PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 97, Number 1, May 1986

# DEFINABLE PRINCIPAL CONGRUENCES AND $R$-STABLE IDENTITIES

G. E. SIMONS

ABSTRACT. We show that an algebra over an infinite field generates a variety with definable principal congruences if and only if it is commutative. A similar result is proved for polynomial rings. The main tool used is the notion from the theory of PI-rings of an $R$-stable identity.

**1. Introduction.** A variety $\mathcal{V}$ of (universal) algebras has definable principal congruences (DPC) if there is a first order formula in the language of $\mathcal{V}$ that defines principal congruences for all algebras in $\mathcal{V}$. There have been a number of papers that deal with this concept for specific types of algebras. In particular, there are complete characterizations of the varieties of lattices with DPC [**4**] and the finite groups that generate varieties with DPC [**1**]. See [**7**] for further background.

This paper and [**7**] deal specifically with varieties of rings with DPC. A variety $\mathcal{V}$ of rings has DPC if there is a first order formula $\phi(x, y)$ in the language of rings such that for all rings $R \in \mathcal{V}$ and all $x, y \in R$, $x \in RyR \Leftrightarrow \phi(x, y)$, where $RyR$ is the two-sided ideal of $R$ generated by $y$. The language of rings used is $\{+, -, \cdot, 0, 1\}$, so that all rings have a 1.

Any variety of commutative rings has DPC, since $\phi(x, y) := \exists z(x = yz)$ defines two-sided ideals (principal congruences) in such a variety. In [**7**] it was shown that if a ring $R$ generates a variety with DPC, then $R$ is a polynomial identity (PI) ring. Results from PI theory were used to prove that if $R$ is a semiprime ring, then $V(R)$ has DPC if and only if $R$ is commutative.

It is not true that a variety of rings has DPC only if it consists of commutative rings, as the example in [**7**, Theorem 13] shows. The results of this paper were motivated by attempts to modify this example in various ways. The example was to take the ring $F\langle X, Y\rangle/(\{X, Y\}^3)$, where $F$ is a finite field, $F\langle X, Y\rangle$ the free (noncommutative) $F$-algebra on two generators and $(\{X, Y\}^3)$ the ideal generated by all monomials in $X$ and $Y$ of degree 3. This ring is clearly noncommutative but the variety it generates has DPC.

In this example, the number of indeterminates can be increased and the variety generated still has DPC. If the ideal is changed to $(\{X, Y\}^m)$ with $m > 3$ then it follows from [**2**, Theorem 2.4] that the variety generated does not have DPC. The remainder of this paper deals with determining what happens when the finite field $F$ is replaced by infinite fields, such as $\mathbf{Q}$ or $\mathbf{R}$, or by a ring such as $\mathbf{Z}$.

**2. $R$-stable identities.** The criterion we use for determining if a variety of rings has DPC is the following theorem.

Received by the editors October 3, 1984 and, in revised form, May 6, 1985.
1980 *Mathematics Subject Classification.* Primary 16A38; Secondary 08B99.
*Key words and phrases.* Varieties of rings, definable principal congruences, stable identities.

THEOREM 2.1 [**2**]. *If $K$ is a class of rings, then $V(K)$ has DPC if and only if there are integers $n$ and $k$, with $n > k \geq 1$, and polynomials $r_i(\overline{x}, y, \overline{z})$ and $s_i(\overline{x}, y, \overline{z})$, where $1 \leq i \leq k$, $\overline{x} = (x_1, \ldots, x_k)$, $\overline{y} = ((y_1, \ldots, y_n)$ such that $K$ satisfies the identity*

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

The example mentioned in §1 generates a variety $\mathcal{V}$ with DPC since it satisfies an identity of the form

$$\sum_{i=1}^{3} x_i y z_i = y\left(\sum_{i=1}^{3} r(x_i, y, z_i)\right) + \left(\sum_{i=1}^{3} s(x_i, y, z_i)\right) y.$$

A first order statement $\phi(x, y)$ defining principal two-sided ideals in this variety is $\exists x_1, x_2, z_1, z_2$ $(x = \sum_{i=1}^{2} x_i y z_i)$, so that $x \in RyR$ if and only if it can be written in the form $\sum_{i=1}^{2} x_i y z_i$, for all $x, y \in R$ and all $R \in \mathcal{V}$.

