ is satisfied in all fields in $\mathscr{V}$.*

Proof. As before, $\mathscr{V}$ satisfies an identity of the form $x^2 = x^3 f(x)$ and the degree of $x^2 - x^3 f(x)$ bounds the size of the fields in $\mathscr{V}$. Thus there are only finitely many fields in $\mathscr{V}$, with finite orders $q_1, q_2, \ldots, q_k$, for some integer k. Any integer $m > 1$ such that $m \equiv 1 \pmod{q_i - 1}$ for $i = 1, 2, \ldots, k$ will give $x = x^m$ in all fields in $\mathscr{V}$. For example, $m = 1 + \operatorname{lcm}(q_1 - 1, \ldots, q_k - 1)$ is one solution. □

Theorem 3.4. *Let R be a subdirectly irreducible ring in $\mathscr{V}$. Then either $R \cong F$ or $R/J(R) \cong F$, where F is a field in $\mathscr{V}$.*

Proof. If $J = 0$, then R is a primitive ring, so by Theorem 2.3 it is a field. Suppose that $J \neq 0$. R must have nonzero characteristic since otherwise $\mathbf{Z}$ and $\mathbf{Z}/q\mathbf{Z} \cong GF(q)$ would be in $\mathscr{V}$ for all primes q, contrary to the preceding theorem. By Corollary 3.2, $CJ = 0$ and so Theorem 2.7 shows that R has no nontrivial idempotents.

R/J is a subdirect product of some set of fields $\{F_i | i \in I\}$ in $\mathscr{V}$. Let $\pi_i : R/J \to F_i$ be the ith projection map, for each $i \in I$. Suppose that for some $i \in I$, π_i is not an isomorphism. Then there is some $a \in R/J$ such that $a \neq 0$ and $\pi_i(a) = 0$. All fields in $\mathscr{V}$ satisfy $x^m = x$ for some $m > 1$, so a^{m-1} is a nontrivial idempotent of R/J which lifts to a nontrivial idempotent of R since $J^2 = 0$. This is a contradiction, so π_i must be an isomorphism and R/J is isomorphic to some field in $\mathscr{V}$. □

Theorem 3.5. *There is a finite bound on the size of the subdirectly irreducible rings in $\mathscr{V}$. If the largest field in $\mathscr{V}$ has q elements, then every subdirectly irreducible ring in $\mathscr{V}$ has at most q^2 elements. If $R \in \mathscr{V}$ is a subdirectly irreducible ring which is not a field, then $|R/J(R)| = |J(R)|$ and $|R| = |R/J(R)|^2$.*

Proof. Let R be a subdirectly irreducible ring in $\mathscr{V}$. If R is a field, then Theorem 3.3 gives a bound, say q, on the size of R. Suppose that R is not a field. By the previous theorem, R/J is isomorphic to a field in $\mathscr{V}$, so it has at most q elements. Choose a set of coset representatives $S = \{c_0, c_1, \ldots, c_t\}$ of J in R, with $c_0 \in J$. Since R is a local ring, $c_1, \ldots, c_t$ are all units in R. Let M be the unique minimal nonzero ideal of R and choose a nonzero element $m \in M$. Define a map $\gamma : J \to S$ as follows. First, put $\gamma(0) = c_0$. If $j \in J$ is not zero, then since $m \in (j)$, there exists some $x \in R$ with $m = jx$ by the definability of principal ideals in R. We have $x = c_i + y$ for some coset representative c_i and some $y \in J$, so $m = jx = j(c_i + y) = jc_i$, since

$jy \in J^2 = 0$. Put $\gamma(j) = c_i$, so that $m = j\gamma(j)$. Note that $c_i \neq c_0$, since $jc_0 \in J^2 = 0$. The map γ is well defined, since if $0 \neq j \in J$ and $jc_i = jc_k$ for $i \neq k$, then $j(c_i - c_k) = 0$. Now $c_i - c_k \notin J$, so it is a unit and therefore $j = 0$, a contradiction. Also γ is 1-1, since $\gamma(j_1) = \gamma(j_2) = c_i$ implies that $m = j_1c_i = j_2c_i$ and then $j_1 = j_2$ since c_i is a unit. Finally, γ is onto since $mc_i^{-1} \in M \subseteq J$ for $1 \leq i \leq t$ and clearly $\gamma(mc_i^{-1}) = c_i$. Therefore γ is a bijection, $|J| = |S| = |R/J|$ and $|R| = |R/J||J| = |J|^2 = |R/J|^2 \leq q^2$. □

As noted in the proof of Theorem 3.3, an upper bound for q is given by the degree of the identity $x^2 = x^3f(x)$ (that is, the degree of the polynomial $x^2 - x^3f(x)$) obtained by substituting x for y in $xy = yp(x, y)$.

The existence of a finite bound on the size of the subdirectly irreducible rings in $\mathscr{V}$ could have been stated earlier, since Theorem 3.1 of McKenzie's paper [M82] shows that $\mathscr{V}$ is residually small. Since $\mathscr{V}$ also has definable principal congruences, a result of Baldwin and Berman [BB] shows the existence of the finite bound, but does not determine the size of the bound.

