UNIVERSITÄT KAISERSLAUTERN

Derived Varieties of Semigroups and Groupoids

Dietmar Schweigert and S.L. Wismath

Preprint Nr. 281

ISSN 0943-8874

Juni 1996

FACHBEREICH MATHEMATIK

Derived Varieties of Semigroups and Groupoids

D. Schweigert and S.L. Wismath*

1 Introduction

Solid varieties are varieties in which every identity also holds as a hyperidentity; that is, every identity of the variety holds not only for the fundamental operations of the variety but also for any other choice of terms of the appropriate arities. As Schweigert has pointed out in [17], this is equivalent to having the variety closed under the usual H, S and P operators plus the additional operator D of formation of all derived algebras. A derived algebra is formed from an algebra by replacing the fundamental operations by some choice of terms of the algebra (of appropriate arity).

In this paper, we consider some variations of derived algebras and the corresponding derived varieties. We use these to define two new concepts, semisolidity and mutual solidity of varieties, and begin the investigation of their properties. In particular, we present a number of examples, based on varieties of semigroups and groupoids. An important tool in these examples is the idea of a derivation diagram, describing for a particular variety or algebra its derived varieties or algebras. The derivation diagram gives some insight into the ordered set of subclones of the clone of a groupoid. One of the motivations of our work is the fact that mutual solidity preserves the finite basis property and Mal'cev conditions, and gives a way to study the equivalence of varieties of the same type.

In Section 2 we introduce the basic concepts to be studied, with definitions of mutually solid and semisolid varieties, and derivation diagrams. These definitions are given for varieties of arbitrary type, but our examples will all be varieties of type <2>. Section 3 presents an investigation of semisolidity and mutual solidity for the varieties of bands, with derivation diagrams for all the varieties of regular bands. Sections 4 and 5 explore derived algebras of cyclic p-groups, and look at two examples of derived groupoids of 3-element groupoids. Finally in Section 6 we look briefly at the interaction of derived algebras with the theory of types of Hobby and McKenzie.

*Research supported by NSERC of Canada

2 Basic Concepts

Let V be a variety, of a fixed type $\tau =< n_0, n_1, \ldots, n_\gamma, \ldots >$, with fundamental operations $F =< f_0, f_1, \ldots, f_\gamma, \ldots >$. Let $\sigma =< t_0, t_1, \ldots, t_\gamma, \ldots >$ be a fixed choice of terms of V, with t_i having arity n_i, $i \geq 0$. For any algebra, $\underline{A} =< A; F >$ in V, the algebra $< A; \sigma >$ is called a derived algebra of $\underline{A}$ (corresponding to σ), and will be denoted by $d_\sigma(\underline{A})$. The σ-derived variety of V, or the variety derived from V using σ, is the variety $d_\sigma(V)$ generated by $\{d_\sigma(\underline{A}) : \underline{A} \in V\}$. A variety $d_\sigma(V)$ is called a derived variety or a derivative of V.

An observation that will be useful later is that if S is a set of generators of the variety V, then $\{d_\sigma(\underline{A}) : \underline{A} \in S\}$ also generates $d_\sigma(V)$. It is well known that it is not always the case that $d_\sigma(V) \subseteq V$. A variety V is called solid if every derived variety of V is contained in V; that is, when $d_\sigma(V) \subseteq V$ for every possible choice σ of appropriate terms. Solid varieties were defined by Graczynska & Schweigert in [10], and solid varieties of semigroups have been studied in [5], [18].

We now introduce two variations of the concept of solidity. First, if two algebras $\underline{A}$ and $\underline{B}$ are each derived algebras of the other, we call them mutually derived algebras. If for a particular choice σ of terms, $(A; F)$ and $(A; \sigma)$ are mutually derived for every $(A; F)$ in V, we call σ an F-equivalent choice of terms. In this case, the derived variety $d_\sigma(V)$ will be called a mutually derived variety of V.

We will call a variety V mutually solid if every mutually derived variety of V is contained in V, and semisolid if every mutually derived variety of any subvariety of V is contained in V.

We may consider the join of all the mutually derived varieties of a given variety V. This variety always contains V (since V is trivially mutually derived from itself), but may be larger. Then V is mutually solid iff this join variety is contained in V, while V is semisolid if this inclusion still holds when the join is extended to include all mutually derived varieties of all subvarieties of V.

It is clear that solidity implies semisolidity, which in turn implies mutual solidity. We will give examples in Section 3 to show that the first implication cannot be reversed; for the moment we present an example showing that mutual solidity does not imply semisolidity.

Example 2.1 Let $\underline{A_5} =< A_5, \cdot >$ be the groupoid defined by the table

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	0	3	3
2	2	0	1	3	3
3	3	3	3	3	3
4	4	3	3	3	3

Note that $\cdot$ is commutative, has 0 as an identity element, and has $3 \cdot a = a \cdot 3 = 3$ for all $a \in A_5$. The operation $\cdot$ is not associative, since $(1 \cdot 2) \cdot 4 = 0 \cdot 4 = 4$

but $1 \cdot (2 \cdot 4) = 1 \cdot 3 = 3$, but it is easily verified that it is associative on the subgroupoid $\{0, 3, 4\}$, a fact we shall use later. We shall show that the variety V generated by $\underline{A}_5$ is mutually solid but not semisolid.

Lemma 2.2 *The variety V generated by $\underline{A}_5$ is not semisolid.*

Proof. Consider the variety W generated by the subgroupoid $\underline{Z}_3 = <\{0, 1, 2\}, \cdot>$ of $\underline{A}_5$, so $W \leq V$. $\underline{Z}_3$ has a derived algebra $\underline{D}_3 = <\{0, 1, 2\}, x \odot y = (x \cdot x) \cdot y>$, from which we may in turn derive $\underline{Z}_3$ (using $x \odot (x \odot y)$). That is, W has a mutually derived variety U generated by $\underline{D}_3$. However, $\underline{D}_3$ is not commutative, so U is not contained in W or V. ∎

Lemma 2.3 *The variety V generated by $\underline{A}_5$ is mutually solid.*

Proof. We will show by contradiction that $\underline{A}_5$ has no mutually derived algebras except the trivial one using $x \cdot y$. Suppose there was a non-trivial $\underline{A}_5$-term $x \oplus y$, which in turn produced a term t whose multiplication table was that of the original operation $\cdot$. Note that we need to have $t(4, 0) = t(0, 4) = 4$. It is easily seen that $x \oplus y$ cannot be either x or y alone, so we assume that $x \oplus y$ is represented by a $\cdot$-word in x and y of length at least 2 (and not just $x \cdot y$).

