Pacific Journal of Mathematics

SYMMETRIC DIFFERENCE IN ABELIAN GROUPS

GEORGE GRÄTZER AND R. PADMANABHAN

Vol. 74, No. 2

June 1978

SYMMETRIC DIFFERENCE IN ABELIAN GROUPS

G. GRÄTZER AND R. PADMANABHAN

A groupoid $\mathfrak{A} = \langle A; * \rangle$ is called a left (resp. right) difference group if there is a binary operation + in A such that the system $\langle A; + \rangle$ is an abelian group and x * y = -x + y(resp. x * y = x - y). A symmetric difference group is a groupoid satisfying all the identities common to both left and right difference groups. In this note we determine the structure of a symmetric difference group. Using this, we show that any finitely based equational theory of symmetric difference groups is one-based. This includes the known result that the theories of left and right difference groups are onebased. Other known results on finitely based theories of rings also follow.

Let I (resp. J) stand for the class of all binary identities true in all left (resp. right) difference groups. Then the equational class of groupoids satisfying all the identities $I \cap J$ is, by definition, the class of all symmetric difference groups (SD-groups, for brevity). For example, the identity

$$(1) \qquad (x * y) * (((x * z) * (u * u)) * y) = z$$

belongs to the class $I \cap J$ and hence valid in every SD-group. To see this we only have to check whether (1) is true when x * y =-x + y or x * y = x - y in abelian groups. This is indeed the case. The main result of this paper is that the converse of the above statement is true, namely, any groupoid satisfying identity (1) is, in fact, an SD-group (Theorem 2). This is obtained through a structure theorem for groupoids satisfying identity (1).

1. The structure theorem. We prepare the proof of the structure theorem with a lemma.

LEMMA 1. Let $\mathfrak{A} = \langle A; F \rangle$ be an algebra having a binary polynomial * and let w be a polynomial of the type of \mathfrak{A} . Then the algebra satisfies the identity

$$(2) \qquad (x * y) * (((x * z) * w) * y) = z$$

iff A has an abelian group reduct $\langle A; +, -, 0 \rangle$ and there exists a map $\alpha: A \rightarrow A$ such that

(i) A satisfies the identity w = 0;

(ii) α is an involutoric¹ endomorphism of the group; and

¹ We call a map $\alpha: A \to A$ involutoric if α^2 is the identity map on A.

(iii) $x * y = x\alpha - y\alpha$.

Proof. If there exists a map $\alpha: A \to A$ satisfying (i)-(iii) then

$$(x * y) * (((x * z) * w) * y)$$

= $(x\alpha - y\alpha)\alpha - ((x\alpha - z\alpha)\alpha^2 - y\alpha)\alpha$
= $(x - y) - (x - z - y)$
= $x - y - x + z + y = z$

and hence (2) is valid in \mathfrak{A} .

Conversely, let \mathfrak{A} satisfy the identity (2). Let us make x * z into a variable a by substituting x = a * w and z = ((a * a) * w) * w to obtain

$$((a * w) * y) * ((a * w) * y) = ((a * a) * w) * w$$

Notice that we can change the term (a * w) * y into an arbitrary variable z by substituting y = ((a * z) * w) * w. So we have

and hence z * z is a constant, say 0.

Observe that we have the left cancellation property for *. Indeed, x * z = x * t implies that

$$z = (x * y) * (((x * z) * w) * y)$$
 by (2)

$$= (x * y) * (((x * t) * w) * y)$$
 by (2)
= t.

So, from (3) we get

(0 * w) * (0 * w) = (0 * w) * w,

which implies that 0 * w = w. Putting x = z = 0 and y = w in (2) and using the above we get

$$w * 0 = 0 = w * w$$

and hence

(4) w = 0.

Let x = z and y = 0 in (2). We have

(5) (x * 0) * 0 = x.

Putting y = 0 in (2) we get, by (5),

(6) (x * 0) * (x * z) = z.