Corollary 3.6. *Let R be a subdirectly irreducible ring in $\mathscr{V}$. If R is not a field, then $J(R)$ is the unique minimal nonzero ideal of R and is the only proper nonzero ideal of R.*

Proof. Suppose that R is subdirectly irreducible and is not a field. Then Theorem 3.4 shows that R is a local ring. As in the previous proof, let $S = \{c_0, \ldots, c_t\}$ be a set of coset representatives for J in R, let M be the unique minimal nonzero ideal of R and choose a nonzero element $m \in M$. Consider the set $mS = \{mc_0, \ldots, mc_t\}$. If $mc_i = mc_k$ and $i \neq k$, then $m(c_i - c_k) = 0$ and $c_i - c_k$ is a unit, since $c_i - c_k \notin J$. This means that $m = 0$, a contradiction. Therefore all the elements of mS are distinct and so $|mS| = |S| = |J|$ by the previous theorem. Since $mS \subseteq J$, we must have $mS = J$, but $mS \subseteq M$, so $J = M$ by the minimality of M. Since R is a local ring, J is both the maximal proper and minimal nonzero ideal of R. □

4. Finite local rings in $\mathscr{V}$

In this section we determine the structure of the finite local rings in $\mathscr{V}$, in particular the subdirectly irreducible rings in $\mathscr{V}$, and use this information to find a standard form for the identity defining $\mathscr{V}$. Throughout this section $\mathscr{V}$ has the same meaning as in the previous section.

Our starting point is a theorem of Wilson [W] that gives a way of representing any finite local ring using matrices. Wilson's theorem uses the Galois rings introduced by Raghavendran [R] and Janusz [J]. Galois rings are finite, local rings that can be viewed as a common generalization of finite fields and $\mathbf{Z}/p^n\mathbf{Z}$. We use the notation $GR(p^n, r)$ for the Galois ring $(\mathbf{Z}/p^n\mathbf{Z})[x]/(f)$, where f is a monic polynomial of degree r that is irreducible modulo p. This construction is independent of the choice of f (up to isomorphism). $GR(p^n, r)$ is commutative, has characteristic p^n, with the Jacobson radical of $GR(p^n, r)$ being $pGR(p^n, r)$ and $GR(p^n, r)/pGR(p^n, r) \cong GF(p^r)$. The following result comes from applying the methods used in the proof of Wilson's theorem to the special case of finite local rings with $J^2 = 0$.

Theorem 4.1. *Suppose that R is a finite local ring, with $R/J(R) \cong GF(p^r)$ and $J(R)^2 = 0$. Then either*

(a) *R has characteristic p and is isomorphic to the ring of all matrices of the form*

$$\begin{pmatrix} a & b_1 & b_2 & \cdots & b_n \\ 0 & \sigma_1(a) & 0 & \cdots & 0 \\ \vdots & \ddots & \sigma_2(a) & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \sigma_n(a) \end{pmatrix}$$

where $n \geq 0$, $a, b_1, \ldots, b_n \in GF(p^r)$ and $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(GF(p^r))$, or

(b) *R has characteristic p^2 and is isomorphic to the set of all objects of the form*

$$\begin{pmatrix} a & \phi(b_1) & \phi(b_2) & \cdots & \phi(b_n) \\ 0 & \sigma_1(\phi(a)) & 0 & \cdots & 0 \\ \vdots & \ddots & \sigma_2(\phi(a)) & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \sigma_n(\phi(a)) \end{pmatrix}$$

where $n \geq 0$, $a, b_1, \ldots, b_n \in GR(p^2, r)$,

$$\phi : GR(p^2, r) \to GR(p^2, r)/pGR(p^2, r) \cong GF(p^r)$$

is the canonical map and $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(GF(p^r))$. These objects form a ring when operations are performed with the preimages of objects in matrix rings over $GR(p^2, r)$ and then the quotient map ϕ is applied to all entries except those in the first column.

The next lemma simplifies the task of checking whether these finite local rings satisfy an identity of the form $xy = yp(x, y)$.

Lemma 4.2. *Let R be a finite local ring with $J(R)^2 = 0$. Then an identity of the form $xy = yp(x, y)$, where p is a polynomial, holds in R if and only if an identity of the form $xy = yq(x)$, where q is a polynomial, holds for all $x \in R$ and $y \in J$.*

Proof. Suppose that $xy = yp(x, y)$. If $y \in J$ then the product of y and any term of p containing a y equals 0, since $J^2 = 0$. Take $q(x) = p(x, 0)$, so that the terms of q are the terms of p containing only x's. Then $xy = yq(x)$ for all $x \in R$ and all $y \in J$.

