Algebra Universalis, **12** (1981) 148–153

0002–5240/81/002148–06$01.50+0.20/0

Two examples concerning the definability of the disjointness property of principal congruences

STANLEY BURRIS[1] AND JOHN LAWRENCE[2]

In [3] we showed that a variety generated by a finite group or a finite ring need not have definable principal congruences. McKenzie [4] had earlier proved a similar result for varieties generated by finite lattices. One of the major reasons for pursuing the question of which varieties have definable principal congruences has been McKenzie's theorem in [4] which connects this concept with the study of finite bases of equational theories. From known counterexamples it was clear that McKenzie's theorem could not be applied to obtain the far-reaching result of Baker [1]. Nonetheless Baker announced during the Oberwolfach meeting on Universal Algebra in 1976 that a related definability problem has a positive solution in the case of the finitely generated congruence distributive varieties he was considering, namely the definability of "$\theta(a, b) \cap \theta(c, d) = \Delta$," which, following a suggestion of K. Baker, we call the definability of the disjointness property of principal congruences, abbreviated DDPC. (This observation of Baker was used by Burris [2] to simplify the original proof of Baker's theorem.)

One of the directions pursued by those working on finitely based equational theories has been a search for a common generalization of Baker's theorem for congruence distributive varieties, the Oates–Powell theorem for groups, and the Kruse/L'vov theorem for rings. Several natural possibilities were recently excluded by Polin's example in [5] of a finite non-associative ring with a non-finitely based equational theory. In this paper we show that finitely generated varieties of groups and rings need not have DDPC, thus eliminating another possibility.

The reader is referred to [3] for definitions and basic results concerning congruence formulas $\pi(x, y, u, v)$. For a fixed type τ of algebras let Π be the set of congruence formulas. Then for A an algebra of type τ and $a, b, c, d \in A$,

$$(c, d) \in \theta(a, b) \quad \text{iff} \quad A \models \bigvee_{\pi \in \Pi} \pi(c, d, a, b).$$

We will say that a variety V of type τ has DDPC iff there is a first order

[1] Research supported by NRC Grant A7256.

[2] Research supported by NRC Grant A4540 and University of Waterloo Grant 131-7052.

Presented by G. Grätzer. Received January 20, 1979. Accepted for publication in final form September 6, 1979.

formula $\phi(x, y, u, v)$ such that for $a, b, a', b' \in A \in V$,

$$\theta(a, b) \cap \theta(a', b') = \Delta \quad \text{iff} \quad A \models \phi(a, b, a', b').$$

By a compactness argument the following is easily established.

LEMMA 1. *V has* DDPC *iff there is some finite* $\Pi_0 \subseteq \Pi$ *such that for every* $a, b, a', b' \in A \in V$,

$$\theta(a, b) \cap \theta(a', b') = \Delta \text{ iff } A \models \forall x \forall y \left\{ \mathop{\&}_{\pi_1, \pi_2 \in \Pi} [\pi_1(x, y, a, b) \mathscr{E} \pi_2(x, y, a', b') \to x = y] \right\}.$$

For groups [rings] one can replace the notion of principal congruence $\theta(a, b)$ by principal normal subgroup $\langle g \rangle$ [principal ideal $\langle r \rangle$] as in [3] to obtain the following special cases of Lemma 1.

LEMMA 2. *If V is a variety of groups of finite exponent then V has* DDPC *iff there is a natural number n such that for* $g, g' \in G \in V$,

$$\langle g \rangle \cap \langle g' \rangle = \{1\}$$

iff

$$G \models \forall x \left\{ \mathop{\&}_{i,j \leq n} \left[\exists y_0 \cdots \exists y_i \left(x = \prod_{s \leq i} y_s^{-1} g y_s \right) \mathscr{E} \exists z_0 \cdots \exists z_j \left(x = \prod_{t \leq j} z_t^{-1} g' z_t \right) \to x = 1 \right] \right\}.$$

LEMMA 3. *If V is a variety of rings (with* 1) *then V has* DDPC *iff there is a natural number n such that for* $r, r' \in R \in V$, $\langle r \rangle \cap \langle r' \rangle = \{0\}$ *iff*

$$R \models \forall x \left[\exists y_0 \cdots \exists y_{2n+1} \left(x = \sum_{s \leq n} y_{2s} r y_{2s+1} \right) \mathscr{E} \exists z_0 \cdots \exists z_{2n+1} \left(x = \sum_{t \leq n} z_{2t} r' z_{2t+1} \right) \to x = 0 \right].$$

Our first example uses a ring which we have already constructed in [3]. Given a finite field let $R = F[X]$ where $X = \{X_n\}_{n<\omega}$, a set of non-commuting indeterminates, and let I be the ideal of R generated by $\{X_{i_1} \cdots X_{i_4} \mid X_{i_1}, \ldots, X_{i_4} \in X\}$. Also let $R' = F[X_0, X_1, X_2]$ and $I' = R' \cap I$.

THEOREM 4. *With R' and I' as constructed above, R'/I' is finite but* $\mathbf{V}(R'/I')$ *does not have* DDPC.