Now multiply (2) on the left by (x * y) * 0 to obtain

$$((x * y) * 0) * \{(x * y) * (((x * z) * 0) * y)\} = ((x * y) * 0) * z,$$

which reduces, by (6), to

$$(7) \qquad ((x*z)*0)*y = ((x*y)*0)*z.$$

Finally, putting x = y = z in (2) we get

$$(8) 0*(0*x) = x.$$

We have obtained enough identities now to recover the group structure. Define

$$x + y = (x * 0) * (0 * y)$$

and

-x = (0 * x) * 0.

We claim that the reduct $\langle A; +, -, 0 \rangle$ is an abelian group. Compute:

$$0 + x = (0 * 0) * (0 * x)$$

= 0 * (0 * x)
= x; by (8)

$$-x + x = (((0 * x) * 0) * 0) * (0 * x)$$

= (0 * x) * (0 * x) by (5)
= 0;

$$(x + y) + z = (((x * 0) * (0 * y)) * 0) * (0 * z)$$

= (((x * 0) * (0 * z)) * 0) * (0 * y) by (7)
= (x + z) + y.

In particular, putting x = 0, we get y + z = z + y. This completes the proof that the reduct $\langle A; +, -, 0 \rangle$ is an abelian group and the algebra \mathfrak{A} satisfies the identity w = 0.

Let us substitute, in (2), x = a * 0 and z = a * c. By (6) we have x * z = c. Hence (2) becomes

$$((a * 0) * y) * ((c * 0) * y) = a * c$$
.

Putting y = c * 0 and multiplying both sides by 0, on the right we obtain using (5)

$$(9) \qquad (a*0)*(c*0) = (a*c)*0.$$

Now define $\alpha: A \rightarrow A$ by $x\alpha = x * 0$.

We have

$$(x + y)\alpha = (x + y) * 0$$

= $((x * 0) * (0 * y)) * 0$
= $((x * 0) * 0) * ((0 * y) * 0)$ by (9)
= $x * ((0 * y) * 0)$
= $x * (0 * (y * 0))$ by (9)
= $x\alpha + y\alpha$.

Moreover,

$$x\alpha^2 = (x * 0) * 0$$
$$= x ,$$

and thus α is an involutoric endomorphism of the abelian group $\langle A; +, -, 0 \rangle$. Finally

$$\begin{aligned} x\alpha - y\alpha &= (x * 0) + (0 * (y\alpha * 0)) \\ &= (x * 0) + (0 * y) \\ &= ((x * 0) * 0) * (0 * (0 * y)) \\ &= x * y \end{aligned}$$

and this completes the proof of the lemma.

Now we are ready to state and prove the structure theorem.

THEOREM 1. Let $\mathfrak{A} = \langle A; * \rangle$ be an SD-group. Then there is a binary operation + on A such that $\langle A; + \rangle$ is an abelian group and $x * y = x\alpha - y\alpha$ for some involutoric endomorphism α of the abelian group $\langle A; + \rangle$.

Proof. If $\mathfrak{A} = \langle A; * \rangle$ is an SD-group then it satisfies identity (1) which is a special case of (2) with w = u * u. Hence, by Lemma 1, \mathfrak{A} has an abelian group reduct with the desired properties. The additional condition u * u = 0 is, of course, true in all SD-groups as it belongs to $I \cap J$. This completes the proof of the theorem.

2. One-based theories. Let L (resp. R) denote the equational class of all left difference groups (resp. right difference groups). So the lattice join $L \vee R$ in the lattice of all equational classes of groupoids is precisely the class of all groupoids satisfying the identities $I \cap J$ and hence $L \vee R$ is the class of all SD-groups. Let S denote the equational class of groupoids satisfying identity (1). Then it is clear that $S \supseteq L \vee R$. Thus to prove that identity (1) is indeed a base for the equational theory of $I \cap J$, it is sufficient to prove

that $S \subseteq L \lor R$. For these and other universal algebraic notions we refer to the relevant sections of [1].