For the converse, note that $U(R)$ is finite, so there is an integer $m \geq 1$ such that $y^m = 1$ for all $y \in U(R)$. Then $(1 - y^m)(xy - yq(x)) = 0$ for all $x, y \in R$, since either $y \in J$ and then $xy - yq(x) = 0$ or $y \in U(R)$ and then $1 - y^m = 0$. Rearranging the identity yields $xy = (1 - y^m)yq(x) + y^m xy$, which is of the required form. □

Theorem 4.3. *Let R be a finite local ring in $\mathscr{V}$, with $R/J(R) \cong GF(p^r)$. Then either*

(a) *R has characteristic p and is isomorphic to the ring of all matrices of the*

form

$$\begin{pmatrix} a & b_1 & b_2 & \cdots & b_n \\ 0 & \sigma(a) & 0 & \cdots & 0 \\ \vdots & \ddots & \sigma(a) & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \sigma(a) \end{pmatrix}$$

where $n \geq 0$, $a, b_1, \ldots, b_n \in GF(p^r)$ *and* $\sigma \in \mathrm{Aut}(GF(p^r))$, *or*

(b) R *has characteristic* p^2 *and is isomorphic to the set of all objects of the form*

$$\begin{pmatrix} a & \phi(b_1) & \phi(b_2) & \cdots & \phi(b_n) \\ 0 & \phi(a) & 0 & \cdots & 0 \\ \vdots & \ddots & \phi(a) & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \phi(a) \end{pmatrix}$$

where $n \geq 0$, $a, b_1, \ldots, b_n \in GR(p^2, r)$, *and*

$$\phi : GR(p^2, r) \to GR(p^2, r)/pGR(p^2, r) \cong GF(p^r)$$

is the canonical map. These objects form a ring as indicated before.

In either case, there are integers $m \geq 1$ *and* $k \geq 2$ *such that* R *satisfies*

$$(1 - y^m)(xy - yx^k) = 0, \quad \text{or} \quad xy = (1 - y^m)yx^k + y^m xy.$$

Proof. By the previous lemma, it is enough to check that $xy = yq(x)$ holds for all $x \in R$ and $y \in J$. We use the description of R given in Theorem 4.1. If R has characteristic p, then $J(R)$ consists of all matrices of the given form with zeros on the diagonal, i.e. $a = 0$. Substituting

$$x = \begin{pmatrix} a & b_1 & b_2 & \cdots & b_n \\ 0 & \sigma_1(a) & 0 & \cdots & 0 \\ \vdots & \ddots & \sigma_2(a) & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \sigma_n(a) \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 0 & c_1 & c_2 & \cdots & c_n \\ 0 & \ddots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

in $xy = yq(x)$ yields $ac_i = c_i q(\sigma_i(a)) = c_i \sigma_i(q(a))$ for all $a, c_i \in GF(p^r)$. Note that the diagonal entries of $q(x)$ are just q applied to the diagonal entries of x. If we let $c_i = 1$ then we have $a = \sigma_i(q(a))$ for all $a \in GF(p^r)$ and $i = 1, 2, \ldots, n$. Therefore $\sigma_1 = \sigma_2 = \cdots = \sigma_n$. Put $\sigma = \sigma_1$. Then $q(a) = \sigma^{-1}(a) = a^{p^t}$ for some integer t. Thus $xy = yx^{p^t}$ for all $x \in R$ and $y \in J$ and as in the lemma, we have $(1 - y^m)(xy - yx^k) = 0$, with $k = p^t$ and m equal to the exponent of $U(R)$.

The other case to be considered is when R has characteristic p^2. The computations are similar to the previous case. In this case, $J(R)$ consists of the objects of the form

$$\begin{pmatrix} pc & \phi(c_1) & \cdots & \phi(c_n) \\ 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

and from $xy = yq(x)$, with $y \in J$, we obtain $\phi(a) = \phi(q(a)) = q(\sigma_i(\phi(a))) = \sigma_i(\phi(q(a)))$ and so $\phi(a) = \sigma_i(\phi(a))$ for all $a \in GR(p^2, r)$. Thus σ_i is the identity map on $GF(p^r)$. If we take $q(a) = a^{p^r}$, then in $GR(p^2, r)$ we have $px = pq(x)$ and as before we have $(1 - y^m)(xy - yx^k) = 0$ with $k = p^r$ and m equal to the exponent of $U(R)$. □

Note that the rings given in case (b) are all commutative, while the rings given in case (a) are commutative if and only if the automorphism σ is the identity map. If σ is not the identity map, the rings in case (a) are new examples of noncommutative rings in a variety with definable principal congruences.

Corollary 4.4. *Let R be a subdirectly irreducible ring in $\mathscr{V}$. Then R is isomorphic to either*

(a) *$GF(q)$, for some prime power q.*

(b) *$GR(p^2, r)$, for some prime p and positive integer r, or*

(c) *the set of 2 by 2 matrices over $GF(q)$ of the form*

$$\begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix}$$

where $\sigma \in \mathrm{Aut}(GF(q))$ and q is a prime power.

