Definable principal congruences in varieties of groups and rings

Stanley Burris[1] and John Lawrence[2]

In [1] Baldwin and Berman showed that for varieties $\mathcal{V}$ with DPC (definable principal congruences) certain results of Taylor concerning residually small varieties could be sharpened. Their question as to whether every variety generated by a finite algebra has DPC was answered in the negative in [2]; however the question remained open for varieties with permutable congruences. The study of DPC became even more interesting when McKenzie [4] proved that this property could be used, in certain cases (such as a variety generated by a para-primal algebra), to give an easy proof of the finite axiomatizablity of the variety. McKenzie then showed that among lattices only the distributive varieties have DPC, and states that the question of whether varieties generated by a finite group or ring have DPC is open.

In the first section we point out that a variety $\mathcal{V}$ has DPC iff the free algebra on countably many generators in $\mathcal{V}$ has SDPC (strongly definable principal congruences), hence a variety generated by a class $\mathcal{K}$ of algebras has DPC iff the quasi-variety generated by $\mathcal{K}$ has DPC. In the second section a finite ring R is constructed such that the variety generated by R does not have DPC. In the third section we prove that if the variety generated by a finite group G has DPC then G must be nilpotent; on the other hand if G is nilpotent class 2 and finite then indeed it generates a variety with DPC. It follows that the properties of having DPC and being finitely axiomatizable are independent for quasi-varieties generated by a finite group. Finally Baldwin's theorem[3] that the variety of all groups of exponent 3 has DPC is shown to be best possible for Burnside varieties.

§1. General results on definable principal congruences

For A an algebra and $a, b \in A$ let $\theta_A(a, b)$ denote the principal congruence on A generated by (a, b). If $\mathcal{K}$ is a class of algebras (for this section we assume that

Presented by G. Grätzer. Received January 27, 1977. Accepted for publication in final form November 14, 1977.

[1] Research supported by NRC Grant A7256

[2] Research supported by University of Waterloo Research Grant 131–7052

[3] The author has kindly permitted us to include this theorem in our manuscript.

we are working within a fixed similarity type) then we say $\mathscr{K}$ has DPC (*definable principal congruences*) if there is a first-order formula $\phi(x, y, u, v)$ such that for any $A \in \mathscr{K}$ and $a, b, c, d \in A$, $(a, b) \in \theta_A(c, d)$ iff $A \models \phi(a, b, c, d)$. A formula $\pi(x, y, u, v)$ of the form

$$\exists \vec{z}[x = p_0(\sigma_0(0), \vec{z}) \;\&\; y = p_n(\sigma_n(1), \vec{z}) \;\&\; \mathop{\&}_{i=0}^{n-1} p_i(\sigma_i(1), \vec{z}) = p_{i+1}(\sigma_{i+1}(0), \vec{z})],$$

where the $p_0, \ldots, p_n$ are arbitrary polynomials in the language of the algebras being considered, and $\{\sigma_i(0), \sigma_i(1)\} = \{u, v\}$, $0 \le i \le n$, will be called a *congruence formula*. Let Π denote the collection of all congruence formulas (in the given language). Then a well known theorem of Mal'cev asserts that for $a, b, c, d \in A$,

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

LEMMA 1.1. *If $\mathscr{K}$ is closed under ultraproducts then $\mathscr{K}$ has* DPC *implies there is a finite subset Π' of Π such that*

$$\mathscr{K} \models \bigvee_{\pi \in \Pi} \pi(x, y, u, v) \leftrightarrow \bigvee_{\pi' \in \Pi'} \pi'(x, y, u, v).$$

Proof. (Standard.)

Let $\mathbf{V}(\mathscr{K})$ be the *variety* generated by $\mathscr{K}$, and $\mathbf{Q}(\mathscr{K})$ the *quasivariety* generated by $\mathscr{K}$. $F_{\mathscr{K}}$ denotes the *free algebra* in $\mathbf{V}(\mathscr{K})$ *with countably many free generators*. $\mathscr{K}$ has SDPC (*strongly definable principal congruences*) if the conclusion of Lemma 1.1 holds. An open formula $\omega(x, y, u, v, \vec{z})$ is *congruence-generating* if $\exists \vec{z}\omega \in \Pi$. Let Γ be the set of all congruence-generating formulas.

