PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 121, Number 3, July 1994

FINITE RINGS IN VARIETIES WITH DEFINABLE PRINCIPAL CONGRUENCES

G. E. SIMONS

(Communicated by Maurice Auslander)

ABSTRACT. A variety $\mathscr{V}$ of rings has definable principal congruences if there is a first-order formula defining principal two-sided ideals for all rings in $\mathscr{V}$. Any variety of commutative rings has definable principal congruences, but many noncommutative rings cannot be in a variety with definable principal congruences. We show that a finite ring in a variety with definable principal congruences is a direct product of finite local rings. This result is used to describe the structure of all finite rings R with $J(R)^2 = 0$ in a variety with definable principal congruences.

1. Introduction

A variety $\mathscr{V}$ of rings has definable principal congruences (two-sided ideals) if there is a formula in the first-order theory of rings that defines principal (two-sided) ideals for all rings in $\mathscr{V}$. Any variety $\mathscr{V}$ of commutative rings has definable principal congruences since if $R \in \mathscr{V}$ and $x, y \in R$ then x is in the principal ideal generated by y (denoted RyR in this paper) if and only if the first-order formula $\phi(x, y) := \exists z(x = yz)$ is satisfied.

Earlier work on varieties of rings with definable principal congruences [S1, S2] has shown that, in a variety with definable principal congruences, rings that meet certain structural conditions, such as primitivity or primeness, must be commutative. In view of these results and others, it seems natural to view rings in varieties with definable principal congruences as being, in some sense, generalizations of commutative rings.

The concept of definable principal congruences originated in universal algebra [BB]. 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 $\mathscr{V}$. 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.

Received by the editors April 11, 1991 and, in revised form, March 12, 1992.

1991 *Mathematics Subject Classification*. Primary 16R10, 16P10; Secondary 08B26, 16R40, 16L30.

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

This has been investigated by McKenzie [M1] for varieties of lattices, Burris and Lawrence [BL1] and Baker [B] for locally finite varieties of groups, and Kiss [K] for congruence distributive varieties generated by a finite algebra.

This paper deals with the structure of finite rings in varieties with definable principal congruences. We are primarily interested in finite noncommutative rings in varieties with definable principal congruences, since any variety of commutative rings has definable principal congruences. Unlike the commutative case, there are finite noncommutative rings that cannot be in any variety with definable principal congruences [BL1]. Some examples of finite noncommutative rings in a variety with definable principal congruences are given in [S1] and [S3].

It was shown in [S1] that certain kinds of rings in varieties with definable principal congruences, such as semiperfect algebras over finite fields, are isomorphic to a direct product of local rings. It is well known that any finite commutative ring is a direct product of local rings. The major result of this paper is to extend this to finite rings in varieties with definable principal congruences—any finite ring in a variety with definable principal congruences is a direct product of local rings. As an application of our result, we determine the structure of a finite ring R with $J(R)^2 = 0$ in a variety with definable principal congruences.

2. Notation and preliminary results

The term 'ring' means 'ring with identity' in this paper, so 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, $U(R)$ for the multiplicative group of units of R, $[x, y]$ for the commutator $xy - yx$ of any two elements x and y of R, $C(R)$ for the commutator ideal of R (the ideal generated by all commutators $[x, y]$ in R), and $\mathrm{Nil}(R)$ for the upper nil radical of R (the unique largest nil ideal of R).

In our study of finite rings, two other types of rings will often appear, namely, semiperfect rings and local rings. Some essential facts about these two types of rings are given here for the reader's convenience. Any standard text on ring theory, such as [AF] or [Ro], should contain these results.

A ring R is local if and only if $R/J(R)$ is a division ring. Any homomorphic image of a local ring is also a local ring. In a local ring R, the ideal $J(R)$ consists of all the nonunits of R, so every element of R is in either $J(R)$ or $U(R)$. If R is a local ring and $x \in R$, then either x or $1 - x$ is a unit. Consequently, the only idempotents of a local ring are 0 and 1.