Proof. By Theorems 3.4 and 3.5 the subdirectly irreducible rings in $\mathscr{V}$ are either finite fields or finite local rings with $J^2 = 0$. The finite local rings in $\mathscr{V}$ were described in the previous theorem and the only subdirectly irreducible rings of this form are listed in (b) and (c). In case (b), $J(R) = (p)$, while in case (c), $J(R) = (e_{12})$. In both cases, $J(R)$ is the only nonzero proper ideal of the ring. □

We will denote by $S(p^r, t)$ rings of the kind described in part (c) of the last theorem, where the entries of the matrices are in $GF(p^r)$ and the automorphism σ of $GF(p^r)$ is given by $\sigma(x) = x^t$. This implies that $t \equiv p^k \pmod{p^r - 1}$ for some integer k. Note that $S(p^r, t) \cong GF(p^r)[x; \sigma]/(x^2)$, a quotient of the skew polynomial ring.

We need a lemma from elementary number theory in the proof of the next theorem. The proof of the lemma, an induction on the number of congruences, is omitted.

Lemma 4.5. *The system of k linear congruences $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, k$, has a solution for x if and only if $a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$, for all $i \neq j$.*

Theorem 4.6. *There are integers $m \geq 1$ and $k \geq 2$ such that $\mathscr{V}$ satisfies the identity*

$$xy = y^m xy + y(1 - y^m)x^k.$$

Proof. It suffices to show that all subdirectly irreducible rings in $\mathscr{V}$ satisfy such an identity. They all satisfy an identity of this form, so we have to find values of m and k such that one identity holds in all the subdirectly irreducible rings in $\mathscr{V}$. There is an identity $xy = yq(x)$ that holds in every subdirectly irreducible ring $R \in \mathscr{V}$ when $x \in R$ and $y \in J(R)$. We claim that there is an integer $k > 1$ such that we can choose $q(x) = x^k$. If R is a subdirectly irreducible ring in $\mathscr{V}$ which is not a field, then it is a local ring with quotient field $R/J(R) \cong GF(p^r)$, for some prime p. The proof of Theorem 4.3 shows that $q(x)$ must

be an automorphism of $GF(p^r)$, so it has the form $x^{p^n} + (x^{p^r} - x)s(x)$, for some polynomial $s(x)$. Therefore, if $q(x) = x^k$, then k must be a solution to the congruence $k \equiv p^n \pmod{p^r - 1}$, where the value of n depends on the automorphism.

There are t subdirectly irreducible rings $R_1, \ldots, R_t$ in $\mathscr{V}$ which are not fields, with $R_i/J(R_i) \cong GF(q_i)$, where $q_i = p_i^{r_i}$ and p_i is prime, and $q(x) = x^{k_i} + (x^{q_i} - x)s_i(x)$, where $k_i = p_i^{n_i}$. This implies that $k_i \equiv k_j \pmod{\gcd(q_i - 1, q_j - 1)}$ for all $i \neq j$. To prove this, suppose that $i \neq j$ and let $g = \gcd(q_i - 1, q_j - 1)$. Then $x^g - 1$ divides both $x^{q_i} - x = x(x^{q_i - 1} - 1)$ and $x^{q_j} - x = x(x^{q_j - 1} - 1)$, so it divides $q(x) - x^{k_i} - (q(x) - x^{k_j}) = x^{k_i}(x^{k_j - k_i} - 1)$ (assuming that $k_j > k_i$; otherwise interchange k_i and k_j). Thus $x^g - 1$ divides $x^{k_j - k_i} - 1$, (or $x^{k_i - k_j} - 1$) so g divides $k_j - k_i$ (or $k_i - k_j$). In either case, $k_i \equiv k_j \pmod{\gcd(q_i - 1, q_j - 1)}$, for all $i \neq j$.

Thus by Lemma 4.5 the system of congruences $k \equiv k_i \pmod{q_i - 1}$, $i = 1, 2, \ldots, t$, has a solution for k. Therefore we can choose $q(x) = x^k$ and so $xy = yx^k$ for all $x \in R$ and $y \in J(R)$, where R is any subdirectly irreducible ring in $\mathscr{V}$.

Choose m to be the least common multiple of the exponents of the groups of units of the subdirectly irreducible rings in $\mathscr{V}$. Then $(1 - y^m)(xy - yx^k) = 0$ holds in all subdirectly irreducible rings in $\mathscr{V}$, since these rings are all finite, local rings and an element y is either a unit, in which case $1 - y^m = 0$, or is in $J(R)$, in which case $xy - yx^k = 0$ for any x. Thus $xy = (1 - y^m)yx^k + y^m xy$ holds in all subdirectly irreducible rings in $\mathscr{V}$, so it holds in all rings in $\mathscr{V}$. □

It is possible to determine exactly those subdirectly irreducible rings which can satisfy the kind of identity given in this theorem. A lemma about the exponent of $U(S(p^r, t))$ is required.

Lemma 4.7. *The exponent of* $U(S(p^r, t))$ *is* $p(p^r - 1)$.