Let X and X' be disjoint sets with $\alpha: X \leftrightarrow X'$ a bijection between them.

Let $Ab(X \cup X') = \langle F; +, -, 0 \rangle$ be the free abelian group generated by the set $X \cup X'$. Now α is a mapping of the set $X \cup X'$ into F and by the freeness of $Ab(X \cup X')$ we can extend this to an endomorphism α . Moreover, since $x\alpha^2 = x$ for all $x \in X \cup X'$, we have $x\alpha^2 = x$ for all $x \in F$. For x, y in F, define $x * y = x\alpha - y\alpha$. It is clear that the groupoid $\mathfrak{A} = \langle F; * \rangle$ satisfies identity (1) of Theorem 1 and hence $\mathfrak{A} \in S$.

LEMMA 2. The groupoid $\mathfrak{A} = \langle F; * \rangle$ constructed above is the free S-groupoid generated by the set X.

Proof. Let $\mathfrak{B} = \langle B; * \rangle$ be any S-groupoid and let φ be a mapping from X into B. By Theorem 1, \mathfrak{B} has an abelian group reduct $\langle B; +, -, 0 \rangle$ and an involutoric endomorphism β of the group structure such that $x * y = x\beta - y\beta$ for all $x, y \in B$. Given an $x' \in X'$, there is a unique $x \in X$ such that $x\alpha = x'$. Define $x'\varphi = x\varphi\beta$ and extend the map $\varphi: X \cup X' \to B$ to a homomorphism of the free abelian group $Ab(X \cup X')$ into $\langle B; +, -, 0 \rangle$. We claim that $x\alpha\varphi = x\varphi\beta$ for all $x \in F$ (see Figure 1). Indeed, if $x \in F$, then $x\alpha\varphi = x'\varphi = x\varphi\beta$ by

$$F \xrightarrow{\alpha} F$$

$$\downarrow \varphi \qquad \qquad \downarrow \varphi$$

$$B \xrightarrow{\beta} B$$
FIGURE 1

definition; if $x' \in X'$ then $x'\alpha\varphi = x\alpha\alpha\varphi = x\varphi$ while $x'\varphi\beta = x\varphi\beta\beta = x\varphi$ and hence $x\alpha\varphi = x\varphi\beta$ for all $x \in X \cup X'$ and hence for all $x \in F$. Now, for $x, y \in F$,

$$(x * y)\varphi = (x\alpha - y\alpha)\varphi$$
$$= x\alpha\varphi - y\alpha\varphi$$
$$= x\varphi\beta - y\varphi\beta$$
$$= x\varphi * y\varphi,$$

and hence $\varphi: \mathfrak{A} \to \mathfrak{B}$ is a homomorphism. This completes the proof that \mathfrak{A} is the free S-groupoid with X as its free set of generators.

LEMMA 3. $\mathfrak{A} = \langle F; * \rangle$ of Lemma 2 belongs to the equational class $L \lor R$.

Proof. For $x, y \in F$, define $\langle x, y \rangle \in \Theta$ iff $x\alpha - y\alpha = -x + y$. It is easy to see that Θ is an equivalence relation on the set F. Moreover, if $\langle x, y \rangle \in \Theta$ and $\langle z, t \rangle \in \Theta$, then

$$-(x * z) + (y * t) = -(x\alpha - z\alpha) + (y\alpha - t\alpha)$$
$$= -(x\alpha - y\alpha) + (z\alpha - t\alpha)$$
$$= -(-x + y) + (-z + t)$$
$$= (x - z) - (y - t)$$
$$= (x\alpha - z\alpha)\alpha - (y\alpha - t\alpha)\alpha$$
$$= (x * z)\alpha - (y * t)\alpha,$$

and hence $\langle x * z, y * t \rangle \in \Theta$ which shows that Θ is a congruence relation on $\mathfrak{A} = \langle F; * \rangle$. Since, by the proof of Lemma 1 x - y is a polynomial of $*, \Theta$ is also a group congruence.