THEOREM 1.2. *For any class $\mathscr{K}$ of algebras we have the following.*

(a) $\mathbf{V}(\mathscr{K})$ *has* DPC *iff* $\mathbf{Q}(\mathscr{K})$ *has* DPC *iff* $F_{\mathscr{K}}$ *has* SDPC.

(b) $F_{\mathscr{K}}$ *has* SDPC *iff there is a finite subset Γ' of Γ such that for each $\omega(x, y, u, v, z_0, \ldots, z_n) \in \Gamma$ we can find a formula $\omega'(x, y, u, v, z_0, \ldots, z_k) \in \Gamma'$ and polynomials $p_i(x, y, u, v, z_0, \ldots, z_n)$, $0 \le i \le k$, such that*

$$\mathscr{K} \models \omega(x, y, u, v, z_0, \ldots, z_n) \rightarrow \omega'(x, y, u, v, p_0, \ldots, p_k).$$

Proof. First we show that (b) holds. So suppose that Π' is a finite subset of Π such that $F_{\mathscr{K}}$ satisfies the conclusion of Lemma 1.1. Then let Γ' be the set of formulas ω' such that $\exists \vec{z}\omega' \in \Pi'$. Then for $\omega(x, y, u, v, z_0, \ldots, z_n) \in \Gamma$ let $\bar{x}, \bar{y}$, etc. be a mapping of the variables of ω into $F_{\mathscr{K}}$ such that $\bar{u}, \bar{v}, \bar{z}_0, \ldots, \bar{z}_n$ are distinct free generators and

$$F_{\mathscr{K}} \models \omega(\bar{x}, \bar{y}, \bar{u}, \bar{v}, \bar{z}_0, \ldots, \bar{z}_n).$$

Then with $\pi = \exists\ \vec{z}\omega$, it follows that there must be a $\pi' \in \Pi'$, say $\pi' = \exists\ \vec{z}\omega'$, where ω' is $\omega'(x, y, u, v, z_0, \ldots, z_k)$, such that

$$F_{\mathscr{K}} \models \pi'(\bar{x}, \bar{y}, \bar{u}, \bar{v}).$$

As $F_{\mathscr{K}}$ is free we can find polynomials $p_i(x, y, u, v, z_0, \ldots, z_n)$, $0 \leq i \leq k$, such that, with $\bar{p}_i = p_i(\bar{x}, \bar{y}, \bar{u}, \bar{v}, \bar{z}_0, \ldots, \bar{z}_n)$, we have

$$F_{\mathscr{K}} \models \omega'(\bar{x}, \bar{y}, \bar{u}, \bar{v}, \bar{p}_0, \ldots, \bar{p}_k).$$

But now an easy argument using the fact that ω, ω' are conjuncts of atomic formulas with x and y being equal to polynomials in the other variables shows that indeed

$$\mathscr{K} \models \omega(x, y, u, v, z_0, \ldots, z_n) \rightarrow \omega'(x, y, u, v, p_0, \ldots, p_k).$$

For the other half of (b) note that implications of the form immediately above are preserved by subdirect products, hence

$$\mathscr{K} \models \omega(x, y, u, v, z_0, \ldots, z_n) \rightarrow \omega'(x, y, u, v, p_0, \ldots, p_k)$$

implies

$$F_{\mathscr{K}} \models \omega(x, y, u, v, z_0, \ldots, z_n) \rightarrow \omega'(x, y, u, v, p_0, \ldots, p_k).$$

But then it is clear that Π' equal to the finite set of formulas $\exists\ \vec{z}\omega'$, where $\omega' \in \Gamma'$, will suffice to show that $F_{\mathscr{K}}$ has SDPC.

Now, to prove (a) it suffices to show that $F_{\mathscr{K}}$ has SDPC implies $\mathbf{V}(\mathscr{K})$ has DPC since $F_{\mathscr{K}} \in \mathbf{Q}(\mathscr{K}) \subseteq \mathbf{V}(\mathscr{K})$, noting that $\mathbf{Q}(\mathscr{K})$ has SDPC if it has DPC by Lemma 1.1. So assume $F_{\mathscr{K}}$ has SDPC and let Γ' be as in (b). Then for $\omega \in \Gamma, \omega' \in \Gamma'$, and polynomials p_i such that

$$\mathscr{K} \models \omega(x, y, u, v, z_0, \ldots, z_n) \rightarrow \omega'(x, y, u, v, p_0, \ldots, p_k),$$

it follows that we have the more general assertion

$$\mathbf{V}(\mathscr{K}) \models \omega(x, y, u, v, z_0, \ldots, z_n) \rightarrow \omega'(x, y, u, v, p_0, \ldots, p_k),$$

and thus with $\Pi' = \{\exists\, \vec{z}\omega' \mid \omega' \in \Gamma'\}$ it is straightforward to show that $\mathbf{V}(\mathcal{K})$ has SDPC, hence DPC.