Proof. Let $R = S(p^r, t)$, $q = p^r$ and let the image of $x \in R$ under the quotient map $R \to R/J$ be $\overline{x}$. $R/J \cong GF(q)$, so if $y \in U(R)$ then $\overline{y}^{q-1} = 1$. Thus $y^{q-1} = 1 + j$ for some $j \in J$. Then $y^{p(q-1)} = (1 + j)^p = 1 + j^p = 1$, since R has characteristic p and $J^2 = 0$, so the exponent of $U(R)$ divides $p(q - 1)$. To see that the exponent is exactly $p(q - 1)$, note that there are elements of order p and $q - 1$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^t \end{smallmatrix}\right)$ respectively, where α is a generator of $U(R/J)$. □

Theorem 4.8. *Consider the equation*

$$xy = y^m xy + y(1 - y^m)x^k$$

for integers $m \geq 1$ *and* $k \geq 2$. *Let* p *be a prime and let* r *and* t *be positive integers. Then*

(a) $GF(p^r)$ *satisfies this equation if and only if* $p^r - 1$ *divides* m *or* $k \equiv 1 \pmod{p^r - 1}$,

(b) $GR(p^2, r)$ *satisfies this equation if and only if* $p^r - 1$ *divides* m *and* $k \equiv 1 \pmod{p^r - 1}$, *and*

(c) $S(p^r, t)$ *satisfies this equation if and only if* $p^r - 1$ *divides* m, $kt \equiv 1 \pmod{p^r - 1}$ *and if* $k \not\equiv 1 \pmod{p^r - 1}$, *then* $p(p^r - 1)$ *divides* m.

Proof. Rewrite the equation in the form $(1 - y^m)(xy - yx^k) = 0$ and let $q = p^r$. For $GF(q)$, this equation is equivalent to $y(1 - y^m)x(1 - x^{k-1}) = 0$, so if $x \neq 0$

and $y \neq 0$ then either $x^{k-1} = 1$ or $y^m = 1$. Since we can choose either x or y to be a generator of $U(GF(q))$, we have either $q-1$ divides $k-1$ or $q-1$ divides m. For the converse, $q-1$ divides $k-1$ implies $x = x^k$ for all x, while $q-1$ divides m implies $y = y^{m+1}$ for all y. Therefore $(x-x^k)(y-y^{m+1}) = 0 = y(1-y^m)x(1-x^{k-1})$.

For the other two cases, first let R be any one of these rings. Then $J \neq 0$ and $R/J \cong GF(q)$, where $q = p^r$. The quotient map $R \to R/J$ induces a surjective group homomorphism $U(R) \to U(R/J)$ with kernel $1+J$. If $x \in R$, then $\overline{x}$ will denote the image of x in R/J under the quotient map.

If $y \in U(R)$ then $1-y^m \in J$, since otherwise it would be a unit and then $xy - yx^k = 0$ for all $x \in R$. In particular, if $x \in J$ then $x^k = 0$, so $xy = 0$ and thus $x = 0$. This is a contradiction since $J \neq 0$. Therefore $\overline{y}^m = 1$ in R/J and so $q-1$ divides m.

If $R = GR(p^2, r)$, let $y \in J$ with $y \neq 0$. Then $xy - yx^k = 0 = y(x-x^k)$ for all x, using the commutativity of R. Therefore $x-x^k \in J$, since otherwise it would be a unit and then $y = 0$, which is false. Therefore $\overline{x} = \overline{x}^k$ in R/J holds for all x and so $q-1$ divides $k-1$.

If $R = S(p^r, t)$ we have $xy = yx^k$ for all $y \in J$ and all x. In particular, for $x = \left(\begin{smallmatrix} a & 0 \\ 0 & a^t \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, where $a \in GF(q)$, we have $a = a^{kt}$. This is true for all $a \in GF(q)$, so $kt \equiv 1 \pmod{q-1}$.

If $k \not\equiv 1 \pmod{q-1}$ and $y \in U(R)$, then there is some x such that $xy - yx^k \in U(R)$, since if $xy - yx^k \in J$ for all x then $\overline{y}(\overline{x} - \overline{x}^k) = 0$ in R/J. This would imply that $\overline{x} = \overline{x}^k$ in R/J for all x, and so $k \equiv 1 \pmod{q-1}$, a contradiction. Now $xy - yx^k \in U(R)$ implies that $1 - y^m = 0$. Since the exponent of $U(R)$ is $p(q-1)$ by Lemma 4.7, $p(q-1)$ divides m.

For the converse, we consider two cases. First, suppose that $k \equiv 1 \pmod{q-1}$. For $S(p^r, t)$ this implies that $t \equiv 1 \pmod{q-1}$, so the automorphism σ is the identity and the ring is commutative. Let R denote either this ring or $GR(p^2, r)$, so that R is commutative. Then $x - x^k \in J$ and $y - y^{m+1} \in J$, since $k \equiv 1 \pmod{q-1}$ and $q-1$ divides m imply that $\overline{x} = \overline{x}^k$ and $\overline{y} = \overline{y}^{m+1}$ in R/J. Therefore $(x-x^k)(y-y^{m+1}) = 0$ since $J^2 = 0$ and the commutativity of R gives $(1-y^m)(xy - yx^k) = 0$.