Our next claim is that $x \oplus y$ cannot be essentially unary; that is, the word for $x \oplus y$ cannot involve only x's or only y's. This is because the multiplication table of any such term would contain no 4's, making the desired term t impossible to achieve. (Any occurrence of $x \cdot x$ or $y \cdot y$ eliminates all 4's.) Thus the term $x \oplus y$ must correspond to a $\cdot$-word of length at least 3 (having ruled out $x \cdot y$, $x \cdot x$ and $y \cdot y$), using both x and y.

Now consider the possible values of $4 \oplus 0$ and $0 \oplus 4$. The set $\{0, 4, 3, \}$ forms a subgroupoid of $\underline{A}_5$, on which $\cdot$ is associative and commutative. Hence to evaluate $4 \oplus 0$ and $0 \oplus 4$, we may express the $x \oplus y$ word as $\underbrace{(x \cdot x \cdot \ldots x)}_{a}\underbrace{(y \ldots y)}_{b}$ or $x^a y^b$, for some $a, b \geq 1$, with either a or $b > 1$. That is, either $x \cdot x$ or $y \cdot y$ must occur. This forces one of $4 \oplus 0$ or $0 \oplus 4$ to produce a 3 as an intermediate result in its evaluation. But from the $\cdot$ table property that $3 \cdot d = d \cdot 3 = 3$ for any d, this intermediate 3 immediately forces the end result to be 3. Therefore, either $4 \oplus 0 = 3$ or $0 \oplus 4 = 3$.

We now have an $x \oplus y$ table with the 3-row and the 3-column all 3's, and either $4 \oplus 0 = 3$ or $0 \oplus 4 = 3$. From this, we must produce a new term t having $t(4, 0) = t(0, 4) = 4$. We now see that such a t is impossible: any use of $x \oplus y$, $x \oplus x$ or $y \oplus y$ in the $\oplus$-word for t causes one of $t(4, 0)$ or $t(0, 4)$ to produce an intermediate 3, which immediately propagates to the end result. ∎

Corollary 2.4 *Mutual solidity does not imply semisolidity.*

This example also shows that a mutually solid variety may have subvarieties which are not mutually solid. Band examples in the next section will show that the same is true of semisolid varieties.

Lemma 2.5 *Any intersection of solid or semisolid varieties of the same type is solid or semisolid, respectively.*

Proof. For solid varieties, see [5]. For semisolid, let U_α, $\alpha \in X$, be semisolid varieties all of the same type, and let W be a mutually derived variety of a subvariety Y of $\bigcap_{\alpha\in X} U_\alpha$. Then W is a mutually derived variety of the subvariety $Y \subseteq \bigcap_{\alpha\in X} U_\alpha \subseteq U_\alpha$, so by semisolidity of U_α we have $W \subseteq U_\alpha$, for each $\alpha \in X$. Hence $W \subseteq \bigcap_{\alpha\in X} U_\alpha$ as required. ■

This shows that the solid and semisolid varieties of a given type each form a lattice. It is not known whether the same is true for mutually solid varieties.

Lemma 2.6 *Let V be a variety, and σ a choice of terms for V. The map $d_\sigma : U \to d_\sigma(U)$ is an order-preserving join homomorphism from the lattice of subvarieties of V to the lattice of subvarieties of $d_\sigma(V)$.*

Proof. Let $\{\underline{A}_i : i \in I\}$ and $\{\underline{B}_j : j \in J\}$ be generating sets for varieties U_1 and U_2 respectively. Then their union generates $U_1 \vee U_2$, so $d_\sigma(U_1 \vee U_2)$ is generated by $\{d_\sigma(\underline{A}_i) : i \in I\} \cup \{d_\sigma(\underline{B}_j) : j \in J\}$. But also $d_\sigma(U_1) \vee d_\sigma(U_2)$ is generated by $\{d_\sigma(\underline{A}_i) : i \in I\} \cup \{d_\sigma(\underline{B}_j) : j \in J\}$. This establishes that $d_\sigma(U_1 \vee U_2) = d_\sigma(U_1) \vee d_\sigma(U_2)$, and hence that the map d_σ is order-preserving. ■

We will show by example in the next section that the map d_σ does not preserve meets.

The next lemma will help in describing the derivation diagram of a variety V.

Lemma 2.7 *Let U, V and W be varieties of the same type. If U is a derived variety of W and W is a derived variety of V, then U is a derived variety of V.*

Proof. Let $W = d_\sigma(V)$ for some choice σ of V-terms, and $U = d_\tau(W)$ for some choice τ of W-terms. Then U is generated by $\{d_\tau(\underline{A}) : \underline{A} \in W\}$, and W is generated by $\{d_\sigma(\underline{B}) : \underline{B} \in V\}$ so that U is generated by $\{d_\tau(d_\sigma\underline{B}) : \underline{B} \in V\}$. Since algebras in W use terms of V as their fundamental operations, it is clear that any W term can be expressed as a V-term. Thus the choice τ of W-terms corresponds to a choice $v(\tau)$ of V-terms. This shows that for any $\underline{B} \in V$, $d_\tau(d_\sigma(\underline{B})) = d_{v(\tau)}(\underline{B})$. Hence U is in fact $d_{v(\tau)}(V)$, a derived variety of V. ■

Let U and V be varieties not mutually derived from each other. U will be called a derivative of V of order one if for every variety W, the following implication holds: if U is a derivative of W and W is a derivative of V, then W is mutually derived from either U or V. A series of derived varieties $V_1 \to V_2 \to V_3 \to \ldots$ is a sequence of varieties, each of which is a derivative of order one of the previous one.

Definition 2.8 Given a variety V, the derivation diagram of V is a directed graph whose vertices are the derived varieties of V. Two vertices U and W are joined by an arc $W \to U$, labelled by a choice σ of terms of V, if $d_\sigma(W) = U$, and U is a derivative of W of order 1 or is mutually derived from W. A vertex W also has a loop $W \to W$ labelled by a non-trivial choice σ if $d_\sigma(W) = W$.

For practical reasons it may be necessary to simplify a derivation diagram. This can be done by deleting an arc with a label σ if there is already an arc with this label in the diagram, and no information is lost.

In the next section we present derivation diagrams for some varieties of semigroups.

3 Mutually Solid and Semisolid Varieties of Bands

In this section we look at the concepts of mutual solidity and semisolidity as they apply to varieties of bands. We also give derivation diagrams for some varieties of bands.

Bands are idempotent semigroups; that is, algebras of type $<2>$ satisfying associativity and the idempotent law $x^2 = x$. The lattice of all varieties of bands was completely described by Birjukov [2], Fennemore [7], and Gerhard [8]. The picture of the lattice shown in Diagram 1 below is due to Gerhard and Petrich [9].

There are a countably infinite number of varieties of bands, each equationally defined by associativity, idempotence, and one additional identity. In this section, we will use the notation $V(u = v)$ for the variety of bands determined by the additional identity $u = v$. An important feature of the lattice is its symmetry about a center column of self-dual varieties. Each variety $V = V(u = v)$ not on the center column has a dual, $V^d = V(u^d = v^d) \neq V$ (where u^d is just the right-to-left dual of u); a variety V on the center column has $V = V^d$.