In the next two sections it is more useful to work with the following slight modification of Theorem 1.2b (however the proof is exactly the same).

THEOREM 1.3. *If Γ^* is a subset of Γ such that for any $\omega(x, y, u, v, \vec{z})$ in Γ there is an $\omega^*(x, y, u, v, \vec{w})$ in Γ^* such that*

$$\mathbf{V}(\mathcal{K}) \models \exists\, \vec{z}\omega(x, y, u, v, \vec{z}) \to \exists\, \vec{w}\omega^*(x, y, u, v, \vec{w})$$

than Theorem 1.2b holds with Γ replaced by Γ^*.

§2. A finite ring R such that $\mathbf{V}(R)$ does not have DPC

We will now restrict out attention to the language $\{+, \cdot, -, 0, 1\}$ of *rings with unity*. It is clear that a class $\mathcal{K}$ of rings has DPC iff there is a first-order formula $\phi(x, y)$ such that for $R \in \mathcal{K}$ and $a, b \in R$, $a \in (b)_R$ iff $R \models \phi(a, b)$, where $(b)_R$ is the principal two-sided ideal of R generated by b. Let $\pi_n(x, y)$ be the formula

$$\exists\, z_0 \cdots \exists\, z_{2n+1}\left(x = \sum_{i=0}^{n} z_{2i} y z_{2i+1}\right).$$

Then one has $a \in (b)_R$ iff $R = \bigvee_{n<\omega} \pi_n(a, b)$. For the class of rings we have $\pi_n(x, y) \to \pi_{n+1}(x, y)$, $n < \omega$, so Theorem 1.3 leads to the following.

LEMMA 2.1. *If $\mathcal{K}$ is a class of rings with unity then $\mathbf{V}(\mathcal{K})$ has DPC iff there are natural numbers k, n with $k < n$, and polynomials $r_i(y, z_0, \ldots, z_{2n+1})$, $s_i(y, z_0, \ldots, z_{2n+1})$, $0 \le i \le n-1$, such that K satisfies the identity*

$$\sum_{i=0}^{n} z_{2i} y z_{2i+1} = \sum_{i=0}^{k} r_i(y, \vec{z}) y s_i(y, \vec{z}).$$

For a given field F and set $X = \{x_i\}_{i<\omega}$ of non-commuting indeterminates let $R = F[X]$. Let I be the ideal generated by X^4, i.e. all products of four elements of X.

LEMMA 2.2. *If r_i and s_i are elements of R such that*

$$\sum_{i=1}^{n} x_i x_0 x_i - \sum_{i=1}^{k} r_i x_0 s_i \in I$$

then $k \ge n$.

Proof. Let $r_i = a_i + b_i$ where a_i and b_i are both sums of monomials with the property that each monomial in a_i is either a scalar or begins with x_0, and no non-zero monomial of b_i is a scalar or begins with x_0. Likewise let $s_i = c_i + d_i$ where each of c_i and d_i is a sum of monomials with each monomial in c_i either a scalar or ending in x_0, and no non-zero monomial of d_i is a scalar or ends in x_0. Then from

$$\sum_{i=1}^{n} x_i x_0 x_i - \sum_{i=1}^{k} a_i x_0 s_i - \sum_{i=1}^{k} b_i x_0 s_i \in I$$

follows

$$\sum_{i=1}^{n} x_i x_0 x_i - \sum_{i=1}^{k} b_i x_0 s_i \in I$$

since the expansion of the middle summation gives precisely those monomials starting with x_0. Similarly we can conclude from the last formula

$$\sum_{i=1}^{n} x_i x_0 x_i - \sum_{i=1}^{k} b_i x_0 d_i \in I.$$

Without loss of generality we can now assume that each b_i and d_i is a linear combination of the indeterminates $x_1, \ldots, x_n$, say $d_i = \sum_{j=1}^{n} a_{ij} x_j$, $a_{ij} \in F$. Then

$$\sum_{i=1}^{n} x_i x_0 x_i = \sum_{i=1}^{k} b_i x_0 d_i = \sum_{i=1}^{n} \left[\sum_{j=1}^{k} a_{ji} b_j \right] x_0 x_i$$

hence

$$x_i = \sum_{j=1}^{k} a_{ji} b_j, \qquad 1 \leq i \leq n.$$

But $x_1, \ldots, x_n$ are linearly independent over F, hence $k \geq n$.