To begin consideration of the questions of the previous section, we first examine some special properties of polynomial identities of algebras over infinite fields.

For the remainder of the paper the term "algebra" is used in its ring-theoretic sense.

DEFINITION [**6**, DEFINITION 2.3.8]. An identity $f$ of a ring $R$ is *$R$-stable* if $f$ is an identity of $R[x]$.

We will be concerned with rings $R$ such that all their identities are $R$-stable. The following lemma gives two well-known classes of rings with this property (see, for example, [**6**, Exercises 2.3.4 and 2.3.8, p. 148]).

LEMMA 2.2. (i) *If $A$ is an algebra over an infinite field, then every identity of $A$ is $A$-stable.*

(ii) *Every identity of $R[x]$ is $R[x]$-stable.*

For our purposes, the most useful property of $R$-stable identities is that they can be decomposed into a sum of certain polynomials which are also identities of the ring.

DEFINITION. A polynomial is *completely homogeneous* if each monomial is composed of the same indeterminates with each indeterminate appearing the same number of times in each monomial. For example, $x_1x_2x_3^3x_2^3x_1 + x_1^2x_2^4x_3^3 + x_3^2x_2^2x_1^2x_2^2x_3$ is a completely homogeneous polynomial. Any polynomial can be written uniquely as a sum of (maximal) completely homogeneous polynomials, called the completely homogeneous components of the polynomial.

LEMMA 2.3 [**5**, PROPOSITION 3.15, p. 14]. *If $f$ is an $R$-stable identity of $R$, then every completely homogeneous component of $f$ is an $R$-stable identity of $R$.*

These are all the facts we need about $R$-stable identities. Before stating the main theorem, we have the following simple lemma:

LEMMA 2.4. *Let $A$ be a noncommutative algebra over a field $F$. If $A$ satifies an identity of the form*

$$a_1xyz + a_2xzy + a_3yxz + a_4yzx + a_5zxy + a_6zyx = 0,$$

*with $a_i \in F$, $i = 1, \ldots, 6$, then $a_1 = a_6$, $a_2 = a_4$ and $a_3 = a5$.*

PROOF. Putting $x = y = z = 1$ yields $a_1 + a_2 + a_3 + a_4 + a_5 + a_6 = 0$. Putting $x = 1$ or $y = 1$ or $z = 1$ yields the three identities

$$(a_1 + a_3 + a_4)yz + (a_2 + a_5 + a_6)zy = 0,$$
$$(a_1 + a_2 + a_3)xz + (a_4 + a_5 + a_6)zx = 0,$$
$$(a_1 + a_2 + a_5)xy + (a_3 + a_4 + a_6)yx = 0.$$

These identities are all of the form $ax_1x_2 - ax_2x_1 = 0$ where $a \in F$. If $a \neq 0$ then we have $x_1x_2 - x_2x_1 = 0$ since $A$ is an algebra over a field, but then $A$ would be commutative, which it is not. Thus $0 = a_1+a_3+a_4 = a_2+a_5+a_6 = a_1+a_2+a_3 = a_4+a_5+a_6 = a_1+a_2+a_5 = a_3+a_4+a_6$, which imply that $a_1 = a_6$, $a_2 = a_4$ and $a_3 = a_5$.