Another key observation about bands is that any variety of bands has at most six binary terms. These terms can be described, using words on the alphabet $\{x, y\}$ and $f(x, y) = xy$ as the fundamental operation, as x, y, xy, yx, xyx and yxy. This makes it easier to work out all the derived varieties of a given variety of bands.

Lemma 3.1 *Let V be a variety of bands, and let σ be the choice of binary term $t(x, y) = yx$. Then $d_\sigma(V) = V^d$, and is a mutually derived variety of V.*

Proof. It is clear that for any algebra $\underline{A}$ in V, $<A; xy>$ and $<A; yx>$ are mutually derived algebras, and $<A; yx>$ is in V^d. ■

As a corollary of this, we get

Theorem 3.2 *If V is a variety of bands which is not self-dual, then V is not mutually solid or semisolid.*

Theorem 3.3 *If V is a self-dual variety of bands, then V is both mutually solid and semisolid.*

Proof. We must show that for any subvariety U of V, all mutually derived varieties of U are contained in V. To do this we must identify which of the six possible derived varieties of U are mutually derived from U. The derived varieties correspond to $d_{\sigma_i}(U)$ for the six possible binary terms σ_i of U: $\sigma_1(x,y) = x$, $\sigma_2(x,y) = y$, $\sigma_3(x,y) = xy$, $\sigma_4(x,y) = yx$, $\sigma_5(x,y) = xyx$ and $\sigma_6(x,y) = yxy$. For $d_{\sigma_i}(U)$ to be mutually derived, we must be able to obtain the U fundamental operation, $\sigma_3(x,y) = xy$, as a term when σ_i is used as the new fundamental operation. We can easily check that σ_1 and σ_2 yield as terms only x and y. The variety $d_{\sigma_3}(U)$ is of course U, and from Lemma 3.1, $d_{\sigma_4}(U) = U^d$; both of these are mutually derived.

Note that for $U \subseteq V = V^d$, we have U, U^d both contained in V. Finally, σ_5 and σ_6 each yield only the terms x, y, xyx and yxy. Thus U has only the two mutually derived varieties, both contained in V. ■

This shows that for varieties of bands, semisolidity and mutual solidity coincide with self-duality. This result also provides us with examples of varieties which are semisolid but not solid: it is known (see [18]) that only four of the countably infinite chain of self-dual band varieties are solid.

We turn now to the question of finding the derivation diagram of a given variety V of bands. For this we must be able to identify the variety $d_{\sigma_i}(V)$ for each of the six possible σ_i listed above. However, this is made more difficult by the fact that if V is an arbitrary variety of bands (or other kind of semigroups), its derived varieties need not be semigroup varieties. This is because not all band or semigroup terms satisfy associativity. For example, the term $t(x,y) = xyx$ does not satisfy $t(t(x,y),z) = t(x,t(y,z))$ in the variety B of all bands, so $d_t(B)$ is not a semigroup variety.

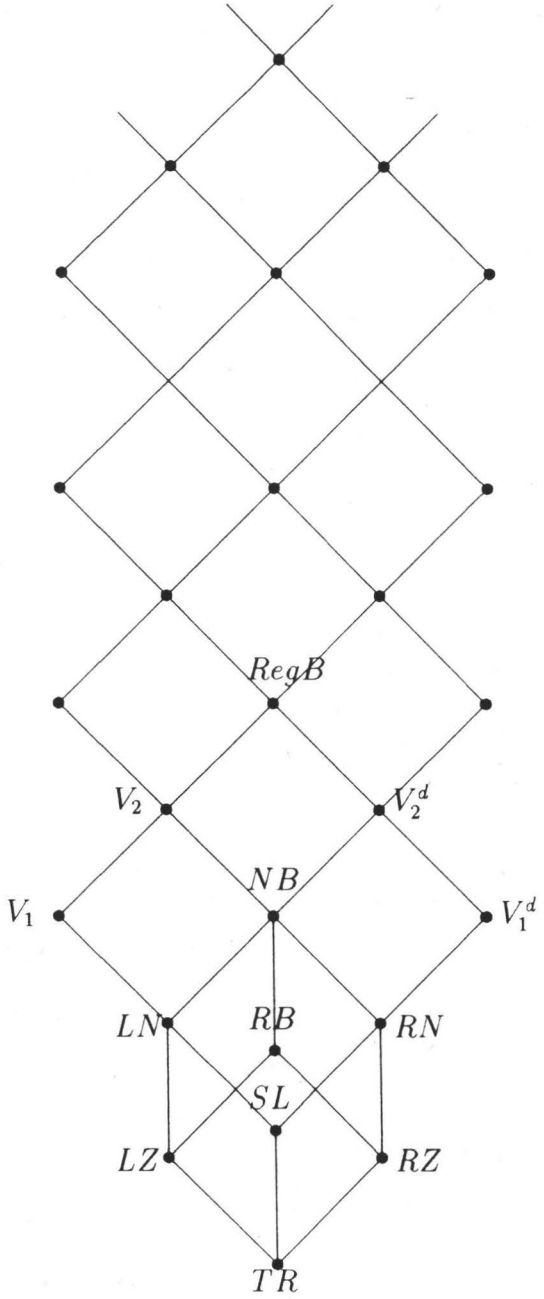
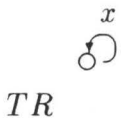


Figure 1: Diagram 1: The lattice of proper varieties of bands

A variety of type <2> in which every binary term satisfies the associative law is called a hyperassociative variety. (Such a variety then satisfies the associative law as a hyperidentity.) Hyperassociative varieties of semigroups have been studied in [3], [5], [14] and [18]. From [18] we know that there are exactly thirteen varieties of bands which are hyperassociative. These are the thirteen subvarieties of the variety $RegB$ of regular bands. These thirteen varieties have been labelled in Diagram 1 above, using the following notation.

$$\begin{aligned}
TR &= V(x = y), \text{the variety of trivial bands;} \\
LZ &= V(xy = x), \text{the variety of left zero bands, with its dual,} RZ; \\
SL &= V(xy = yx), \text{the variety of commutative bands;} \\
RB &= V(xyx = x), \text{the variety of rectangular bands;} \\
LN &= V(xyz = xzy), \text{the variety of left normal bands, with dual } RN; \\
NB &= V(xyzw = xzyw), \text{the variety of normal bands;} \\
V_1 &= V(xy = xyx), \text{with dual } V_1^d; \\
V_2 &= V(xyz = xyxz), \text{with dual } V_2^d; \\
RegB &= V(xyzx = xyxzx), \text{the variety of regular bands.}
\end{aligned}$$