LEMMA 2.3. $\mathbf{V}(R/I)$ *does not have* DPC.

Proof. Just combine Lemmas 2.1 and 2.2.

Now let R' be the ring $F[x_0, x_1, x_2]$, and let I' be the ideal of R' generated by $\{x_0, x_1, x_2\}^4$.

THEOREM 2.4. $\mathbf{V}(R'/I')$ *does not have* DPC.

Proof. By Lemma 2.3 it suffices to show that $R/I \in \mathbf{V}(R'/I')$, where of course we are using the same field F for the polynomial rings R and R'. Let us say that a sum of monomials in R is reduced if it cannot be written as a sum of fewer monomials. Suppose $\sum_{0\le i\le t} m_i$ is a reduced sum of monomials in R but not in I. Then m_0 is not in I, and after applying a suitable automorphism (determined by a bijection of the indeterminates) we can further assume that m_0 is in R' but not in I'. Then the homomorphism $\alpha: R/I \to R'/I'$ satisfying $\alpha(x_i) = x_i$ if $0 \le i \le 2$, and $\alpha(x_i) = 0$ if $i > 2$, is such that $\alpha(m_0 + I) \ne 0$, hence $\alpha(\sum_{0\le i\le t} m_i + I) \ne 0$, so R/I is a subdirect power of R'/I'.

Letting F be a finite field we obtain a finite ring R'/I' such that $\mathbf{V}(R'/I')$ does not have DPC. These rings are rather large, however, for if F is the two-element field then R'/I' has 2^{40} elements. One can sharpen the above argument slightly by increasing I' and reducing R' to $F[x_0, x_1]$ to obtain a ring with only 64 elements such that the variety it generates does not have DPC.

§3. The DPC property for varieties of groups.

For groups we have, parallel to the reasoning which led to Lemma 2.1, the following.

LEMMA 3.1. *If $\mathcal{K}$ is a class of groups of finite exponent then $\mathbf{V}(\mathcal{K})$ has* DPC *iff for some $n > k \ge 0$ and polynomials $p_i(y, x_0, \dots, x_n)$, $0 \le i \le k$, the class $\mathcal{K}$ satisfies the identity*

$$\prod_{i=0}^{n} x_i^{-1} y x_i = \prod_{i=0}^{k} p_i^{-1}(y, x_0, \dots, x_n) y p_i(y, x_0, \dots, x_n). \tag{*}$$

It is well-known that the variety of Abelian groups of exponent e has DPC, for $e < \omega$. A simple extension of this result gives our strongest positive result.

THEOREM 3.2. *If $\mathcal{V}$ is the variety of nilpotent class 2 groups of exponent e (where e is finite) then $\mathcal{V}$ has* DPC.

Proof. By Lemma 3.1 it suffices to show that $\mathcal{V}$ satisfies

$$\prod_{i=0}^{e} x_i^{-1} y x_i = (x_0 \dots x_e)^{-1} y (x_0 \dots x_e).$$

But this is an easy consequence of the existence of a polynomial $p(x, y)$ such that $\mathcal{V}$ satisfies the identities $zp(x, y) = p(x, y)z$ and $x^{-1}yx = yp(x, y)$.

The next lemma contains the key observation for showing that various groups generate varieties without DPC.