THEOREM 2.5. *Let $A$ be an algebra over a field $F$. Suppose that all identities of $A$ are $A$-stable. Then $V(A)$ has DPC if and only if $A$ is commutative.*

PROOF. Assume that $V(A)$ has DPC and that $A$ is noncommutative. By Theorem 2.1, $A$ satisfies an identity of the form

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

with $n > k \geq 1$ and $r_i(\overline{x}, y, \overline{z})$, $s_i(\overline{x}, y, \overline{z})$ polynomials with integer coefficients. By iterating this identity as required, we can assume that $n > 2k$. Since all the identities of $A$ are $A$-stable, Lemma 2.3 shows that we can restrict this identity to monomials of degree 3 that contain exactly one $y$. Thus $A$ satisfies the identity

$$\sum_{i=1}^{n} x_i y z_i = \sum_{i=1}^{k} (r_{i0} y s_{i2} + r_{i1} y s_{i1} + r_{i2} y s_{i0})$$

where $r_{ij}$ is the sum of the monomials of $r_i$ of degree $j$ with no $y$ occurring, and $s_{ij}$ is defined similarly. This identity can be written as

$$\sum_{i=1}^{n} x_i y z_i = y s(\overline{x}, \overline{z}) + r(\overline{x}, \overline{z}) y + \sum_{i=1}^{k} \left[ \left( \sum_{j=1}^{n} \beta_{ij} x_j + \sum_{j=1}^{n} \gamma_{ij} z_j \right) y \left( \sum_{m=1}^{n} \sigma_{im} x_m + \sum_{m=1}^{n} \tau_{im} z_m \right) \right]$$

for some integers $\beta_{ij}, \gamma_{ij}, \sigma_{im}, \tau_{im}$ and polynomials $r, s$ with integer coefficients.

Using Lemma 2.3 to further restrict to only those monomials involving $x_i$, $y$ and $z_j$, $i \neq j$, we obtain the following identity of $A$

$$0 = \phi_1 y x_i z_j + \phi_2 y z_j x_i + \phi_3 x_i z_j y + \phi_4 z_j x_i y + \psi_{ij} x_i y z_j + \lambda_{ij} z_j y x_i$$

where $\psi_{ij} = \sum_{m=1}^{k} \beta_{mi}\tau_{mj}$ and $\lambda_{ij} = \sum_{m=1}^{k} \gamma_{mj}\sigma_{mi}$. Then Lemma 2.4 shows that $\phi_1 = \phi_4$, $\phi_2 = \phi_3$, and $\psi_{ij} = \lambda_{ij}$ for $i \neq j$.

Similarly considering only the monomials involving $x_i, y$ and $z_i$ we obtain the identity

$$x_i y z_i = \phi_1' y x_i z_i + \phi_2' y z_i x_i + \phi_3' x_i z_i y + \phi_4' z_i x_i y + \psi_{ii} x_i y z_i + \lambda_{ii} z_i y x_i.$$

Again Lemma 2.4 shows that $\phi'_1 = \phi'_4$, $\phi'_2 = \phi'_3$, $\psi_{ii} - 1 = \lambda_{ii}$.

Define $k \times n$ matrices $\beta = (\beta_{ij})$, $\gamma = (\gamma_{ij})$, $\sigma = (\sigma_{ij})$, $\tau = (\tau_{ij})$ and $n \times n$ matrices $\psi = (\psi_{ij})$, $\lambda = (\lambda_{ij})$. Then $\psi - \lambda = I_n$ since $\psi_{ij} = \lambda_{ij}$ if $i \neq j$ and $\psi_{ij} = \lambda_{ii} + 1$. By definition $\psi = \beta^t\tau$, $\lambda = \sigma^t\gamma$ so $\operatorname{rank}\psi \leq \min\{\operatorname{rank}\beta, \operatorname{rank}\tau\} \leq k$ and similarly $\operatorname{rank}\lambda \leq k$. Then $n = \operatorname{rank} I_n = \operatorname{rank}(\psi - \lambda) \leq \operatorname{rank}\psi + \operatorname{rank}\lambda \leq 2k$, contradicting our choice of $n > 2k$. Thus if $V(A)$ has DPC then $A$ must be commutative.