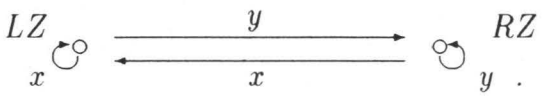
The variety TR of trivial bands has only one binary term, $x(= y)$, and its derivation diagram is just



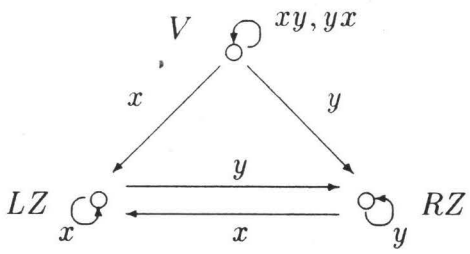
TR

The varieties LZ and RZ play a special role in derivation diagrams. They each have only two binary terms, x and y, since $xy = x$ in LZ and $xy = y$ in RZ. For $\underline{A} \in LZ$, we have $\sigma_y(\underline{A}) \in RZ$, and dually. And for any algebra $\underline{A} = <A, xy>$ of type <2>, $\sigma_x(\underline{A})$ is in LZ and $\sigma_y(\underline{A})$ is in RZ. Thus LZ and RZ will be derived varieties of every type <2> variety.

Theorem 3.4 *The dual varieties LZ and RZ of left and right zero bands have derivation diagram*

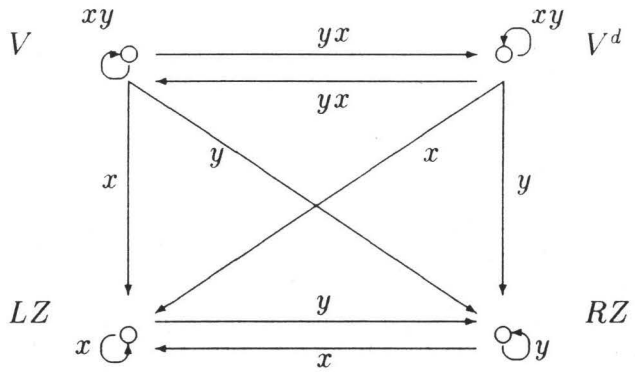


Theorem 3.5 *Let V be either of the varieties SL or RB. Then V has the following derivation diagram (where $xy = yx$ when $V = SL$):*



Proof. The variety SL has only the three binary terms x, y, and xy, and its diagram is clear. The variety RB has the one additional term yx. We have seen that $d_x(RB) = LZ$, $d_y(RB) = RZ$, and from Lemma 3.1, $d_{yx}(RB) = RB^d = RB$. ■

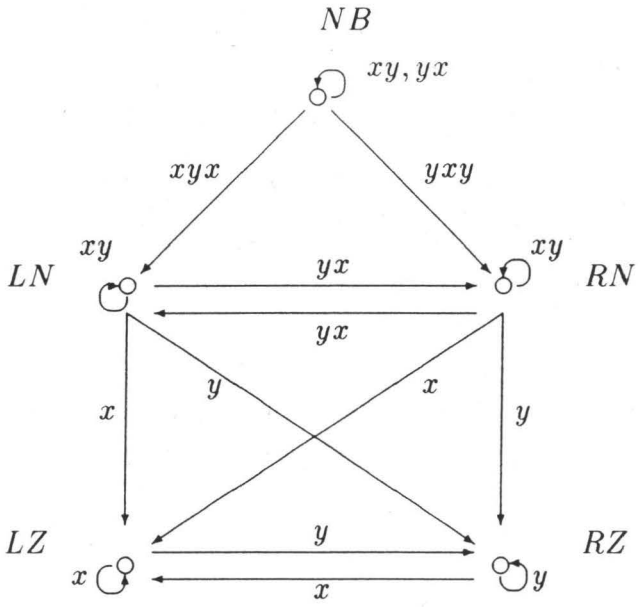
Theorem 3.6 *Let V be either of the varieties LN or V_1. Then V and its dual have the derivation diagram*



Proof. As always $d_x(V) = LZ$, $d_y(V) = RZ$, and $d_{xy}(V) = V$. From Lemma 3.1, $d_{yx}(V) = V^d$. ■

The remaining subvarieties of $RegB$ (NB, V_2, V_2^d, and $RegB$) all have all six possible binary terms. The diagram obtained for each depends on whether the variety is self-dual or not.

Theorem 3.7 *The variety NB of normal bands has the derivation diagram*



and the variety RegB of regular bands has a similar derivation diagram, with LN and RN replaced by V_1 and V_2 respectively.

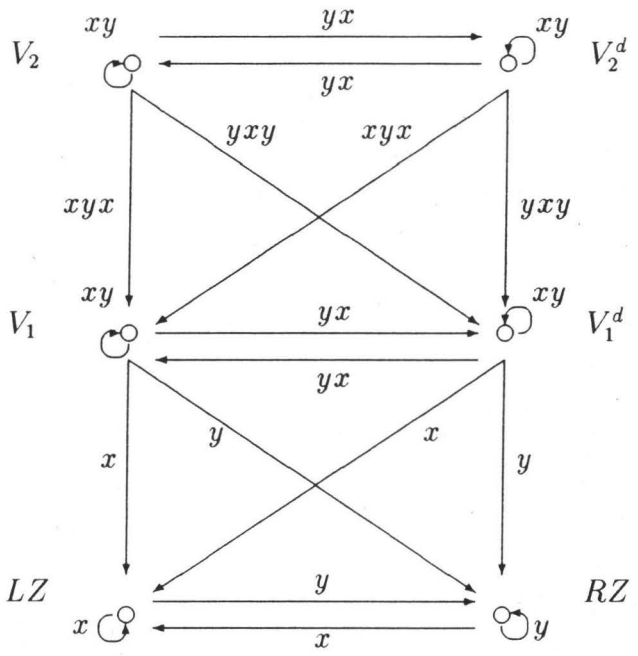
Proof. The only new claim here for NB is $d_{xyx}(NB) = LN$ and dually $d_{yxy}(NB) = RN$. Since the term xyx satisfies both associativity and idempotence, $d_{xyx}(NB)$ is a variety of bands. We will show that xyx satisfies the identity for LN but not those for LZ or SL, to conclude that $d_{xyx}(NB) = LN$.

So consider the substitution of $t(x, y) = xyx$ in the LN identity $xyz = xzy$. The left hand side yields $t(t(x, y), z) = xyxzxyx$, while the right hand side yield $(t(t(x, z), y) = xzxyxzx$; in the variety NB, these are both equal to $xyzx$. However, substituting t in the LZ and SL identities $xy = x$ and $xy = yx$ yields the identities $xyx = y$ and $xyx = yxy$, neither of which holds in NB.

For $RegB$, we need only verify that $d_{xyx}(RegB) = V_1$ and dually, $d_{yxy}(RegB = V_1^d)$.