Now, for all $x, y \in F$,

$$(x * y)lpha - (x - y)lpha = (xlpha - ylpha)lpha - (xlpha - ylpha)$$

= $(x - y) - (x lpha - y lpha)$
= $(x - y) - (x * y)$
= $-(x * y) + (x - y)$,

and hence $\langle x * y, x - y \rangle \in \Theta$ for all x, y in F. So, in the S-groupoid \mathfrak{A}/Θ , we have x * y = x - y, the left difference and hence $\mathfrak{A}/\Theta \in L$. Similarly, the S-groupoid $\mathfrak{A}/\Phi \in \mathbf{R}$ where

$$\Phi = \{ \langle x, y \rangle | x, y \in F, x\alpha - y\alpha = x - y \}$$

and so their direct product $\mathfrak{A}/\Theta \times \mathfrak{A}/\Phi \in L \vee R$. Now, for each $x \in F$, let $x\lambda = \langle [x]\Theta, [x]\Phi \rangle$. Thus λ is a homomorphism of \mathfrak{A} into $\mathfrak{A}/\Theta \times \mathfrak{A}/\Phi$. If $x\lambda = y\lambda$ for some x, y in F then $\langle x, y \rangle \in \Theta \cap \Phi$ and this implies that -x + y = x - y or 2x = 2y. But since the group structure in \mathfrak{A} is free, we have x = y. Thus \mathfrak{A} is isomorphic to subalgebra of the direct product and hence $\mathfrak{A} \in L \vee R$. This completes the proof of the lemma.

THEOREM 2. The identity (1) is a base for the equational theory of $I \cap J$.

Proof. As mentioned in the beginning of this section, it is sufficient to prove that $S \subseteq L \lor R$. Now, if $\mathfrak{B} = \langle B; * \rangle$ is any S-groupoid then it is a homomorphic image of some free S-groupoid $\mathfrak{A} = \langle F; * \rangle$ and by Lemma 2 every such \mathfrak{A} belongs to $L \lor R$. Since

equational classes are closed under homomorphic images we get the conclusion that $S \subseteq L \lor R$.

3. Applications. In $\S2$ we have used only identity (1) which is a special case of identity (2) of Lemma 1. In this section we will apply identity (2) to establish that certain familiar theories are onebased.

THEOREM 3. A finitely based equational theory Θ of symmetric difference groups is one-based.

Proof. Let Θ be an equational theory of groupoids by defined $I \cap J$ together with a finite set of identities. Recalling that Θ has the left cancellation property (because of (1) which belongs to $I \cap J$), any identity f = g is equivalent to f * g = 0. Now let f = 0 and g = 0 be any two identities in Θ with disjoint sets of variables. It is clear that, in presence of $I \cap J$, these two identities are equivalent to the single identity f * g = 0. Thus we can assume that Θ is defined by $I \cap J$ together with one identity w = 0. Hence Θ contains the identity (2) of Lemma 1. Conversely, the theory defined by the identity (2) with the above w contains, by Lemma 1, identity (1) and w = 0. Now, by Theorem 2, identity (1) is a base for $I \cap J$ and hence we have $I \cap J$ together with w = 0. This completes the proof of the theorem.

COROLLARY 1 (G. Higman and B. H. Neumann [3]). Any finitely based equational theory of J is one-based.

Proof. J has the identity x * 0 = x. Conversely, if a groupoid $\mathfrak{A} = \langle A; * \rangle$ satisfies both (1) and x * 0 = x then by property (iii) of Lemma 1, $x\alpha - 0\alpha = x$, that is $x\alpha = x$ for all x and hence x * y = x - y, the right difference and hence \mathfrak{A} satisfies all the identities of J. Thus J itself is defined by (1) together with x * 0 = 0 and hence any finitely based theory of J is one-based.

COROLLARY 2. Any finitely based theory which contains a theory of rings with right unit as a reduct is one-based.