For the second case, suppose that $k \not\equiv 1 \pmod{q-1}$, so that we are dealing with $S(p^r, t)$ only. Let $R = S(p^r, t)$. Since $kt \equiv 1 \pmod{q-1}$, an easy computation shows that $xy = yx^k$ for all $x \in R$ and all $y \in J$. If $y \in U(R)$, then $p(q-1)$ divides m implies that $y^m = 1$, since the exponent of $U(R)$ is $p(q-1)$ by Lemma 4.7. Thus $(1-y^m)(xy - yx^k) = 0$ since either $y \in J$ and the second factor equals 0 for all x, or $y \in U(R)$ and the first factor is 0. □

This result can be used in two ways. Given an equation as in Theorem 4.6, we can determine all the subdirectly irreducible rings satisfying the equation by finding values of p, r, and t that meet the indicated conditions. Alternatively, given the subdirectly irreducible rings in $\mathscr{V}$, we can find an equation of the form given in Theorem 4.6 satisfied by $\mathscr{V}$ by solving the systems of congruences for m and k given by the conditions indicated above. For example, to find an equation of the given form that is satisfied by both $S(7^3, 7^2)$ and $S(3^2, 3)$ we have to solve the system of congruences $m \equiv 0 \pmod{7(7^3-1)}$, $m \equiv 0 \pmod{3(3^2-1)}$, $49k \equiv 1 \pmod{7^3-1}$ and $3k \equiv 1 \pmod{3^2-1}$. The smallest

solutions in positive integers to these congruences are $m = 9576$ and $k = 691$, so both these rings satisfy $xy = y^{9576}xy + y(1 - y^{9576})x^{691}$.

The theorem also shows that certain combinations of subdirectly irreducible rings are not possible in the varieties we are considering. For example, no variety satisfying an identity of the form $xy = yp(x, y)$, where all terms of p have degree greater than one, can contain the rings $S(3^2, 3)$ and $S(5^2, 5)$, since the variety would satisfy some equation of the form given in Theorem 4.6 and then k would have to satisfy the two congruences $3k \equiv 1 \pmod 8$ and $5k \equiv 1 \pmod{24}$, that is, $k \equiv 3 \pmod 8$ and $k \equiv 5 \pmod{24}$. It is obvious that this system has no solution. In more complicated cases, Lemma 4.5 can be used. The system of congruences for m can always be solved, since the congruences are all of the form $m \equiv 0$.

5. Structure results

In this section, we derive some further identities that hold in $\mathscr{V}$ and use them to prove structure theorems for the finite and semiperfect rings in the variety. $\mathscr{V}$ has the same meaning as in the preceding sections.

Our first result is just the statement of a classical theorem true in any variety, although the results of the previous section give much information about the subdirectly irreducible rings in $\mathscr{V}$.

Theorem 5.1. *Let R be any ring in $\mathscr{V}$. Then R is isomorphic to a subdirect product of the subdirectly irreducible rings in $\mathscr{V}$.*

It is well known that the subdirect product construction is very flexible, too flexible to give strong structure results in many cases. We can use the identities given in the next theorem to derive much stronger results for the semiperfect or finite rings in $\mathscr{V}$.

Theorem 5.2. *There is an integer $m \geq 1$ such that $\mathscr{V}$ satisfies the identities*

$$x^m y = yx^m, \quad x^2 = x^{m+2}, \quad x^m = (x^m)^2, \quad (x - x^{m+1})(y - y^{m+1}) = 0.$$

Proof. Let m be the least common multiple of the exponents of the groups of units of the subdirectly irreducible rings in $\mathscr{V}$ and let R be any subdirectly irreducible ring in $\mathscr{V}$. Then for all $x \in R$, either $x \in U(R)$ and so $x^m = 1$ or $x \in J(R)$ and so $x^2 = 0$, hence $x^m = 0$ for any $m > 1$. Thus $x^m y = yx^m$ holds in R. For the second identity, either x is a unit and so $x^{m+2} = x^m x^2 = x^2$ or $x \in J$ and then $x^2 = 0 = x^{m+2}$. Thus $x^2 = x^{m+2}$ holds in R, from which the third identity immediately follows. Finally, note that if x is a unit then $x - x^{m+1} = 0$, while if $x \in J$ then $x - x^{m+1} = x$. Therefore $(x - x^{m+1})(y - y^{m+1}) = 0$, since either x or y is a unit and so one factor is 0, or both x and y are in J, and then $xy \in J^2 = 0$. □

Corollary 5.3. *Let $R \in \mathscr{V}$. Then all idempotents of R are central.*

Proof. If $e = e^2 \in R$, then $e = e^m$, which is central by the theorem. □

Theorem 5.4. *Let R be a semiperfect ring in $\mathscr{V}$. Then R is isomorphic to a finite direct product of local rings in $\mathscr{V}$.*

Proof. A semiperfect ring contains a finite set of orthogonal local idempotents. These are all central by Corollary 5.3 so R is isomorphic to a finite direct product of local rings in $\mathscr{V}$. □

Corollary 5.5. *Let R be a finite ring in $\mathscr{V}$. Then R is isomorphic to a finite direct product of finite local rings in $\mathscr{V}$.*

The finite local rings in $\mathscr{V}$ were described in Theorem 4.3. Note that the restrictions given by Theorems 4.6 and 4.8 on the subdirectly irreducible rings in $\mathscr{V}$ give similar restrictions on the finite local rings in $\mathscr{V}$, since they are subdirect products of the subdirectly irreducible local rings in $\mathscr{V}$.