Substitution of xyx for t in the V_1 identity $t(x, y) = t(t(x, y), x)$ yields the identity $xyx = xyxxyx$, which holds in any band variety. However, the LN identity $t(t(x, y), z) = t(t(x, z)y)$ yields $xyxzxyx = xzxyxzx$, which does not hold as an identity in $RegB$. ∎

Theorem 3.8 *The variety V_2 and its dual have the derivation diagram*



Proof. Combined with the previous results, it will suffice to prove that $d_{xyx}(V_2) = V_1$, and dually. As we have seen in Theorem 3.9, using xyx for t in the V_1 identity $t(x,y) = t(t(x,y),x)$ yields an identity which holds in any band variety. Hence $d_{xyx}(V_2) \subseteq V_1$. But substitution in the LN identity gives $xyxzxyx = xzxyxzx$; in V_2 this reduces to $xyzyx = xzyzx$, which does not hold in V_2. Thus $d_{xyx}(V_2) \not\subseteq LN$, giving $d_{xyx}(V_2) = V_1$. The dual results are obtained similarly. ■

In Lemma 2.6 in the previous section we showed that the map d_σ preserves joins of varieties. Our band examples now show that d_σ does not preserve meets. Consider the choice $\sigma = xyx$. We have seen that $d_\sigma(V_2 \cap V_2^d) = d_\sigma(NB) = LN$, while $d_\sigma(V_2) \cap d_\sigma(V_2^d) = V_1 \cap V_1 = V_1$.

4 Derived Algebras of p-groups

As was noted earlier, not every binary term t of a semigroup $<A; xy>$ satisfies the associative law. Thus the derived algebra $<A; t>$ may be a groupoid which is not a semigroup. In this section we will explore what kinds of groupoids can be obtained as derived or mutually derived algebras, starting from a cyclic p-group.

Theorem 4.1 *Let t be a binary term of some semigroup $\underline{A} = <A; xy>$, for which $\underline{B} = <A; t>$ is mutually derived from A. If $\underline{B}$ is neither equal to $\underline{A}$ nor anti-isomorphic to $\underline{A}$, then $\underline{A}$ satisfies the identity*

$$x^{2+\ell} = x^2$$

for some $\ell \geq 1$.

Proof. Using the $\underline{A}$-term t for the fundamental operation of $\underline{B}$ means that every term function of $\underline{B}$ can be represented as a term function of $\underline{A}$. In particular, since $\underline{A}$ can also be derived from $\underline{B}$, xy can be obtained in this way. That is, we have an identity of the form

$$x^{k_1}y^{\ell_1}\cdots x^{k_n}y^{\ell_n} = xy,$$

for some $n \geq 1$, $k_i,\ \ell_i \geq 0$.

If $\underline{B}$ is just $\underline{A}$, or $\underline{B}$ is anti-isomorphic to $\underline{A}$ (i.e., if t is xy or yx), this identity is trivial. Otherwise we have $k_1 + \ell_1 + \ldots + k_n + \ell_n > 2$, and we may write $k_1 + \ell_1 + \ldots + k_n + \ell_n = 2 + \ell$, for some $\ell \geq 1$. The substitution $y = x$ then gives

$$x^{2+\ell} = x^2$$

as an identity holding in $\underline{A}$. ∎

As a corollary of this proof, we obtain:

Corollary 4.2 *If the group* $\underline{A}$ *has a non-trivial, non-anti-isomorphic mutually derived algebra, then* $\underline{A}$ *is of finite exponent.*

The next results deal with mutually derived groupoids of cyclic abelian groups. For convenience we adopt an additive notation for the group's fundamental operation. We also use the notation (a, b) for the greatest common divisor of two numbers a and b.

Theorem 4.3 *Let* $\underline{G} =< G; + >$ *be a cyclic group of order* p^n, *where* p *is a prime number and* $n \geq 1$. *Let* $\underline{H} =< G; \oplus >$ *be a derived groupoid of* $\underline{G}$. *If* $x \oplus y = kx + \ell y$ *for some natural numbers* k, ℓ *such that* $(k, p^n) = 1$, $(\ell, p^n) = 1$ *and either* $k + \ell$ *is a primitive root of* p^n *or* p *divides* $k + \ell$, *then* $\underline{H}$ *is mutually derived from* $\underline{G}$.

Proof. Let $x \oplus y = kx + \ell y$, with $(k, p^n) = 1$ and $(\ell, p^n) = 1$.

Case 1: Suppose $k + \ell$ is a primitive root of p^n. Then $k + \ell, (k + \ell)^2, \ldots, (k + \ell)^{\varphi(p^n)}$ represents the cyclic group of units modulo p^n. Since k is also a unit with $k^{\varphi(p^n)-1}$ as inverse, we have $k^{\varphi(p^n)-1} = (k+\ell)^s$ for some number s, $1 \leq s \leq \varphi(p^n)$. Then $x \oplus x = (k + \ell)x$, $(x \oplus x) \oplus (x \oplus x) = (k + \ell)^2 x$, and so on, and hence $k^{\varphi(p^n)-1}x = (k + \ell)^s x$ is a term $\sigma(x)$ of $\underline{H}$, with $k\sigma(x) = x$. Similarly, there is a term $\tau(x)$ of $\underline{H}$ with $\ell\tau(x) = x$. These combine to produce the $\underline{H}$-term $\sigma(x) \oplus \tau(y) = k\sigma(x) + \ell\tau(y) = x + y$. Thus $< G, + >$ is derived from $< H, \oplus >$, making these mutually derived algebras.

Case 2: Suppose p divides $k + \ell$. Then $(k + \ell)^n \equiv 0 \bmod p^n$, and there is a term $t(x)$ of $\underline{H}$ such that $t(x) = (k + \ell)^n x = 0$. Then $x \oplus t(x)$ is a term of $\underline{H}$, and $kx = x \oplus t(x)$. From this we can form a term $\sigma(x) = k^{\varphi(p^n)-1}x$. Similarly, we can construct a term $\tau(x)$ and as in Case 1, show that $x + y$ is obtained as a term of $\underline{H}$. ∎

Theorem 4.4 *Let* $\underline{G} =< G; + >$ *be a cyclic group of order* p^n, *where* p *is a prime number and* $n \geq 1$. *If* $\underline{H} =< G; \oplus >$ *is mutually derived from* $\underline{G}$, *then* $x \oplus y = kx + \ell y$ *for some natural numbers* k, ℓ *for which* $(k, p^n) = 1$, $(\ell, p^n) = 1$ *and either* $k + \ell$ *is a primitive root of* p^n *or* p *divides* $k + \ell$.