LEMMA 3.3. *Let G be a group of finite exponent e and with elements a, b such that b commutes with each $a^{-i}ba^{i}$, $1 \leq i < e$. If G satisfies an identity* (*) *and t is any natural number such that $b = a^{-t}ba^{t}$ then for any finite sequence $i_0, \ldots, i_m$ of natural numbers with $i_0 + \cdots + i_m \equiv 0 \bmod (t)$ it follows that*

$$b^{m+1} = \prod_{j=0}^{m} a^{-i_j} b a^{i_j}.$$

Thus, in particular,

$$b^t a = ab^t.$$

Proof. Suppose an identity of the form (*) holds in G. Then we select an identity of the form (*) which holds in G such that $n > me^{k+1}$. This is indeed possible as (*) implies that for *any* s there is an $r < n$ and q_i such that $\prod_{i=0}^{s} x_i^{-1} y x_i = \prod_{i=0}^{r} q_i^{-1}(y, x_0, \ldots, x_s) y q_i(y, x_0, \ldots, x_s)$ holds in $\mathcal{V}$, e.g.

$$\prod_{i=0}^{n+1} x_i^{-1} y x_i = \left(\prod_{i=0}^{n} x_i^{-1} y x_i\right) x_{n+1}^{-1} y x_{n+1}$$
$$= \left(\prod_{i=0}^{k} p_i^{-1} y p_i\right) x_{n+1}^{-1} y x_{n+1}, \text{ etc., so we can choose } s > me^{n+1}$$

and then an appropriate $r < n$ to obtain a suitable form of (*).

Let us write out the expression $p_i^{-1}(y, x_0, \ldots, x_n) y p_i(y, x_0, \ldots, x_n)$ in the form

$$(x_{\lambda_0}^{\pm\mu_0} y^{\pm\sigma_0} x_{\lambda_1}^{\pm\mu_1} y^{\pm\sigma_1} \cdots x_{\lambda_s}^{\pm\mu_s}) y (x_{\lambda_s}^{\mp\mu_s} y^{\mp\sigma_{s-1}} x_{\lambda_{s-1}}^{\mp\mu_{s-1}} \cdots x_{\lambda_0}^{\mp\mu_0}).$$

If we now assume that y commutes with $x_{\lambda_i}^{\pm\mu_i} y x_{\lambda_i}^{\mp\mu_i}$ and the x_i's commute with each other (which is true if we let $y \in \{b, 1\}$, $x_i \in \{1, a, \ldots, a^{e-1}\}$) then this can be rewritten as

$$(x_0^{-t_{i0}} \cdots x_n^{-t_{in}}) y (x_0^{t_{i0}} \cdots x_n^{t_{in}}), \qquad 0 \leq t_{ij} < e,$$

by cancelling the y^{σ_i}'s and collecting terms. Thus for $\alpha(x_i) \in \{1, a, \ldots, a^{e-1}\}$,

$$p_i(1, \alpha(\vec{x})) = \alpha(x_0)^{t_{i0}} \cdots \alpha(x_n)^{t_{in}}, \quad \text{so}$$

$$p_i^{-1}(1, \alpha(\vec{x})) b p_i(1, \alpha(\vec{x})) = p_i^{-1}(b, \alpha(\vec{x})) b p_i(b, \alpha(\bar{x})).$$

An easy counting argument shows that for some $x_{j_0}, \ldots, x_{j_m}$, $0 \leq j_0 < j_1 < \cdots < j_m \leq n$ we must have $t_{ij_0} = \cdots = t_{ij_m}$ for $0 \leq i \leq k$. For let E be the equivalence relation on $\{0, \ldots, n\}$ defined by $r \approx s$ iff $t_{ir} = t_{is}$, $0 \leq i \leq k$. This divides $\{0, \ldots, n\}$ into $\leq e^{k+1}$ classes (as each $t \in \{0, \ldots, e-1\}$). Consequently if $n > me^{k+1}$ then some class will contain $> m$ elements, i.e. there will be $j_0 < j_1 < \cdots < j_m \leq n$ such that $t_{ij_0} = t_{ij_1} = \cdots = t_{ij_m}$ for $0 \leq i \leq k$. Now define $\alpha(x_{j_s}) = a^{i_s}$, $0 \leq s \leq m$, and $\alpha(x_j) = 1$ otherwise; and let $\beta(x_j) = 1$ for $0 \leq j \leq n$. Then, for $0 \leq i \leq k$, we can use the congruence $i_0 + \cdots + i_m \equiv 0 \bmod (t)$ to show

$$p_i^{-1}(1, \beta(\vec{x}))bp_i(1, \beta(\vec{x})) = p_i^{-1}(1, \alpha(\vec{x}))bp_i(1, \alpha(\vec{x})),$$

and hence

$$p_i^{-1}(b, \beta(\vec{x}))bp_i(b, \beta(\vec{x})) = p_i^{-1}(b, \alpha(\vec{x}))bp_i(b, \alpha(\vec{x})).$$