REMARK. The above result was announced independently in [2] and [4].

Proof. Let Θ be a finitely based theory of type τ and let +, -, \cdot , 0, 1 be operation symbols in Θ such that their reduct in Θ is a theory of rings with right unit i.e. x1 = x is an identity. It is

well-known that such a theory of rings is definitionally equivalent to a theory in which + and - are replaced by a single binary operation * which stands for, say, the right difference. Now let f = 0 and g = 0 be two identities in Θ and let z and t be variables not occurring in f or g. It is clear that these two identities imply fz * gt = 0. Conversely, if fz * gt = 0, then fz * gt = fz * fz and one left cancellation yields fz = gt. Finally the substitution z = 1, t = 0yields f = 0 and similarly g = 0. In other words, modulo x1 = x, x0 = 0x = 0, and the symmetric difference properties of *, any finite number of identities in Θ can be equivalently expressed by a single identity, say $w_1 = 0$. Now define the polynomial w as

$$(w_1x * w_1y) * (((x_1(x_2 * x_3)) * (x_1x_2 * x_1x_3)) * ((x_41 * 0x_5) * (x_4 * 0)))$$
,

where x, y, x_1, \dots, x_5 are variables not occurring in w_1 and multiplication has precedence over *.

Let $\mathfrak{A} = \langle A; F \rangle$ be an algebra of type τ satisfying identity (2) of Lemma 1 with this w. Then the reduct $\langle A; * \rangle$ is an SD-group and \mathfrak{A} satisfies the identity w = 0.

In the following computation we will often apply the property that a * b = 0 implies a = b which is true in any SD-group. From w = 0 we get immediately

$$(10) \qquad (w_1x)*(w_1y) = ((x_1(x_2*x_3))*(x_1x_2*x_1x_3))*(x_4x_1*0x_5)*(x_4*0).$$

The substitution x = y in the above yields

(11)
$$(x_1(x_2 * x_3)) * (x_1x_2 * x_1x_3) = (x_4 1 * 0x_5) * (x_4 * 0)$$

Now $x_4 = 0$, $x_5 = 1$ in the above makes the right hand side 0 * (0 * 0) = 0 * 0 = 0 and hence we obtain the distributive identity

(12)
$$x_1(x_2 * x_3) = x_1 x_2 * x_1 x_3 .$$

Setting $x_2 = x_3$ in the above we get

(13)
$$x_1 0 = 0$$
.

Now from (11) and (12) we have

$$x_4 1 * 0 x_5 = x_4 * 0$$
.

Putting $x_5 = 0$ and using (13) and (15) we obtain

(14)
$$x_4 1 = x_4$$
,

which, in turn, yields, by the left cancellation property of *,

$$0x_5=0,$$

and hence $w_1 = 0$ is satisfied in \mathfrak{A} . This proves that the theory Θ is one-based.

References

1. G. Grätzer, Universal Algebra, University Series in Higher Mathematics, Princeton, N.J., Van Nostrand (1968).

2. G. Grätzer and R. McKenzie, Equational spectra and reduction of identities, Notices of the Amer. Math. Soc., 14 (1967), 697.

3. G. Higman and B. H. Neumann, Groups as groupoids with one law, Publ. Math. Debrecen, 2 (1952), 215-221.

4. A. Tarski, Equational logic and equational theories of algebras, In Contributions to Mathematical Logic, North-Holland Publishing Company, 1968, 275-288.

Received March 26, 1974 and in revised form September 10, 1977. This research of both the authors was supported by the National Research Council of Canada.