Proof. Let $\underline{H} =< G; \oplus >$ be mutually derived from $\underline{G}$. Suppose that (k, p^n) is not 1, so that p divides k. Let $t(x, y)$ be any term of $< G; \oplus >$. Then $t(x, 0) = mx$, for some number $m \geq 0$. We show by induction that p must divide m. For the basic operation $s(x, 0) = x \oplus 0 = kx$, we have p divides k. Assuming the claim to be true for terms $t_1(x, 0) = m_1 x$ and $t_2(x, 0) = m_2 x$, we have $t(x, 0) = t_1(x, 0) \oplus t_2(x, 0) = km_1 x + \ell m_2 x = (km_1 + \ell m_2)x$, with p dividing $km_1 + \ell m_2$.

Now since $\underline{G}$ and $\underline{H}$ are mutually derived, the term $x + y$ is one of the terms $t(x, y)$. Therefore $x = x + 0 = t(x, 0) = mx$, with p dividing m. This is a contradiction.

Now suppose that neither $k + \ell$ is a primitive root of p^n nor p divides $k + \ell$. Then $(k + \ell)^m$ is congruent to 1 mod p^n for some m with $m < \varphi(p^n)$. We then have that $x = (k + \ell)^m x$ and $((k + \ell)^m - 1)x = 0$, which contradicts that fact that $\underline{G}$ is of order p^n. ∎

We next use the information from Theorem 4.4 to examine what kinds of groupoids are obtained as mutually derived algebras for p-groups. Recall that a quasigroup is a groupoid $(G; xy)$ in which for any two elements a, b of G, the equations $ax = b$ and $ya = b$ each have exactly one solution. More information about quasigroups may be found in [6]. We shall need the following definitions, also from [6].

Let $< G; \bullet >$ and $< H; * >$ be two quasigroups. An ordered triple $(\mathcal{O}, \varphi, \sigma)$ of bijections $\mathcal{O}$, φ, and σ of G onto H is called an isotopism of $< G; \bullet >$ onto $< H; * >$ if $\mathcal{O}(x \cdot y) = \varphi(x) * \sigma(y)$ for all x, y in G. $< H; * >$ is then called an isotope of $< G; \bullet >$.

Now let $< G; \bullet >$ be a quasigroup, and let φ, σ be bijections of G onto G. The isotope $< G; \otimes >$ defined by $x \otimes y = \varphi(x) \cdot \sigma(y)$ is called a principal isotope of $< G; \bullet >$.

We note that a derived algebra of a cyclic group $< G_p; + >$ of prime order need not be a quasigroup. For example, $< G_5; + >$ has a derived algebra $< G_5; x \oplus y = 3x >$ in which $3 \oplus x = 2$ has no solution. However, we do have the following result.

Theorem 4.5 *Every mutually derived algebra of a cyclic group* $< G; + >$ *of order* p^n, *where* p *is a prime and* $n \geq 1$, *is a medial and non-idempotent quasigroup.*

Proof. Let $< G; \oplus >$ be a mutually derived algebra of the cyclic group $< G; + >$ of order p^n. From Theorem 4.4, $x \oplus y = kx + \ell y$ for some $k, \ell \geq 1$ and $(\ell, p^n) = 1$ and $k + \ell$ is not congruent to 1 mod p. We define maps φ, σ on G by $\varphi(x)$

$= kx$ and $\sigma(x) = \ell x$. Both maps are bijections in this case, and $<G; \oplus>$ is the associated principal isotope of the quasigroup $<G; +>$. But from [6, p.24], every principle isotope of a quasigroup is a quasigroup.

For mediality, we have

$$\begin{aligned}(x \oplus y) \oplus (z \oplus w) &= k(kx + \ell y) + \ell(kz + \ell w) \\ &= k^2 + k\ell y + \ell kz + \ell^2 w \\ &= k(kx + \ell x) + \ell(ky + \ell w) \\ &= (x \oplus z) \oplus (y \oplus w).\end{aligned}$$

For idempotence, suppose that $x \oplus x = x$, and hence $(k + \ell)x = x$. If $k + \ell$ is a primitive root of p^n, then $k + \ell$ is not congruent to 1 mod p^n and hence $(k + \ell)x$ is not equal to x. If p divides $k + \ell$ then $x = 0$. Both cases thus yield contradictions. ■

Theorem 4.6 *Every groupoid which is mutually derived from an abelian group is a medial and non-idempotent quasigroup.*

Proof. Let $\underline{A}$ be an abelian group, and B be mutually derived from $\underline{A}$ with $x \oplus y = \lambda x + \mu y$. If $\underline{B}$ is not isomorphic to $\underline{A}$ itself, then by Corollary 4.2 $\underline{A}$ must be of finite exponent. This means that $\underline{A}$ is a direct product of cyclic groups $\underline{A_i}$ of prime power orders (see for instance [15,5.1.12]. Then for each $\underline{A_i}$ of order $p_i^{n_i}$, we define $x \oplus_i y = k_i x + l_i y$, where $k_i = \lambda$ mod $p_i^{n_i}$ and $\ell_i = \mu$ mod $p_i^{n_i}$. This produces subgroupoids $\underline{B_i} = <A_i; \oplus_i>$ of order $p_i^{n_i}$, which by Theorem 4.5 are medial, non-idempotent quasigroupoids. $\underline{B}$ is then the direct product of these $\underline{B_i}$, completing the proof. ■

5 Examples of 3-element Groupoid Derivations

In this section we present two examples in which we determine all the derived algebras of a given 3-element groupoid. For each, we give a derivation diagram, analogous to the derivation diagrams for varieties described above. A key tool is the recent enumeration and classification by Berman and Burris ([1]) of all possible 3-element groupoids. Thus we can identify each of the derived groupoids obtained by its Berman-Burris number. The cyclic group $<G_3; +>$ of order 3, for example, is #2124.

Example 5.1 $<G_3; +>$, the cyclic group of order 3.

This group has nine binary terms, x, y, $2x$, $2y$, $x + y$, $2x + y$, $x + 2y$, $2x + 2y$, and $3x$, with corresponding nine derived groupoids on $G_3 = \{0, 1, 2\}$. From Theorems 4.3 and 4.4, we know that only $<G_3; x + 2y>$ and $<G_3; 2x + y>$ are mutually derived from $<G_3; +>$. We obtain the following derivation diagram.