Proof. From [3] we know that $R/I \in \mathbf{V}(R'/I')$. Given a positive natural number n it is clear that $\langle \sum_{i=1}^{n} X_i X_0 X_i + I \rangle \subseteq \langle X_0 + I \rangle$ holds in R/I. Noting that

$$\left\langle \sum_{i=1}^{n} X_i X_0 X_i + I \right\rangle = \left\{ f \sum_{i=1}^{n} X_i X_0 X_i + I \mid f \in F \right\}$$

we see that if

$$\sum_{r=1}^{m} a_r X_0 b_r + I \in \left\langle \sum_{i=1}^{n} X_i X_0 X_i + I \right\rangle - \{I\}$$

then, after multiplying by a scalar we have

$$\sum_{i=1}^{n} X_i X_0 X_i + I = \sum_{r=1}^{m} a_r' X_0 b_r + I.$$

But then, from Lemma 2.2 in [3] we have $m \geq n$, so by Lemma 3 $\mathbf{V}(R'/I')$ does not have DDPC. □

For the group example we need a variation on the above construction, namely let J be the ideal of R generated by $\{X_0^2, X_0 X_i X_0, X_i X_j\}_{1 \leq i,j}$. The following is almost the same as Lemma 2.2 of [3] with I replaced by J, hence noting that $R/J \in \mathbf{V}(R/I)$ we could also have proved Theorem 4 using R/J rather than R/I.

LEMMA 5. *Let $\{i_1, \ldots, i_n\}$ and $\{j_1, \ldots, j_n\}$ be sets of n distinct positive integers. If*

$$\sum_{k=1}^{n} X_{i_k} X_0 X_{j_k} - \sum_{r=1}^{m} a_r X_0 b_r \in J$$

for some $a_r, b_r \in R$, then $m \geq n$.

Proof. Without loss of generality we can assume $b_r = \sum_{l \geq 1} g_{rl} X_l$ where $g_{rl} \in F$. Thus

$$\sum_{r=1}^{m} a_r X_0 b_r = \sum_{r=1}^{m} a_r X_0 \left(\sum_{l \geq 1} g_{rl} X_l \right)$$
$$= \sum_{l \geq 1} \left(\sum_{r=1}^{m} g_{rl} a_r \right) X_0 X_l,$$

and then it follows that

$$X_{i_k} - \sum_{r=1}^{m} g_{rj_k} a_r \in J.$$

But the $(X_{i_k} + J)$'s are linearly independent over F, so $m \geq n$. □

Let G be the group of units of R/J. Note that if $1+m+J \in G$ and each monomial in m contains X_0 then $(1+m+J)^{-1} = 1-m+J$ and this is a product of conjugates of $1+m+J$ (namely a power of $1+m+J$).

LEMMA 6. *If* $1 \leq i < j$ *then* $1+X_iX_0X_j+X_jX_0X_i+J$ *is a product of conjugates of* $1+X_0+J$.

Proof. Let

$$1+\alpha+J = (1+X_i)(1+X_0)(1-X_i)(1-X_0)+J,$$

a product of conjugates of $1+X_0+J$. Then

$$1+\alpha+J = 1+X_iX_0-X_0X_i-X_iX_0X_i+J.$$

Let

$$\begin{aligned}1+\beta+J &= (1-X_j)(1+\alpha)(1+X_j)+J\\ &= 1+\alpha-X_j\alpha+\alpha X_j+J\\ &= 1+\alpha+X_jX_0X_i+X_iX_0X_j+J\end{aligned}$$

so

$$(1+\beta)(1-\alpha)+J = 1+X_jX_0X_i+X_iX_0X_j+J.$$

Thus $1+X_jX_0X_i+X_iX_0X_j+J$ is a product of conjugates of $1+X_0+J$. □

LEMMA 7. $\mathbf{V}(G)$ *does not have* DDPC *if* $F=\mathrm{GF}(2)$.

Proof. let

$$\gamma+J = \prod_{i=1}^{n} (1+X_{2i-1}X_0X_{2i}+X_{2i}X_0X_{2i-1})+J.$$

Then $\gamma+J$ is central, $(\gamma+J)^2=1+j$, and $\gamma+J$ is a product of conjugates of $1+X_0+J$. Thus

$$\{1+j, \gamma+J\}=\langle\gamma+J\rangle\subseteq\langle 1+X_0+J\rangle.$$

Now if

$$\gamma+J=\prod_{j=1}^{m}(1+a_j)(1+X_0)(1+b_j)+J$$

where

$$(1+a_j+J)^{-1}=1+b_j+J,$$

then

$$\gamma+J=\prod_{j=1}^{m}(1+X_0+a_jX_0+X_0b_j+a_jX_0b_j)+J.$$

It is now clear that we can assume, without loss of generality, that each a_j is a sum of X_i's $i\geq 1$, and hence that $b_j=a_j$. Then, equating the terms of degree 3 in the last equation gives

$$\sum_{i=1}^{n}(X_{2i-1}X_0X_{2i}+X_{2i}X_0X_{2i-1})+J=\sum_{j=1}^{m}a_jX_0a_j+J,$$

and then by Lemma 5, $m\geq n$. Thus by Lemma 2 $\mathbf{V}(G)$ does not have DDPC. □

With $F=GF(2)$ let G' be the group of units of R'/I'.

THEOREM 8. *G' is a finite group and $\mathbf{V}(G')$ does not have* DDPC.

Proof. In [3] we pointed out that the group G'' of units of R/I is in $\mathbf{V}(G')$, and G is a quotient of G'', hence $G\in\mathbf{V}(G')$. Now we apply Lemma 7. □

REFERENCES

[1] K. Baker, *Finite equational bases for finite algebras in congruence distributive equational classes.* Advances in Math. *24* (1977), 207–243.

[2] S. Burris, *On Baker's finite basis theorem for congruence distributive varieties.* Proc. AMS *73* (1979), 141–148.

[3] S. BURRIS and J. LAWRENCE, *Definable principal congruences in varieties of groups and rings.* Alg. Univ. *9* (1979), 152–164.
[4] R. MCKENZIE, *Para primal varieties: a study of finite axiomatizability and definable principal congruences in locally finite varieties.* Alg. Univ. *8* (1978), 336–348.
[5] S. V. POLIN, *Identities of finite algebra.* Sibirsk Mat. Z. *17*(1976), 1356–1366.

University of Waterloo
Waterloo, Ontario
Canada