But then from (*) we must have

$$\prod_{i=0}^{n} \beta(x_i)^{-1}b\beta(x_i) = \prod_{i=0}^{n} \alpha(x_i)^{-1}b\alpha(x_i),$$

that is,

$$b^{n+1} = b^{n-m} \prod_{j=0}^{m} a^{-i_j}ba^{i_j},$$

and thus

$$b^{m+1} = \prod_{j=0}^{m} a^{-i_j}ba^{i_j}.$$

Finally, with $m = t-1$ and $i_0 = \cdots = i_m = 1$ we have $b^ta = ab^t$.

COROLLARY 3.4. *The variety* $\mathbf{V}(D_n)$, *where* D_n *is the dihedral group of order* $2n$, *has* DPC *iff* $n = 1,2$ *or* 4.

Proof. If $n = 4$ then D_n is nilpotent class 2, hence Theorem 3.2 applies. If $n > 4$ or $= 3$ then, as D_n has the presentation $\{a^2 = 1,\ b^n = 1,\ aba = b^{-1}\}$, we can use this a and b in Lemma 3.3 to show $\mathbf{V}(D_n)$ does not have DPC by letting $t = 2$ and noting that $ab^2 \neq b^2a$.

Now we are in a position to show that for quasi-varieties generated by finite groups the properties of having DPC and having a finitely axiomatizable theory are independent, in view of Ol'šanskiĭ's theorem.

THEOREM 3.5. (Ol'šanskiĭ [6]) *For G a finite group $\mathbf{Q}(G)$ is finitely axiomatizable iff all Sylow subgroups of G are Abelian.*

Thus, for the two-element group Z_2, $\mathbf{Q}(Z_2)$ has DPC and is finitely axiomatizable. The symmetric group on three letters, S_3, is such that $\mathbf{Q}(S_3)$ is finitely axiomatizable but does not have DPC. $\mathbf{Q}(D_4)$ has DPC, but is not finitely axiomatizable; and $\mathbf{Q}(D_8)$ has neither property. (According to Ol'šanskiĭ [5] the first two examples are actually varieties.)

We return to our study of finite groups G such that $\mathbf{V}(G)$ does not have DPC.

LEMMA 3.6. *If G is a finite solvable group and $\mathbf{V}(G)$ has* DPC *then G is nilpotent.*

Proof. We proceed by induction on $|G|$, the cardinality of G. For $|G|=1$ the argument is trivial, so suppose $|G|>1$ and the lemma holds for all groups smaller than G. Let H be a proper normal subgroup such that G/H is a cyclic q-group (q being a prime number). If $\mathbf{V}(G)$ has DPC then clearly $\mathbf{V}(H)$ has DPC, hence H is nilpotent. If H is a q-group then G is also a q-group and we are finished. Otherwise H has a non-trivial Sylow p-group S with $p \neq q$. Let C be the center of S. Then choose $g \in G$ such that g/H generates G/H and the order of g is q^m for some m. Since $g^{-1}Sg \subseteq H$ and S is a Sylow subgroup of H we have $g^{-1}Sg = S$, and thus $g^{-1}Cg = C$ as the center of H is invariant under automorphisms.

We want to show that C is in the center of G. For this it suffices to show that g commutes with elements of C. If $c \in C$ then from Lemma 3.3, with t the order of g, follows $gc^t = c^t g$. But since g and c have relatively prime orders this implies $gc = cg$. Thus $|G/C(G)| < |G|$, $C(G)$ being the center of G, so $G/C(G)$ is nilpotent as $\mathbf{V}(G/C(G))$ has DPC, hence G is nilpotent.

THEOREM 3.7. *If G is a finite group such that $\mathbf{V}(G)$ has* DPC *then G is nilpotent.*

Proof. Again we use induction on the cardinality of G. The ground case is trivial, so suppose $|G|>1$ and the theorem holds for all smaller groups. As the proper subgroups of G are nilpotent (by induction), a theorem in [7] (p. 148) says G is solvable, and we apply Lemma 3.6.