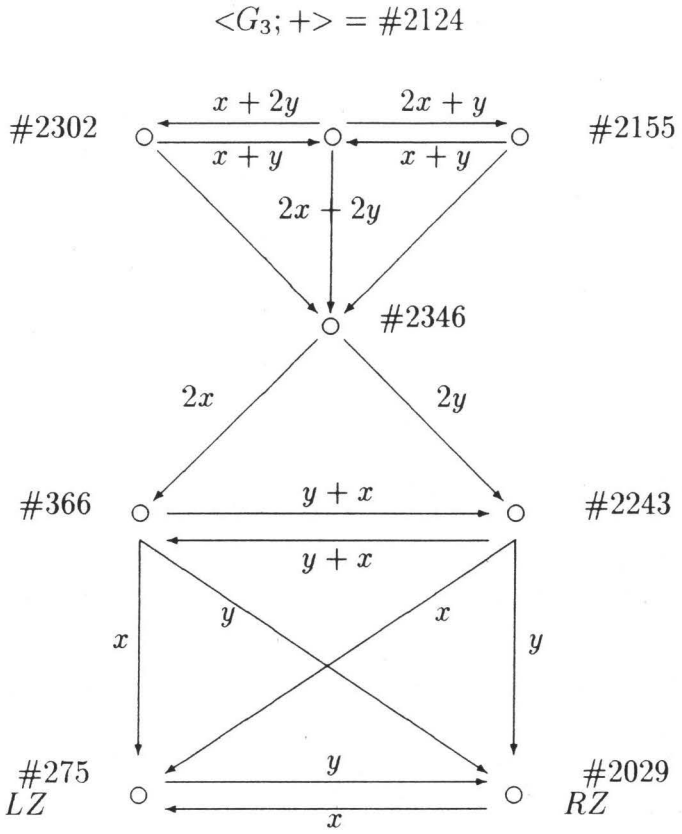


DIAGRAM 2: Derived groupoids of $<G_3; +>$.

Example 5.2 Murski's groupoid.

Murski's groupoid is the 3-element groupoid $<\{0,1,2\}; \bullet>$ with operation table given by

$\bullet$	0	1	2
0	0	0	0
1	0	0	1
2	0	2	2

, and it appears as #35 in the Berman-Burris enumeration. It is non-associative, since $(1 \bullet 2) \bullet 1 = 0$ while $1 \bullet (2 \bullet 1) = 1$. It is the smallest groupoid which is not finitely based (see [11], p.386.) It has 11 terms, which we list here with their corresponding derived groupoid number.

xy, #35	yx, #58
$(xx)y$, #9	$(yy)x$, #55
$x(yy)$, #29	$y(xx)$, #6
$(xx)(yy)$, #3	
x^2, #27	y^2, #1045
x, #275	y, #2079

We can then work out the terms of each of these derived groupoids (still based on the original fundamental operation), and whether any of them are derived from any others. For example, #9 and #55 have terms x, y, x^2y, y^2x, x^2, y^2 and x^2y^2, while #29 and #6 have x, y, xy^2, yx^2, x^2, y^2, and x^2y^2. Hence #29 cannot be derived from #9, and vice versa. Of course, each pair of groupoids listed on the

same line above are mutually derivable.

Compiling this information, we obtain the following diagram for the derived groupoids of Murski's groupoid.

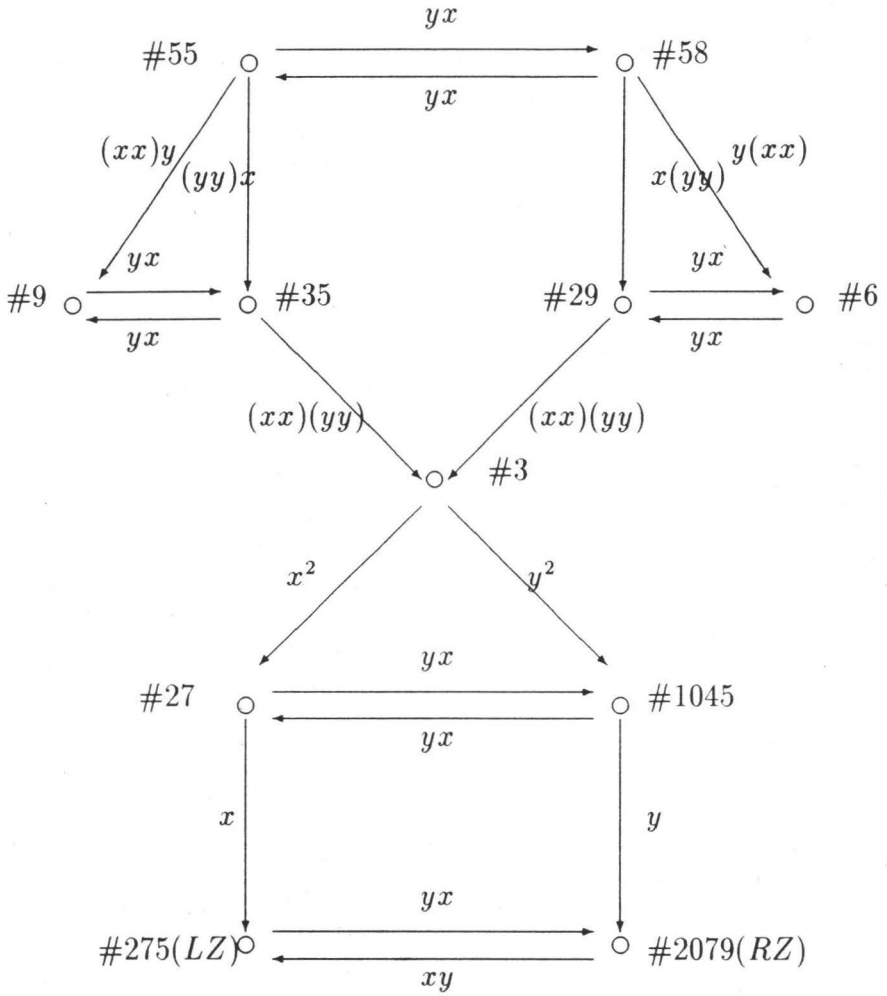


DIAGRAM 3: Derived groupoids of Murski's groupoid.

Collapsing mutually derived varieties lead to the following picture:

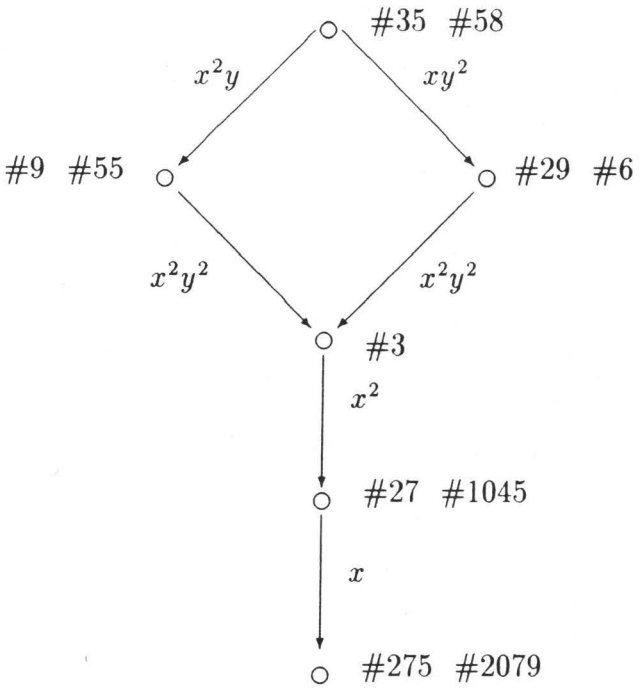


DIAGRAM 4: Derivation diagram modulo mutual derivation.