**3. Applications.** Our first result here is an immediate corollary of Theorem 2.5 that answers one of the questions from §1.

THEOREM 3.1. *If $A$ is an algebra over an infinite field, then $V(A)$ has DPC if and only if $A$ is commutative.*

PROOF. Lemma 2.2(i) and Theorem 2.5.

Thus if $F$ is an infinite field and $R = F\langle X, Y\rangle/(\{X, Y\}^3)$, then $V(R)$ does not have DPC. To determine what happens if $F$ is replaced by $\mathbf{Z}$ requires a bit more work.

THEOREM 3.2. *Let $A$ be an algebra over an infinite integral domain $D$. If $A$ is torsion free as a $D$ module, then $V(A)$ has DPC if and only if $A$ is commutative.*

PROOF. Assume that $V(A)$ has DPC. Let $A_l$ be the localization of $A$ at $D\backslash\{0\}$ and let $D_l$ be the localization of $D$ at $D\backslash\{0\}$. Then $D_l$ is just the quotient field of $D$, so it is infinite and $A_l$ is an algebra over $D_l$. By [**3**, Theorem 2, p. 52] $A_l$ satisfies all the identities of $A$, so by Theorem 2.1 $V(A_l)$ has DPC. By Theorem 3.1 $A_l$ is commutative. Since $A$ is torsion free as a $D$ module, the canonical map $A \to A_l$ is an injection, so $A$ is commutative.

An immediate consequence of this result is that $\mathbf{Z}\langle X, Y\rangle/(\{X, Y\}^3)$ does not generate a variety with DPC. This answers another of the questions of §1. Similar results can also be proved for polynomial rings.

THEOREM 3.3. *Let $A$ be an algebra over a field $F$. Then $V(A[x])$ has DPC if and only if $A$ is commutative.*

PROOF. Lemma 2.2(ii) and Theorem 2.5.

As before, we can weaken the requirement that $A$ be an algebra over a field.

THEOREM 3.4. *Let $R$ be a ring and $C$ the subring of $R$ generated by* 1. *If $\operatorname{ann}_C[R, R] = 0$, then $V(R[x])$ has DPC if and only if $R$ is commutative.*

PROOF. $[R, R]$ is the commutator ideal of $R$, which is generated by $\{xy - yx; x, y \in R\}$. Since $C \subset Z(R)$, $\operatorname{ann}_C[R, R] = \{c \in C; c[R, R] = 0\}$. It is straightforward to check that Lemma 2.4 and Theorem 2.5 hold with $F$ replaced by $C$, since the condition that $\operatorname{ann}_C[R, R] = 0$ permits us to conclude that if $c \in C$ and $c(xy - yx) = 0$, then $xy = yx$.

ACKNOWLEDGEMENT. These results are part of the author's Ph.D. thesis written at the University of Waterloo under Professor John Lawrence.

## REFERENCES

1. K. A. Baker, *Definable normal closures in locally finite varieties of groups*, Houston J. Math. **7** (1981), 467–471.
2. S. Burris and J. Lawrence, *Definable principal congruences in varieties of groups and rings*, Algebra Universalis **9** (1979), 152–164.

3. N. Jacobson, *PI-algebras*, Lecture Notes in Math., vol. 441, Springer-Verlag, New York, 1981.
4. R. McKenzie, *Paraprimal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties*, Algebra Universalis **8** (1978), 336–348.
5. C. Procesi, *Rings with polynomial identities*, Marcel Dekker, New York, 1973.
6. L. H. Rowen, *Polynomial identities in ring theory*, Academic Press, New York, 1980.
7. G. E. Simons, *Varieties of rings with definable principal congruences*, Proc. Amer. Math. Soc. **87** (1983), 397–402.

DEPARMENT OF MATHEMATICS AND COMPUTER SCIENCE, ROYAL MILITARY COLLEGE OF CANADA, KINGSTON, ONTARIO, CANADA K7K 5L0