A ring R is semiperfect if and only if $R/J(R)$ is a semiprime Artinian ring and idempotents of $R/J(R)$ can be lifted to idempotents of R. This means that if $x + J(R)$ is an idempotent of $R/J(R)$, then there is an idempotent e of R such that $e - x \in J(R)$. An important characterization of semiperfect rings is that R is semiperfect if and only if there is a finite set $e_1, e_2, \dots, e_n$ of idempotents of R such that $e_ie_j = 0$ for all $i \neq j$, $e_1 + \cdots + e_n = 1$, and e_iRe_i is a local ring for $i = 1, 2, \dots, n$. From this characterization, it follows that a commutative semiperfect ring is a finite direct product of local rings. The class of semiperfect rings includes all finite, Artinian or local rings, as well as many non-Artinian Noetherian rings.

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

Theorem 2.1 [BL1]. *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, $n > k \geq 1$, $\overline{x} = (x_1, \dots, x_n)$, $\overline{z} = (z_1, \dots, z_n)$, and $r_i(\overline{x}, y, \overline{z})$, and $s_i(\overline{x}, y, \overline{z})$, $1 \leq i \leq k$, are polynomials.

This furnishes another demonstration that if R is a commutative ring then $V(R)$ has definable principal congruences, since any commutative ring R satisfies the identity $\sum_{i=1}^{2} x_i y z_i = 1y(\sum_{i=1}^{2} x_i z_i)$.

If a variety $\mathscr{V}$ of rings has definable principal congruences, then it satisfies an identity of the form given in Theorem 2.1. A first-order formula defining principal congruences (two-sided ideals) in the variety $\mathscr{V}$ would be

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

If $R \in \mathscr{V}$ and $x, y \in R$, then $x \in RyR$ if and only if $\phi(x, y)$ holds. If 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 $V(R) \subseteq \mathscr{V}$.

Some of the principal results from earlier papers about the structure of rings generating varieties with definable principal congruences are summarized in the following two theorems.

Theorem 2.2 [S1]. *Let R be a nontrivial ring. Then $V(M_n(R))$ does not have definable principal congruences if $n \geq 2$.*

Theorem 2.3 [S1, S2]. *If R is a ring and $V(R)$ has definable principal congruences, then*:

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

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

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

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

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

The next two theorems appeared in [S3] and are used later in this paper. They are included here with proofs for the reader's convenience.

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, Theorem 2.3(c) shows that R/P is commutative, so $C \subseteq P$. For any ring, $P(R)$ is a nil ideal, so 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 $N = \operatorname{Nil}(R) \subseteq J$. Since R is a PI-ring, $P = \operatorname{Nil}(R) = N$ [P, p. 40]. Finally, the semiprimitive ring R/J is a subdirect product of its primitive images. These primitive rings are in $\mathscr{V}$ and so, by Theorem 2.3(b), they must be fields. □

In particular, if R is a finite ring in a variety $\mathscr{V}$ with definable principal congruences, then $P(R) = \operatorname{Nil}(R) = J(R) = \{x \in R | x \text{ is nilpotent}\}$ since $J(R)$ is nilpotent, and $R/J(R)$ is isomorphic to a finite direct product of finite fields in $\mathscr{V}$ by the Artin-Wedderburn theorem and Theorems 2.2 and 2.3(b).

Theorem 2.5. *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. Let $C = C(R)$ and $J = J(R)$. 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 Theorem 2.3(d) shows that 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. Varieties generated by finite local rings

We begin with some simple observations about the structure of rings in a variety generated by finitely many finite local rings.

Theorem 3.1. *Let $\mathscr{V}$ be a variety of rings generated by a finite set of finite local rings. Then:*

(i) *there is an integer $n \geq 1$ such that $[x^n, y] = 0$ is an identity of all rings in $\mathscr{V}$;*

(ii) *if $R \in \mathscr{V}$, then all idempotents of R are central; and*

(iii) *if $R \in \mathscr{V}$ is semiperfect, then R is isomorphic to a finite direct product of local rings.*

Proof. Let $S_1, \dots, S_k$ be the finite local rings generating $\mathscr{V}$. For each i, $U(S_i)$ is a finite multiplicative group and $J(S_i)$ is nilpotent. Thus there are integers $u_i \geq 1$ and $j_i \geq 1$ such that if $x \in U(S_i)$ then $x^{u_i} = 1$ and if $y \in J(S_i)$ then $y^{j_i} = 0$. Let n_i be the smallest multiple of u_i that is greater than or equal to j_i. Then since S_i is local, x^{n_i} is either 0 or 1 for all $x \in S_i$, so S_i satisfies the identity $[x^{n_i}, y] = 0$. If n is the least common multiple of $n_1, \dots, n_k$, then each S_i satisfies the identity $[x^n, y] = 0$. Since $S_1, \dots, S_k$ generate $\mathscr{V}$, all rings in $\mathscr{V}$ satisfy this identity.