UNIVERSITY OF MANITOBA WINNIPEG R3T 2N2 CANADA

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

RICHARD ARENS (Managing Editor)

University of California Los Angeles, CA 90024

CHARLES W. CURTIS

University of Oregon Eugene, OR 97403

C.C. MOORE University of California Berkeley, CA 94720

J. DUGUNDJI

Department of Mathematics University of Southern California Los Angeles, CA 90007

R. FINN and J. MILGRAM Stanford University Stanford, CA 94305

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF K. YOSHIDA

111 1 001110

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA CALIFORNIA INSTITUTE OF TECHNOLOGY UNIVERSITY OF CALIFORNIA MONTANA STATE UNIVERSITY UNIVERSITY OF NEVADA, RENO NEW MEXICO STATE UNIVERSITY OREGON STATE UNIVERSITY UNIVERSITY OF OREGON UNIVERSITY OF SOUTHERN CALIFORNIA STANFORD UNIVERSITY UNIVERSITY OF HAWAII UNIVERSITY OF TOKYO UNIVERSITY OF UTAH WASHINGTON STATE UNIVERSITY UNIVERSITY OF WASHINGTON

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and journal, rather than by item number. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

50 reprints to each author are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The Pacific Journal of Mathematics is issued monthly as of January 1966. Regular subscription rate: \$72.00 a year (6 Vols., 12 issues). Special rate: \$36.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708. Older back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.).

8-8, 3-chome, Takadanobaba, Shinjuku-ku, Tokyo 160, Japan.

Copyright © 1978 by Pacific Journal of Mathematics Manufactured and first issued in Japan

Pacific Journal of Mathematics Vol. 74, No. 2 June, 1978

Aharon Atzmon, Spectral synthesis in some spaces of bounded continuous	
functions	277
Karl Egil Aubert and Isidor Fleischer, <i>Tensor products of ideal systems and their modules</i>	285
Richard F. Basener. Several dimensional properties of the spectrum of a uniform	
algebra	297
R. H. Bing and Michael Peter Starbird, <i>Super triangulations</i>	307
Andrew Carson, <i>Coherent polynomial rings over regular rings of finite index</i>	327
Robert M. DeVos and Frederick W. Hartmann, <i>Sequences of bounded summability</i>	
domains	333
George Grätzer and R. Padmanabhan, <i>Symmetric difference in abelian groups</i>	339
Robert L. Griess, Jr., A remark about groups of characteristic 2-type and	
<i>p-type</i>	349
Emil Grosswald and F. J. Schnitzer, A class of modified ζ and L-functions	357
Jutta Hausen and Johnny Albert Johnson, <i>Ideals and radicals of some</i>	
endomorphism rings	365
Jean Ann Larson, A solution for scattered order types of a problem of	
Hagendorf	373
Peter A. McCoy, <i>Extremal properties of real biaxially symmetric potentials in</i> $r^{2(\alpha+\beta+2)}$	201
$E^{2(\alpha+p+2)}$	381
Hector Alfredo Merklen, <i>Hereditary crossed product orders</i>	391
Hal G. Moore and Adıl Mohamed Yaqub, Equational definability of addition in	407
certain rings	407
Robert Laurens Moore, Reductivity in C*-algebras and essentially reductive	410
operators	419
Joseph Alvin Neisendorfer, Lie algebras, coalgebras and rational homotopy	420
theory for nupotent spaces	429
William Raymond Nico, <i>Bounded monoids</i>	461
Richard Paul Osborne, Simplifying spines of 3-manifolds	473
Richard Paul Osborne, <i>The simplest closed 3-manifolds</i> . With an appendix by	101
Osborne and J. Yelle	481
Clayton Collier Sherman, <i>The K-theory of an equicharacteristic discrete valuation</i>	407
ring injects into the K-theory of its field of quotients	497
Mitchell Herbert Taibleson, The failure of even conjugate characterizations of H ⁺	501
on local fields	501
Keti Tenenblat, On characteristic hypersurfaces of submanifolds in Euclidean	
<i>space</i>	507
Jeffrey L. Tollefson, <i>Involutions of Seifert fiber spaces</i>	519
Joel Larry Weiner, An inequality involving the length, curvature, and torsions of a	
curve in Euclidean n-space	531
Neyamat Zaheer, On generalized polars of the product of abstract homogeneous	
polynomials	535