6. Varieties satisfying $xy = p(x, y)x$

Our previous results also apply to any variety of rings satisfying an identity of the form $xy = p(x, y)x$, where p is a polynomial and every term of p has degree greater than one. It is easy to see that such varieties have definable principal congruences, either by observing that they satisfy $x_1yz_1 + x_2yz_2 = (x_1p(y, z_1) + x_2p(y, z_2))\cdot y\cdot 1$ or by noting that principal two-sided ideals are just principal left ideals.

It is straightforward to check that our earlier proofs are valid for such varieties, in particular, that the subdirectly irreducible rings are finite local rings with $J^2 = 0$. Then similar arguments as before show that the subdirectly irreducible rings have the same description as before, and that all the subdirectly irreducible rings in the variety satisfy an equation of the form

$$(xy - y^jx)(1 - x^n) = 0, \quad \text{or} \quad xy = xyx^n + y^j(1 - x^n)x.$$

This gives us the following theorem, the analog of Theorem 4.6.

Theorem 6.1. *Let $\mathscr{W}$ be any variety of rings. Then $\mathscr{W}$ satisfies an identity of the form $xy = p(x, y)x$, where p is a polynomial and every term of p has degree greater than one, if and only if there are integers $n \geq 1$ and $j \geq 2$ such that $\mathscr{W}$ satisfies*

$$xy = xyx^n + y^j(1 - x^n)x.$$

We also have the following analog of Theorem 4.8, which can be proved in essentially the same way.

Theorem 6.2. *Consider the equation*

$$xy = xyx^n + y^j(1 - x^n)x$$

for integers $n \geq 1$ and $j \geq 2$. Let p be a prime and let r and t be positive integers. Then

(a) *$GF(p^r)$ satisfies this equation if and only if $p^r - 1$ divides n or $j \equiv 1 \pmod{p^r - 1}$,*

(b) *$GR(p^2, r)$ satisfies this equation if and only if $p^r - 1$ divides n and $j \equiv 1 \pmod{p^r - 1}$, and*

(c) *$S(p^r, t)$ satisfies this equation if and only if $p^r - 1$ divides n, $j \equiv t \pmod{p^r - 1}$, and if $j \not\equiv 1 \pmod{p^r - 1}$ then $p(p^r - 1)$ divides n.*

Combining these results with their analogs, we can show that the two different types of varieties are very closely related.

Theorem 6.3. *Let $\mathscr{W}$ be any variety of rings. Then the following are equivalent:*

(a) *$\mathscr{W}$ satisfies an identity of the form $xy = yp(x, y)$, where p is a polynomial and every term of p has degree greater than one,*

(b) *there are integers* $m \geq 1$ *and* $k \geq 2$ *such that* $\mathscr{W}$ *satisfies*

$$xy = y^m xy + y(1 - y^m)x^k,$$

(c) $\mathscr{W}$ *satisfies an identity of the form* $xy = p(x, y)x$, *where* p *is a polynomial and every term of* p *has degree greater than one,*

(d) *there are integers* $n \geq 1$ *and* $j \geq 2$ *such that* $\mathscr{W}$ *satisfies*

$$xy = xyx^n + y^j(1 - x^n)x.$$

Proof. It follows from Theorem 4.6 that (a) and (b) are equivalent and from Theorem 6.1 that (c) and (d) are equivalent. We now show that (b) implies (d). If R is a subdirectly irreducible ring in $\mathscr{W}$, then it must be of one of the three types indicated in Theorem 4.4 and it must also satisfy the conditions given in Theorem 4.8, so there are certain congruences satisfied by m and k. If R is to satisfy an equation of the type given in (d), then n and j must satisfy the congruences given by the previous theorem. We can certainly solve the system of congruences for n, since they are all of the form $n \equiv 0$. In fact, we can take $n = m$, since they both satisfy the same set of congruences.