If $R \in \mathcal{V}$, then R satisfies $[x^n, y]$, so if $e \in R$ is an idempotent, then $e = e^2 = e^n$ and $[e, y] = 0$ holds for all $y \in R$. Therefore, e is central in R. If $R \in \mathcal{V}$ is semiperfect, then R contains a finite orthogonal set of local idempotents, each of which must be central in R. Hence R is isomorphic to a finite direct product of local rings. □

The following theorem is the main result of this paper. It shows that a finite ring in a variety with definable principal congruences lies in a subvariety generated by finitely many finite local rings, so the structure results of the previous theorem apply.

Theorem 3.2. *Suppose that $\mathcal{V}$ is a variety of rings with definable principal congruences and $R \in \mathcal{V}$ is finite. Then R is isomorphic to a finite direct product of finite local rings.*

Proof. Since R is finite, $J(R)$ is nilpotent and [AF, Proposition 27.17] shows that $e \in R$ is a central idempotent if and only if $e + J(R)^2 \in R/J(R)^2$ is a central idempotent. Thus, if every idempotent of $R/J(R)^2$ is central, then every idempotent of R is central, and since R is semiperfect, this implies that R is isomorphic to a finite direct product of finite local rings.

Without loss of generality, we can therefore assume that R is finite and $J(R)^2 = 0$. By the remarks after Theorem 2.4, $R/J(R)$ is isomorphic to a finite direct product of finite fields. Then there is an integer $n > 1$ such that $r = r^n$ for all $r \in R/J(R)$, so $z - z^n \in J(R)$ for all $z \in R$. By Theorem 2.4, $C(R) \subseteq J(R)$, so $C(R)J(R) \subseteq J(R)^2 = 0$. Then $[x, y](z - z^n) \in C(R)J(R)$, so R satisfies the identity $[x, y](z - z^n) = 0$.

R is a subdirect product of its subdirectly irreducible homomorphic images $S_1, \dots, S_k$, so $V(R) = V(S_1, \dots, S_k)$ and each S_i satisfies the identity $[x, y](z - z^n) = 0$ since R does. If $z \in J(S_i)$, then $1 - z^{n-1}$ is invertible and so $[x, y]z = 0$. This implies that $C(S_i)J(S_i) = 0$. Then by Theorem 2.5, S_i has no nontrivial idempotents. Since S_i is semiperfect, this means that S_i is a finite local ring. By Theorem 3.1, R is isomorphic to a finite direct product of finite local rings and every idempotent of R is central. □

From this and Theorem 3.1, we can deduce the following results about finite rings in any variety with definable principal congruences.

Corollary 3.3. *If $\mathcal{V}$ is a variety of rings with definable principal congruences and $R \in \mathcal{V}$ is finite, then every idempotent of R is central and there is an integer $n \geq 1$ such that R satisfies the identity $[x^n, y] = 0$.*

Corollary 3.4. *If $\mathcal{V}$ is a variety of rings with definable principal congruences and $S \in \mathcal{V}$ is finite and either subdirectly irreducible or directly indecomposable, then S is a local ring.*

If a variety with definable principal congruences is generated by a finite ring, then the following result, similar to the above but slightly stronger, can also be deduced immediately from Theorems 3.2 and 3.1.

Corollary 3.5. *If R is a finite ring such that $V(R)$ has definable principal congruences and $S \in V(R)$ is semiperfect and either subdirectly irreducible or directly indecomposable, then S is a local ring.*

Corollary 3.6. *If R is a finite ring and $V(R)$ has definable principal congruences, then there are finite, subdirectly irreducible, local rings $S_1, \dots, S_k$ such that*

$V(R) = V(S_1, \ldots, S_k)$ and R is a subdirect product of $S_1, \ldots, S_k$. If $J(R)^n = 0$, then $S_1, \ldots, S_k$ can be chosen so that $J(S_i)^n = 0$ for $i = 1, \ldots, k$.