Originally we conjectured that Theorem 3.7. could be improved to state "then

G is nilpotent class 2". Examples of nilpotent class 3 groups which we examined included D_8, the generalized quaternions, and the group of units of the local ring R'/I' defined in §2. In these cases we knew the conjecture to be true. However Baldwin soon informed us that, thanks to a suggestion of P. Fong, he has proved the following result, negating the conjecture. In the following we let $y^x = x^{-1}yx$ and $[x, y] = x^{-1}y^{-1}xy$.

THEOREM 3.8. (Baldwin) *The variety of all groups of exponent* 3 *has definable principal congruences.*

Proof. First we list some basic facts about groups of exponent 3 (see [3], p. 150, p. 321, 322):

(a) commutators of weight four give the identity element,
(b) for any element y, all conjugates and commutators of y commute,
(c) $[x, y, z] = [y, z, x]$,
(d) $[x, yz] = [x, y][x, z][x, y, z]$,
(e) $[x, y, z]^{-1} = [x, z, y]$.

Claim 1: $[x, y, uv] = [x, y, u][x, y, v]$ (from a, b, d).

Claim 2: $y^{x_1 \cdots x_n} = y \prod_{1 \le i \le n} [y, x_i] \prod_{1 \le i < j \le n} [y, x_i, x_j]$.

Proof. This is clearly true for $n = 1$, and easily checked for $n = 2$ using (d), so assuming it is true for $k < n$, we have

$$\begin{aligned} y^{x_1 \cdots x_n} &= y[y, x_1 \ldots x_n] \\ &= y[y, x_1][y, x_2 \ldots x_n][y, x_1, x_2 \ldots x_n] \qquad \text{by (d)} \end{aligned}$$

so, using the induction hypothesis and (1), this is

$$= y[y, x_1]\Big(\prod_{2 \le i \le n} [y, x_i] \prod_{2 \le i < j \le n} [y, x_i, x_j] \Big) \prod_{2 \le j \le n} [y, x_1, x_j]$$

= the desired answer by (b).

Claim 3: $[x,[y, z]] = [x, z, y]$.

Proof.

$$\begin{aligned} [x,[y, z]] &= [[y, z], x]^{-1} \\ &= [y, z, x]^{-1} \\ &= [y, x, z] \qquad \text{by (e)} \\ &= [x, z, y] \qquad \text{by (c)}. \end{aligned}$$

Claim 4:

$$y^{\prod_{1\le i<j\le n}[x_j, x_i]} = y \prod_{1\le i<j\le n} [y, x_i, x_j]$$

Proof. Use (2), (3) and (a).

Claim 5:

$$y^n y^{x_1\cdots x_n} = y^{x_1}\dots y^{x_n} y^{\prod_{1\le i<j\le n}[x_j, x_i]}.$$

Proof. This is immediate from (b), (2) and (4) as $y^{x_i} = y[y, x_i]$.

Claim 6: $y^{x_1}\dots y^{x_n} = y^n y^{x_1\cdots x_n}(y^{\prod_{1\le i<j\le n}[x_j, x_i]})^2$ follows from claim 5 and the exponent 3 law.

Thus

$$y^{x_1}\dots y^{x_6} = (y^{x_1\cdots x_6})(y^{\prod_{1\le i<j\le 6}[x_j, x_i]})^2,$$

hence by Lemma 3.1 the variety of groups of exponent 3 has DPC.

Baldwin's result is best possible for the Burnside varieties, i.e. varieties of groups defined by an equation $x^n = 1$, as we shall see. Letting R be the ring $F[X]$, F a finite field, and I the ideal defined in §2, note that for $m \in XF[X]$ the element $1 + m + I$ is a unit of the ring R/I as $(1+m)(1-m+m^2-m^3)+I = 1+I$. Let G be the subgroup of the group of units of R/I consisting of those elements of the form $1 + m + I$, $m \in XF[X]$.

LEMMA 3.9. *With R and I as defined above suppose*

$$\prod_{1\le i\le n} (1+x_i)^{-1}(1+x_0)(1+x_i) - \prod_{1\le i\le k} (1+m_i)^{-1}(1+x_0)(1+m_i) \in I$$

where $m_i \in XF[X]$. *Then* $k \ge n$.