Note that Diagram 3 illustrates a series of derived algebras, #35 → #9 → #3 → #27 → #275.

We note here that there are other variations one might consider on these ideas. For example, Denecke and Koppitz in [4] have introduced the idea of pre-solid varieties, that is varieties for which all derived varieties obtained by using non-projection terms are still contained in the variety. Obviously one can generalize our concepts to cover those cases related to pre-solidity.

6 Derived Algebras and McKenzie's Theory of Types

In [12] an algebra $\underline{A}$ is called abelian if for every natural number n and every n-ary term function t of $\underline{A}$, and for all $u, v, x_1, \ldots, x_{n-1}, y_1, \ldots y_{n-1}$, the following equivalence holds:

$$t(u, x_1, \ldots, x_{n-1}) = t(u, y_1, \ldots, y_{n-1})$$
$$\text{iff } t(v, x_1, \ldots, x_{n-1}) = t(v, y_1, \ldots, y_{n-1}).$$

Lemma 6.1 *A derived algebra $d(\underline{A})$ of an abelian algebra $\underline{A}$ is abelian.*

Proof. This follows immediately from the definition and the fact that a term function of $d(\underline{A})$ is also a term function of $\underline{A}$. ∎

We note that the equivalence defining abelian algebras can also be considered as an implication of hyperidentities.

Definition 6.2 Let $\underline{A}$ be an algebra and α and β congruence relations of $\underline{A}$ with $\alpha \leq \beta$. β is abelian over α if for every natural number n , every n-ary term function t of $\underline{A}$, and for all (u, v) in α and $(x_1, y_1), \ldots (x_n, y_n)$ in β, the following equivalence holds:

$$t(u, x_1, \ldots, x_{n-1}) \overset{\alpha}{=} t(u, y_1, \ldots, y_{n-1})$$
$$\text{iff } t(v, x_1, \ldots, x_{n-1}) \overset{\alpha}{=} t(v, y_1, \ldots, y_{n-1}).$$

Definition 6.3 Let $\underline{A}$ be an algebra, let $1_{\underline{A}}$ be the total relation and $0_{\underline{A}}$ the identity relation on $\underline{A}$. $\underline{A}$ is solvable if there exists a finite chain of congruences $\alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_n$ such that $\alpha_0 = 0_{\underline{A}}$, $\alpha_n = 1_{\underline{A}}$, and α_{i+1} is abelian over α_i for $i < n$.

Lemma 6.4 *A derived algebra $d(\underline{A})$ of a solvable algebra $\underline{A}$ is solvable.*

Proof. Every congruence relation of $\underline{A}$ is also a congruence relation on $d(\underline{A})$. Hence there exists a finite chain of congruences $\alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_n$ as in the algebra $\underline{A}$. If α_{i+1} is abelian over α_i in $\underline{A}$ then α_{i+1} is abelian over α_i in $d(\underline{A})$, because every term function of $d(\underline{A})$ is also a term function of $\underline{A}$. ■

As an example, let $<Q; o>$ be a quasigroup which is derived from a solvable group $<Q; \cdot>$. Then $<Q; \cdot>$ is solvable. For example, the groupoid $<C_3; o>$ where $xoy = 2x + 2y$ is an abelian algebra; see Section 3.

In the proofs of the previous two Lemmas, one could also use an argument based on snags, as in [12, p.113]: if $\underline{A}$ contains no $1-$snag (2-snag) then neither does $d(\underline{A})$.

Derived algebras behave well with respect to types of algebras. This can be observed for the theory of types developed in [16], as well as for the theory of types of Hobby and McKenzie in [12]. In the first case it is easy to see that a subclone $P(d(\underline{A}))$ of polynomial functions preserves all the relations which characterizes the clone $P(\underline{A})$ of polynomial functions of $\underline{A}$. If a finite algebra is of one of the types O, L, C, Z, or R, then a derived algebra is of the same type.

In the second case it can be observed that an algebra derived from one of type α will be of type β if in the lattice of types ([12, p.72]) $\beta \leq \alpha$. Therefore the operator d induces an order homomorphism on the lattice of types.

References

[1] Berman, J. and S. Burris, *A computer study of 3-element groupoids*, preprint 1994 (ftp thoralf.waterloo.ca).

[2] Birjukov, P.A., *Varieties of idempotent semigroups,* Algebra i Logika **9**(1970), 255–273 (Russian).

[3] Denecke, K. and J. Koppitz, *Hyperassociative varieties of semigroups,* Semigroup Forum **49**(1994), 41–48.

[4] Denecke, K. and J. Koppitz, *Pre-Solid Varieties of Semigroups*, preprint, Nov. 93.

[5] Denecke, K. and S.L. Wismath, *Solid varieties of semigroups,* Semigroup Forum **48**(1994), 219–234.

[6] Denés, J. and A.D. Keedwell, *Latin Squares and their Applications*, Academic Press, 1974.

[7] Fennemore, C., *All varieties of bands I, II,* Math. Nachr. **48**(1971), 237–252, 253–262.

[8] Gerhard, J.A., *The lattice of equational classes of idempotent semigroups*, J. Algebra **15**(1970), 195–224.

[9] Gerhard, J.A. and M. Petrich, *Varieties of bands revisited,* Proc. London Math. Soc. **(3)58**(1989), 323–350.

[10] Graczynska, E. and D. Schweigert, *Hyperidentities of a given type,* Algebra Universalis **27**(1990), 305–318.

[11] Gratzer, G., Universal Algebra, Second Edition, Springer-Verlag, New York, 1979.

[12] Hobby, D. and R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics, AMS, Providence, 1988.

[13] LeVeque, W., Fundamentals of Number Theory, Addision-Wesley, 1977.

[14] Polak, L., *On hyperassociativity,* preprint 1994.

[15] Scott, W.R., Group Theory, Prentice Hall, 1964.

[16] Schweigert, D., *On prepolynomially complete algebras*, J. London Math. Soc. (2), **20**(1979), 179-185.

[17] Schweigert, D., *Hyperidentities,* in I.G. Rosenberg and G. Sabidussi, eds., "Algebras and Orders," Kluwer Academic Publishers 1993, 401–502.

[18] Wismath, S.L., *Hyperidentity bases for rectangular bands and other semigroup varieties,* J. Australian Math. Soc. (Series A) **55**(1993), 270–286.

Fachbereich Mathematik,
Universitat Kaiserslautern,
Postfach 3049,
67663 Kaiserslautern,
Germany.

Dept. of Mathematics and
Computer Science,
University of Lethbridge,
Lethbridge, Alberta,
Canada T1K-3M4.