Proof. By Theorem 3.2, R is isomorphic to the direct product of local rings $A_1, \ldots, A_m$. Since $J(R)^n = 0$, it follows that $J(A_i)^n = 0$. Each A_i is a subdirect product of its subdirectly irreducible homomorphic images, say A_{ij}, for $j = 1, \ldots, k_i$. Since A_i is local, so is each A_{ij} and $J(A_i)^n = 0$ implies that $J(A_{ij})^n = 0$. Then R is a subdirect product of all the A_{ij}, so $V(R) = V(\{A_{ij}\})$ and each A_{ij} is a finite, local, subdirectly irreducible ring with $J(A_{ij})^n = 0$. □

4. Finite rings with $J^2 = 0$

As an application of our results, we determine the structure of a finite ring R in a variety $\mathscr{V}$ with definable principal congruences, when $J(R)^2 = 0$.

There is a way of representing finite local rings as rings of matrix-like objects, called Szele matrices, due to Wilson [W]. This representation uses the Galois rings that were introduced independently by Raghavendran [R] and Janusz [J], although they were apparently also known much earlier to Krull. Galois rings are finite, local rings that can be viewed as a common generalization of both finite fields and the rings $\mathbf{Z}/p^n\mathbf{Z}$, where p is a prime and n a positive integer. 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 and has characteristic p^n, the Jacobson radical of $GR(p^n, r)$ is $pGR(p^n, r)$, and $GR(p^n, r)/pGR(p^n, r) \cong GF(p^r)$.

Theorem 4.1. *Let R be a finite ring with $J(R)^2 = 0$ contained in a variety $\mathscr{V}$ with definable principal congruences. Then R is a subdirect product of rings of the following three types, for various primes p, positive integers r, and automorphisms σ:*

(i) $GF(p^r)$,

(ii) $GR(p^2, r)$,

(iii) $\begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix}$, *where $a, b \in GF(p^r)$ and σ is an automorphism of $GF(p^r)$.*

Proof. By Corollary 3.6, R is a subdirect product of finite, local, subdirectly irreducible rings $T_1, \ldots, T_k$ with $J(T_i)^2 = 0$ for $i = 1, \ldots, k$. It follows from the results of Wilson [W] (see also [S3, Theorem 4.1]) that the only finite, local, subdirectly irreducible rings T with $J(T)^2 = 0$ are the three kinds of rings listed. Therefore, R is a subdirect product of these three types of rings. □

Note that Galois fields and rings are commutative but rings of the third type are commutative if and only if σ is the identity map. Each of these types of rings generates a variety with definable principal congruences, the first two types since they are commutative. The third type was shown to generate a variety with definable principal congruences in [S3]. Rings of this third type were shown to satisfy identities of the form $xy = yp(x, y)$ and $xy = q(x, y)x$, where p and q are polynomials in which each term has degree at least two. The varieties generated by rings of this type are residually small, that is, there is a bound (which can be shown to be finite) on the size of the subdirectly irreducible rings in the variety. Residually small varieties of rings are characterized in [M2].

It is not known to the author if an arbitrary subdirect product of these three types of rings always generates a variety with definable principal congruences, so it is possible that not all rings of this form generate varieties with definable principal congruences. See [S3, §4] for some details on when products of these types of rings generate varieties with definable principal congruences.

Acknowledgment

The author thanks the referee for a very careful reading of the paper and suggestions which improved the exposition.

References

[AF] F. Anderson and K. Fuller, *Rings and categories of modules*, Springer-Verlag, New York, 1973.

[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.

[BL1] S. Burris and J. Lawrence, *Definable principal congruences in varieties of groups and rings*, Algebra Universalis **9** (1979), 152–164.

[BL2] ——, *A correction to ibid.*, 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.

[M1] R. McKenzie, *Paraprimal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties*, Algebra Universalis **8** (1978), 336–348.

[M2] ——, *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, *Ring theory*, Academic Press, San Diego, 1988.

[S1] G. E. Simons, *Varieties of rings with definable principal congruences*, Proc. Amer. Math. Soc. **87** (1983), 397–402.

[S2] ——, *Definable principal congruences and R-stable identities*, Proc. Amer. Math. Soc. **97** (1986), 11–15.

[S3] ——, *The structure of rings in some varieties with definable principal congruences*, Trans. Amer. Math. Soc. **331** (1992), 165–179.

[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 K7K5L0

E-mail address: simons-g@rmc.ca