Proof. The above can be written as

$$\prod_{1\le i\le n} (1-x_i+x_i^2-x_i^3)(1+x_0)(1+x_i) - \prod_{1\le i\le k} (1-m_i+m_i^2-m_i^3)(1+x_0)(1+m_i) \in I$$

so

$$\prod_{1\le i\le n} [1+(1-x_i+x_i^2)x_0(1+x_i)] - \prod_{1\le i\le k} [1+(1-m_i+m_i^2)x_0(1+m_i)] \in I.$$

From this follows (collecting terms of degrees 3 with x_0 only in the middle)

$$\sum_{1\le i\le n} x_i x_0 x_i - \sum_{i\in J} m_i x_0 m_i \in I, \quad \text{for some} \quad J\subseteq\{1, \ldots, k\},$$

hence by Lemma 2.2, $k \ge n$.

LEMMA 3.10. *For G as defined above,* $\mathbf{V}(G)$ *does not have* DPC.

Proof. An easy consequence of Lemma 3.9 in view of Lemma 3.1.

Let R' and I' be as defined in §2, and let G' be the finite group of units of R'/I' of the form $1+m+I'$, $m\in\{x_0, x_1, x_2\}F[\{x_0, x_1, x_2\}]$.

LEMMA 3.11. For G' as defined above, $\mathbf{V}(G')$ does not have DPC.

Proof. This follows from noting that G is a subdirect power of G' (since R/I is a subdirect power of R'/I' as shown in §2) and Lemma 3.10.

THEOREM 3.12. *Let $\mathcal{V}_n$ be the variety of groups defined by $x^n = 1$. Then $\mathcal{V}_n$ has* DPC *iff $n \le 3$.*

Proof. $\mathcal{V}_2$ consists of abelian exponent 2 groups, hence it satisfies $\prod_{0\le i\le 2} x_i^{-1} y x_i = y$, so by Lemma 3.1 it has DPC. $\mathcal{V}_3$ was discussed in Theorem 3.8. For $n=4$ let F be the two element field and note that $(1+m)^4 + I = 1 + I$ for $m\in XF[X]$, hence the corresponding G' is in $\mathcal{V}_4$, so by Lemma 3.11 $\mathcal{V}_4$ does not have DPC. Consequently, if $4\mid n$ then $\mathcal{V}_4 \subseteq \mathcal{V}_n$ so $\mathcal{V}_n$ does not have DPC. For $n=6$ note that $D_3\in\mathcal{V}_6$, so Corollary 3.4 says $\mathcal{V}_6$ does not have DPC. Finally, if $n>3$, $n\ne 6$ and $4\nmid n$ then for some prime $p\ge 5$, $p\mid n$. For this case let F be the p-element field and observe that $(1+m)^p + I = 1 + I$ for $m\in XF[X]$, so the corresponding G' is in $\mathcal{V}_p$, hence in $\mathcal{V}_n$. Then again by Lemma 3.11, $\mathcal{V}_n$ does not have DPC.

PROBLEM 1. Complete the classification of finite groups G such that $\mathbf{V}(G)$ has DPC. (In particular, is there a finite group which does not satisfy $x^3 = 1$ and is not nilpotent class 2 such that $\mathbf{V}(G)$ has DPC?)

PROBLEM 2. Carry out a similar program for rings, looking at questions such as: is there an interesting connection between a local ring and its group of units insofar as the property DPC is concerned?

REFERENCES

[1] JOHN BALDWIN and JOEL T. BERMAN, *The number of subdirectly irreducible algebras in a variety.* Alg. Univ. *5* (1975), 379–389.

[2] STANLEY BURRIS, *An example concerning definable principal congruences.* Alg. Univ. *7* (1977), 403–404.

[3] M. HALL, JR., *The Theory of Groups*, Macmillan Co., N.Y., 1959.

[4] RALPH MCKENZIE, *Para-primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties.* (Preprint).

[5] A. JU. OL'ŠANSKIĬ, *Varieties of finitely approximable groups.* Izv. Akad. Nauk SSSR Ser. Mat. *33* (1969), 915–927.

[6] A. JU. OL'ŠANSKIĬ, *Conditional identities in finite groups.* Sibirsk. Mat. Z. *15* (1974), 1409–1413, 1432.

[7] W. R. SCOTT, *Group Theory*, Prentice Hall, 1964, Englewood Cliffs, N. J.

University of Waterloo
Waterloo, Ontario
Canada