It remains to show that the system of congruences for j has a solution. The congruences on k are either of the form $k \equiv 1 \pmod{q-1}$ or $kt \equiv 1 \pmod{q-1}$, for various prime powers q. Congruences of the second form can be written in the form $k \equiv s \pmod{q-1}$, where $st \equiv 1 \pmod{q-1}$, since t is always relatively prime to $q-1$. Thus the system of congruences on k can be taken to be $k \equiv s_i \pmod{q_i - 1}$, where $s_i t_i \equiv 1 \pmod{q_i - 1}$ and q_i is a prime power, for all i in some finite index set I. In the same notation, the system of congruences for j is $j \equiv t_i \pmod{q_i - 1}$. This system has a solution if and only if $t_i \equiv t_h \pmod{\gcd(q_i - 1, q_h - 1)}$ for all $i, h \in I$ with $i \neq h$, by Lemma 4.5. Thus, suppose that $i \neq h$ and let $g = \gcd(q_i - 1, q_h - 1)$. Then $s_i t_i \equiv 1 \pmod{g}$ and $s_h t_h \equiv 1 \pmod{g}$, so $t_i - t_h \equiv t_i t_h s_h - t_h t_i s_i \equiv t_i t_h (s_h - s_i) \pmod{g}$. Since the system of congruences for k has a solution, Lemma 4.5 shows that $s_h \equiv s_i \pmod{g}$, hence $t_i - t_h \equiv 0 \pmod{g}$. Therefore the system of congruences for j has a solution and we can find an equation of the required form that is satisfied by $\mathscr{W}$.

A similar argument shows that (d) implies (b). □

Corollary 6.4. *Let* $\mathscr{W}$ *be a variety of rings satisfying any (hence all) of the conditions of the theorem. If* R *is a ring in* $\mathscr{W}$, *then the two-sided ideal* RyR *generated by an element* $y \in R$ *equals both the left ideal* Ry *and the right ideal* yR. *Both of the statements* $\exists z(x = zy)$ *and* $\exists z(x = yz)$ *hold precisely when* $x \in RyR$ *and so either of these statements defines principal ideals in* R, *for any* $R \in \mathscr{W}$.

7. Connections with residually small varieties

McKenzie [M82] showed that a variety of rings is residually small if and only if it satisfies and equation of the form $xy = f(x, y)$, where f is a polynomial and every term of f has degree at least three. The condition we have considered is clearly a special case of this condition and all the varieties we have considered are residually small.

The varieties we have considered and residually small varieties have many similarities. For example, in both cases $J(R)^2 = 0$ for all rings R in the

variety. McKenzie proved that any residually small variety satisfies the equation $(x - x^n)(y - y^n) = ((x - x^n)(y - y^n))^n$ for some integer $n > 1$, while Theorem 5.2 shows that the varieties with definable principal congruences considered in this paper satisfy $(x - x^n)(y - y^n) = 0$ for some integer $n > 1$.

However, residual smallness and definable principal congruences are distinct notions, since there are varieties with definable principal congruences that are not residually small and there are residually small varieties that do not have definable principal congruences. For example, the ring given in Theorem 13 of [S83] generates a variety with definable principal congruences, but since it has $J^2 \neq 0$ it cannot be in a residually small variety. Conversely, $M_2(GF(q))$ can be in a residually small variety, but not in a variety with definable principal congruences, by Theorem 2.2.

Acknowledgment

This paper was completed during a visit to the Department of Mathematics, Universitaire Instelling Antwerpen, Antwerp, Belgium. The author would like to thank the department and Professor F. Van Oystaeyen for their hospitality.

References

[B] K. Baker, *Definable normal closures in locally finite varieties of groups*, Houston J. Math. **7** (1981), 467–471.

[BB] J. Baldwin and J. Berman, *The number of subdirectly irreducible algebras in a variety*, Algebra Universalis **5** (1975), 379–389.

[BL79] S. Burris and J. Lawrence, *Definable principal congruences in varieties of groups and rings*, Algebra Universalis **9** (1979), 152–164.

[BL81] ——, *A correction to "Definable principal congruences in varieties of groups and rings"*, Algebra Universalis **13** (1981), 264–267.

[J] G. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), 461–479.

[K] E. Kiss, *Definable principal congruences in congruence distributive varieties*, Algebra Universalis **21** (1985), 213–224.

[M78] R. McKenzie, *Paraprimal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties*, Algebra Universalis **8** (1978), 336–348.

[M82] ——, *Residually small varieties of K-algebras*, Algebra Universalis **14** (1982), 181–196.

[P] C. Procesi, *Rings with polynomial identities*, Marcel Dekker, New York, 1973.

[R] R. Raghavendran, *Finite associative rings*, Compositio Math. **21** (1969), 195–229.

[Ro] L. H. Rowen, *Polynomial identities in ring theory*, Academic Press, New York, 1980.

[S83] G. E. Simons, *Varieties of rings with definable principal congruences*, Proc. Amer. Math. Soc. **87** (1983), 397–402.

[S86] ——, *Definable principal congruences and R-stable identities*, Proc. Amer. Math. Soc. **97** (1986), 11–15.

[T] S. Tulipani, *On classes of algebras with the definability of congruences*, Algebra Universalis **14** (1982), 269–279.

[W] R. S. Wilson, *Representations of finite rings*, Pacific J. Math. **53** (1974), 643–679.

Department of Mathematics and Computer Science, Royal Military College of Canada, Kingston, Ontario, Canada K7K 5L0